MAYER·BROWN

How Smart, Connected Products Are Transforming Business

Linda L. Rhodes

The Connected World

- Connected products are now ubiquitous, and their use is projected to dramatically increase in the foreseeable future.
- Gartner's past and future forecasts:
  - 8.4 billion connected "things" were in use worldwide in 2017, and will reach 20.4 billion by 2020.
  - Total spending on endpoints and services reached almost $2 trillion in 2017.
- The vast majority of which were consumer products and applications.

  (source: https://www.gartner.com/newsroom/id/3598917)
- B2B: Spending will be concentrated in three industries:
  - Discrete manufacturing
  - Transportation and logistics
  - Utilities

U.S. Legal and Regulatory Framework

- U.S. legal and regulatory landscape is still developing:
  - Legislators are considering new laws to address the new issues raised by connected products; and
  - Regulators seek to adapt policy and guidance to new circumstances.
- FTC enforcement actions generally charge device manufacturers with engaging in unfair or deceptive acts or practices:
  - **ASUS:** FTC alleged that ASUS failed to secure routers and cloud services it marketed to consumers. ASUS entered into a settlement requiring it to maintain a comprehensive security program.
  - **Vizio**: The FTC and Vizio reached a settlement related to Vizio's collection of consumer television viewing habits without viewer consent, which data could be aggregated with other data to derive personal information of the viewer.
  - State Breach Notification Laws

Sector-Specific Regulations and Best Practices

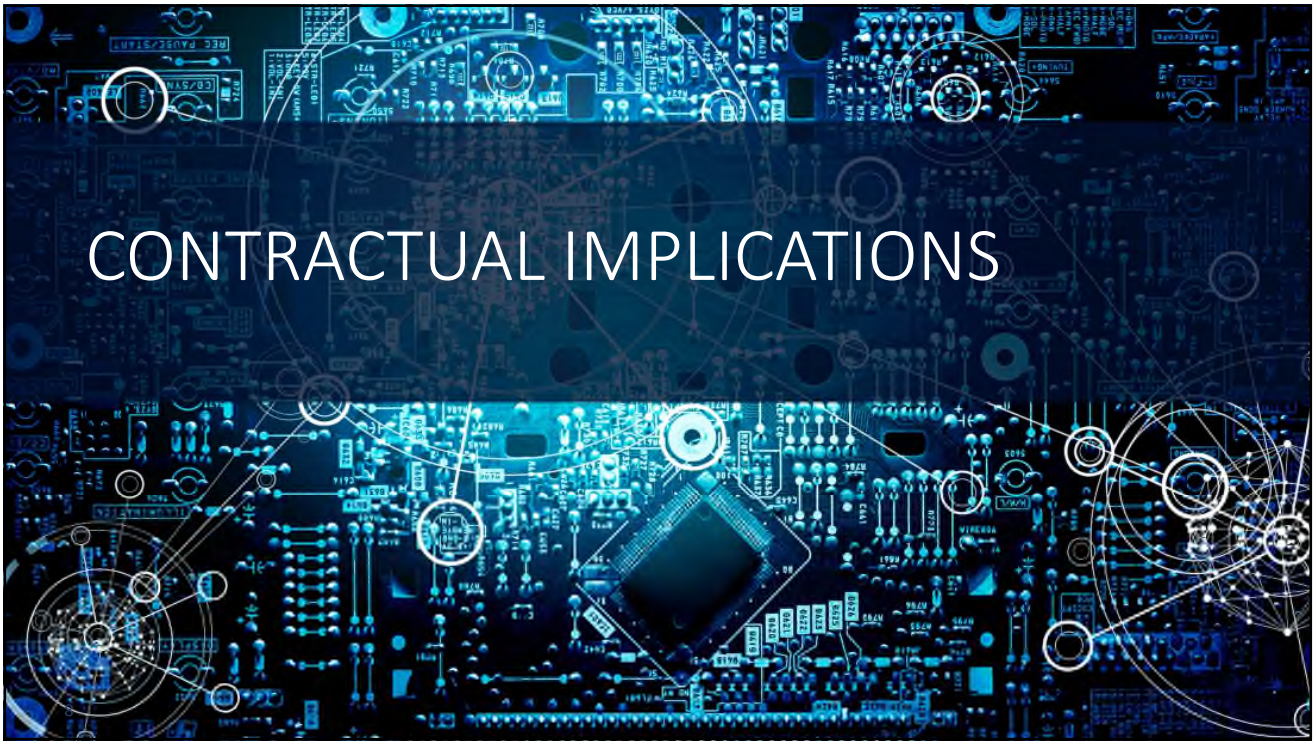
- Sector-specific regulations: bringing technology providers into the regulatory fold:
  - PCI Compliance
  - HIPAA
  - NHTSA Safety Act
- Sector-specific best practices and guidance:
  - FDA's recommendations in "Postmarket Management of Cybersecurity in Medical Devices"
  - NHTSA's "Enforcement Bulletin," "Federated Automated Driving Systems" and "Cybersecurity Best Practices"
  - Privacy Principles
- Employee Issues: Various states (*e.g.*, Minnesota) have privacy aspects of their employment statutes

European General Data Protection Regulation

- The European General Data Protection Regulation ("GDPR") contains many new requirements that will have an impact on development and use of Connected Devices, including 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 connected solutions that involve personal data capture.
- Other Country Data Protection Laws (*e.g.*, data localization).

Data Collection, Use and Consent: Case Study

- 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 that farmers negotiate data rights. Data gathered may reveal trade secrets or information about employees.



Contractual Implications: Standards, Protocols and Best Practices

- Standards, protocols and best practices need to be retooled to address the evolving risks raised by the inclusion of interconnected technologies.
  - Think "by design."
  - Consider the applicability of enterprise IT techniques to connected products (*e.g.*, limit access to the minimum extent necessary for performance of obligations: segmentation and isolation techniques).

Contractual Implications: Roles and Responsibilities

- Allocate responsibility for monitoring, identifying and remediating vulnerabilities and risks:
  - Which party is best suited to monitor and identify vulnerabilities? To assess the impact of the vulnerability on the security and safety of the connected product?
- Enhance testing approaches to ensure security and safety across integrated technologies.
- Address documentation requirements and obligations to evidence "by design" requirements.
- Tie audit cadence to risk assessment.
- Require regularly reporting on testing.

Data Collection, Use and Consent

- The fast-paced growth of connected devices will result in exponential growth in data collection, raising issues with respect to