MAYER • BROWN

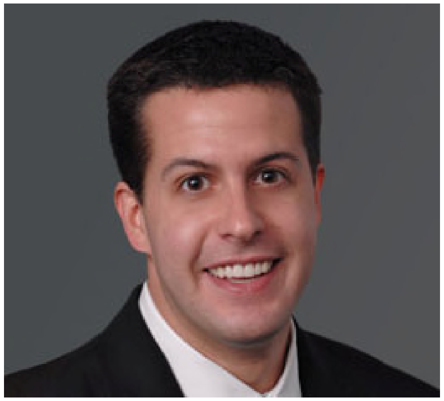
Internet of Things for B2B

Connected Devices, Data and IoT

Rebecca Eisner	Joe Pennell
Partner	*Partner*
+1 312 701 8577	+1 312 701 8354
reisner@mayerbrown.com	jpennell@mayerbrown.com

Speakers

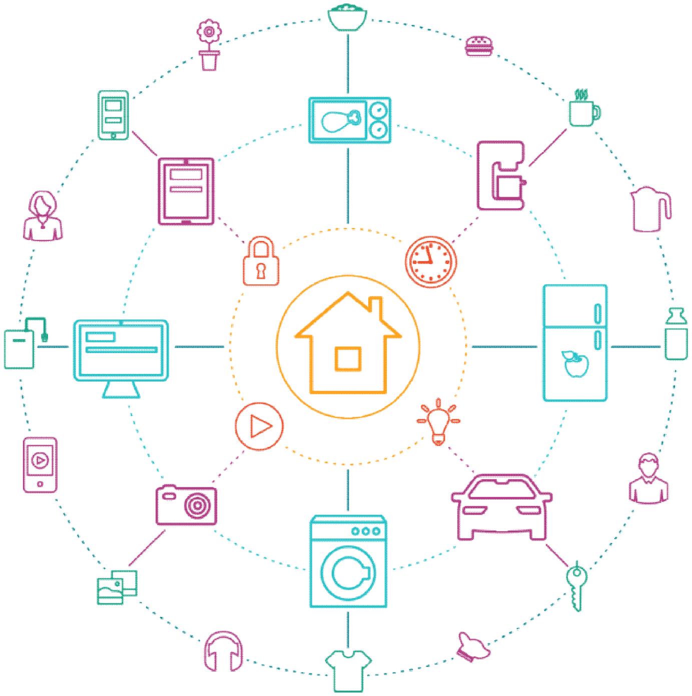
Rebecca Eisner
Partner - Chicago

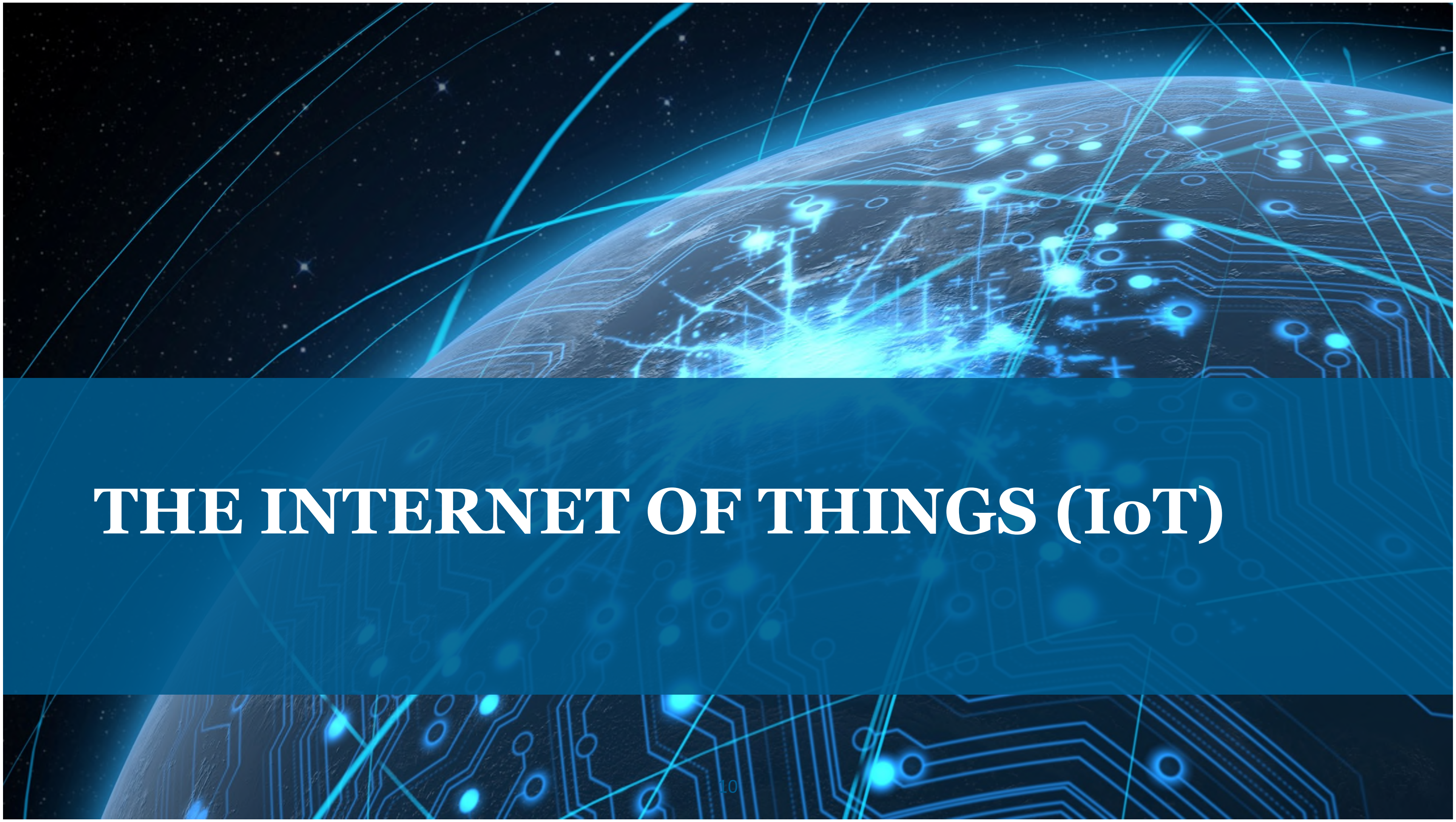


Joe Pennell
Partner - Chicago

Agenda

- Internet of Things (IoT) for B2B Overview
- Regulatory Response to IoT
- Contracting Challenges for IoT





THE INTERNET OF THINGS (IoT)

Internet of Things - Definition

- What is the Internet of Things?
  - No widely accepted definition, but common thread: “How computers, sensors and objects interact with one another and process data” (FTC Staff Report, Jan 2015)
  - Includes smart hardware/devices used in B2B (RFID tags to monitor inventory, jet engines, oil rigs) and consumer-facing devices (e.g., thermostats, door locks, appliances, vehicles)
  - Wide range of benefits from data and value derived from data (e.g., improved health care, reduced energy use, industrial efficiency, safety and convenience)

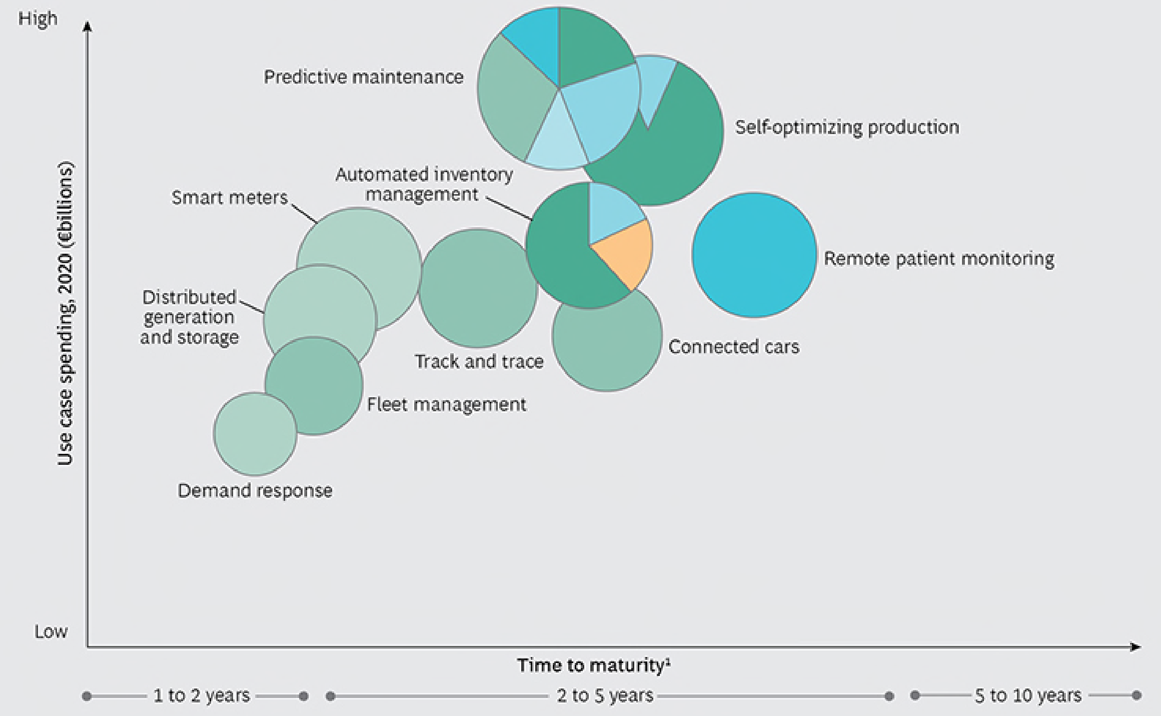
"Smart Everything"—
the Impact of the Internet of Things

- Growth
  - Cisco estimates that connected devices will increase from 16 billion (as of 2015) to 26 billion by 2025
  - McKinsey estimates that by 2025, overall IoT impact on global economy will be $4 to $11 trillion

(Source: Department of Commerce, Jan 2017)

IoT for B2B

EXHIBIT 2 | Ten Use Cases Will Drive IoT Growth Through 2020



Most relevant industries

- ● Discrete manufacturing
- ● Transportation and logistics
- ● Utilities
- ● Health care
- ● Process industry
- ● Energy and natural resources
- ● Retail

Sources: BCG (Boston Consulting Group) Internet of Things buyer survey; IDC; expert interviews; BCG analysis.

Note: The bubble sizes indicate relative amounts of spending.

IoT for B2B

- Growth within the Internet of Things ecosystem will occur at an uneven rate, with Boston Consulting Group estimating:
  - Two layers of the IoT technology stack (services and analytics/applications) will capture 60% of IoT-related growth by 2020;
  - Approximately half of IoT spending will be concentrated in three industries
    - Discrete manufacturing
    - Transportation and logistics
    - Utilities

https://www.bcgperspectives.com/content/articles/hardware-software-energy-environment-winning-in-iot-all-about-winning-processes/

IoT FOR B2B – THE REGULATORY RESPONSE

Regulatory Issues

- Overview
- Personal data regulation
- Security concerns and liability
- New potential sources of risk and liability

IoT US Regulatory Overview

- U.S. federal regulation is a combination of the FTC's general consumer protection and industry-specific standards
  - FTC enforcement actions (such as those against D-Link and ASUS) generally charge device manufacturers with engaging in unfair or deceptive acts or practices
- Sector-specific regulations provide non-binding best practices to IoT stakeholders
  - FDA's recommendations in "Postmarket Management of Cybersecurity in Medical Devices"
  - NHTSA's "Federated Automated Vehicles Policy"

IoT US Regulatory Overview

- U.S. Regulatory Environment – Consumer Protection Oriented, and "Wait and See" Approach
  - Rep. Greg Walden (R-Ore. and Chairman of the Subcommittee on Communications and Technology) has raised concerns over IoT legislation or regulation locking ineffective policies into statute, allocating resources unwisely, or stymieing innovation: *"While I'm not taking a certain level of regulation off the table, the question is whether we need a more holistic approach."*
  - Maureen Ohlhausen (acting head of the FTC): *"We're saying not 'Let's speculate about harm five years out,' but 'Is there something happening that harms consumers right now or is likely to cause harm to consumers,'… If there is potential harm to consumers in a new technology, the FTC should not act until that harm manifests. We don't know if that risk will materialize. It may well materialize, but a solution may materialize at the same time."*

IoT Europe Regulatory Overview

- Though the European Union (EU) has not adopted regulations that are specifically designed for IoT, the following data protection regulations apply:
  - EU Data Protection Directive 95/46/EC for IoT data related to identified or identifiable natural persons (i.e., personal data)
    - Once the GDPR replaces Directive 95/46/EC in May 2018, it will become the primary mechanism for IoT regulation throughout Europe
  - Specific provisions of ePrivacy Directive 2002/58/EC (as modified by Directive 2009/136/EC) also apply with respect to the privacy of end users of IoT devices

IoT Personal Data Concerns

- Use of IoT in business and commercial settings may result in gathering of personal data, triggering privacy regulatory concerns (even more challenging in the EU)
- Even with B2B applications, incidental personal data about employees may be collected
- Smart devices leave a digital footprint on users, which can create a “Big Brother” effect for employees and users

IoT Personal Data Concerns

- For example, machine data may indicate how long equipment was in operation, geolocation data, and even user behavior data, which may highlight job performance or other issues
  - *Does idle machinery mean the operator is not performing her job?*
  - *What if geolocation data indicate an employee is somewhere that they were not supposed to be?*
  - *What if a sensor on equipment indicates that the person who performed maintenance on the equipment recently forgot to replace a part or perform a safety check?*

IoT Personal Data Concerns

- Various states (e.g., Minnesota) have privacy aspects of their employment statutes
  - There have been invasion of privacy cases – e.g., claim based on employer’s use of telematics to track an employee’s location 24 hours a day without the employee’s knowledge
  - Some states (e.g., Connecticut) prohibit employers from using electronic surveillance, including GPS, without express employee consent
- IoT-related employee data may also arise as a result of employee wellness programs (e.g., through the use of fitness wearables such as Fitbit) triggering HIPAA, EEOC and other state obligations

IoT Europe Regulatory Overview

- GDPR contains many new requirements that will have an impact on IoT development and use, even in the B2B context
  - EU defines personal data much more broadly, so personal data collected in a B2B setting is subject to GDPR
  - Businesses are required to follow “privacy by design”
  - Businesses must complete “data protection impact assessments” in some situations, including those that result in “profiling” or where there is systematic monitoring of publicly accessible areas on a large scale
  - Data subjects have other privacy rights that must be accommodated in IoT solutions that involve personal data capture

IoT Security Concerns

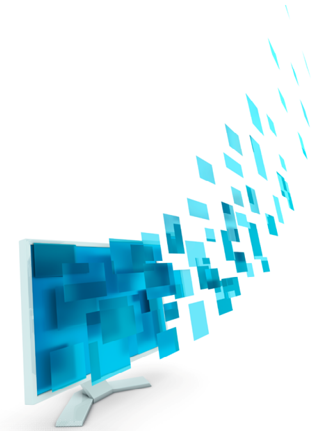
- IoT Device Manufacturers May Not Prioritize Security
- Standardized IoT Devices = Increased Risk of Breach
- Increased Physical Access = Increased Vulnerabilities
- Highly Networked = More Openings to Your Network
- **Example:** DDOS attack by "an army of IoT devices protected only by factory default passwords."

IoT Security Concerns

- Manufacturer Liability Case Study: VTech
  - VTech makes children’s learning toys that rely on web-based services.
  - VTech’s products required consumers to provide personal information.
  - A malicious third party allegedly bypassed VTech’s security measures by using a structured query language (SQL) “injection attack.”
  - The plaintiffs claim the attack was successful because VTech’s security was poorly designed and implemented.
  - The plaintiff’s complaint alleged violations of the Illinois Consumer Fraud and Deceptive Business Practices Act, breach of contract, breach of good faith and fair dealing, breach of implied warranty and negligence.

IoT Data Use and Ownership

- Who owns the data or who is the “controller?”
  - Raw data
  - Derived or aggregated data
- Anonymization and de-identification may be impossible
- Data portability / exit rights



IoT Data Use and Ownership

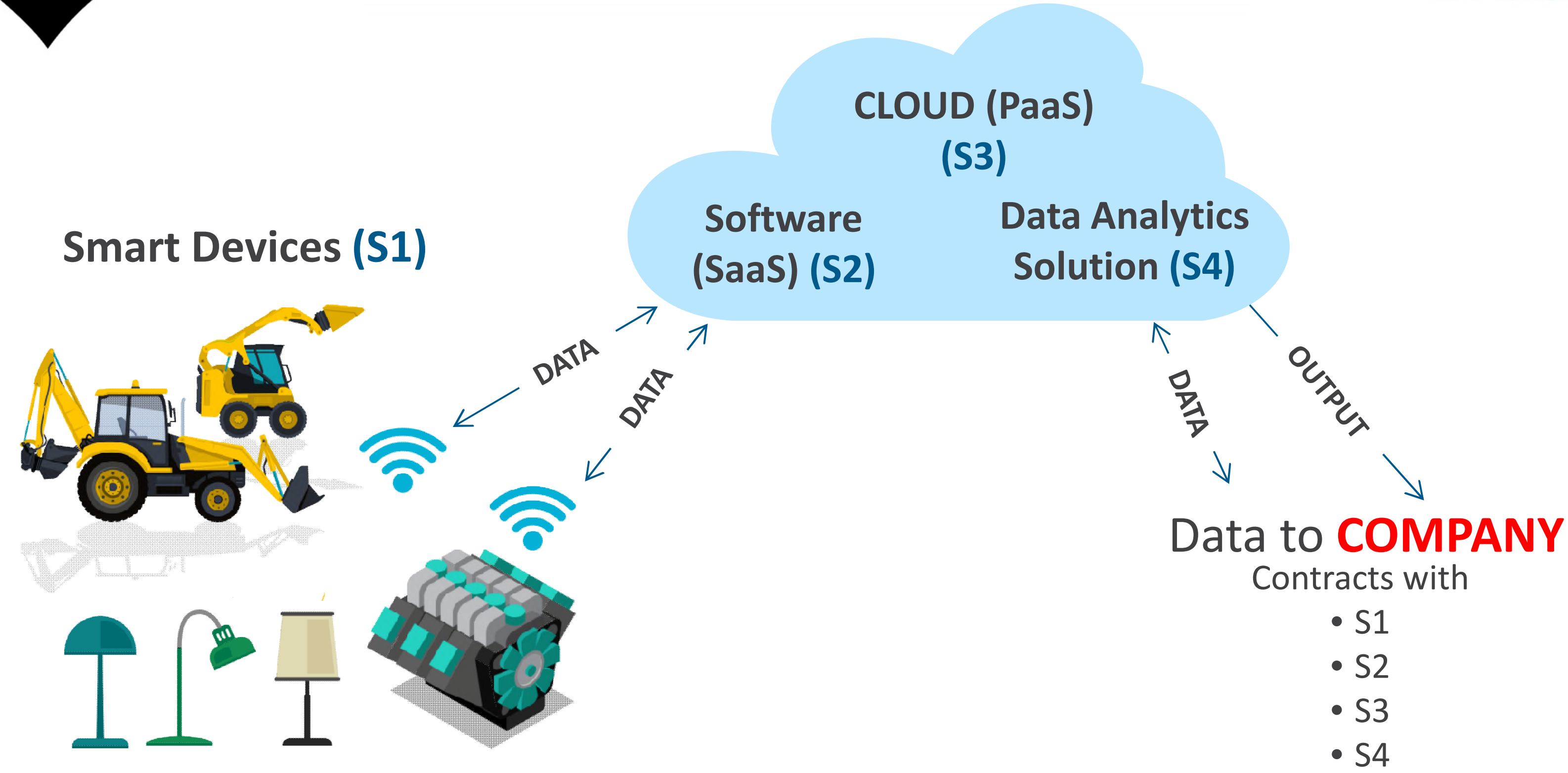
- Data Ownership Case Study: PrecisionHawk
  - PrecisionHawk sells unmanned aircraft systems (UAS), including hardware, software and training services.
  - UAS technology is being utilized for agricultural applications, such as crop scouting and water management.
  - PrecisionHawk’s clients include a number of companies that are competitors in the large-scale feed industry.
  - The American Farm Bureau Federation recommends farmers negotiate data rights - data gathered may reveal trade secrets or information about employees

IoT Issue: New Potential Liability/Regulatory Oversight Concerns

- Increased risk of harm to a person or property (e.g., smart machinery operating autonomously)
- Additional data from IoT sensors may increase discovery obligations (and data available to plaintiffs)
- Increased liability for product defects or other safety problems because more harms are arguably foreseeable
- Commentators have noted that ease of availability of compliance and risk data may increase risk of more regulatory oversight
- Regulators may demand data relating to regulatory compliance issues (e.g., work site safety compliance)

IoT FOR B2B - CONTRACTING CONSIDERATIONS

Example IoT Scenario



Smart Devices (S1)

CLOUD (PaaS) (S3)

Software (SaaS) (S2)

Data Analytics Solution (S4)

Data to **COMPANY**

Contracts with

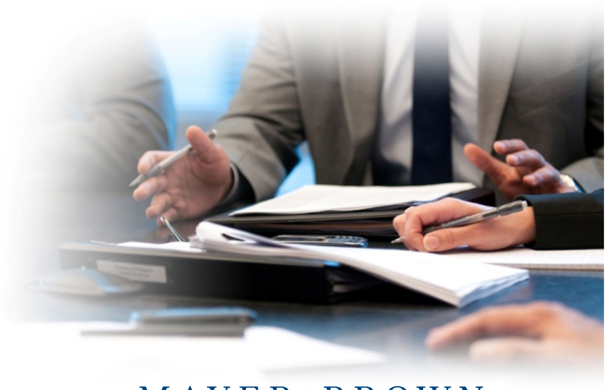
- S1
- S2
- S3
- S4

IoT Issue: Preparing to Contract

- Develop contracting policies (e.g., cloud)
- Conduct due diligence (legal, technical, security)
- Identify risks and risk mitigation strategies
- Understand hidden costs
- Avoid one-sided supplier forms – negotiate
- Understand where you may compromise – in advance
- Invest in templates (e.g., end-to-end IoT solution, cloud, data analytics, etc.)
- Appoint individuals who will serve as contact point with supplier

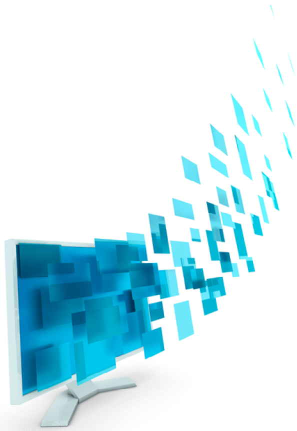
IoT Issue: Contracting Challenges

- IoT Reliance on Open Source Licenses
  - If the Customer becomes subject to these licenses, is the Customer obligated to disclose Customer IP to Open Source community?
  - Can the Supplier identify the Open Source in its supply chain?
  - Rep and warrant as to Open Source
- “As-Is” Contract Terms
  - One-sided, Supplier-oriented
  - Subject to unilateral change at a URL
  - Click wraps
- Interoperability / “Walled Gardens”



IoT Issue: Technology Currency Challenges

- Difficulties in patching/updating
- Related integration problems
- Allocate responsibility for maintenance and updates
- End-of-life issues
    - How long will devices be supported?
    - Deprecation/sunset policies
    - Notice period before support ends



IoT Issue: Integration Challenges

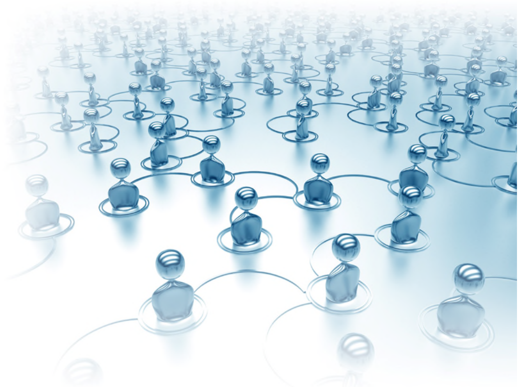
- Few “end-to-end” solutions
  - Customer must map integration points
  - Use service integrators as prime contractors
- Change Management
  - Require advance notice of changes
  - Request roadmap insight
  - Monitor URLs, websites and portals used to communicate changes
- Incident Response
  - Outage and security incident response plans must account for multiple providers

IoT Issue: Supplier Governance Challenges

- Standardized service platforms do not allow for customized supplier relationship management
  - Designated governance teams and committees are not within the cost model
  - Robotically automated processes cannot speak to you
- Invest in a new governance model and new skills to manage across the contracting, technology and integration issues
- Implement master agreements for panel providers to supersede click-wrap terms and achieve adequate scale for governance efforts
- Assign customer personnel to build personal connections via sales channels and user groups

Summary

- IoT presents a host of B2B opportunities
- Businesses that adopt IoT will need to keep a close eye on regulatory developments and adoption of relevant industry standards
- Contracting for IoT in B2B presents different issues than traditional procurement of IT goods and services
- You can help your Company to be better prepared to use B2B IoT with advance preparation through policies, templates, knowledgeable business stakeholders, and governance models



QUESTIONS?

Rebecca Eisner
Partner

+1 312 701 8577
reisner@mayerbrown.com

Joe Pennell
Partner

+1 312 701 8354
jpennell@mayerbrown.com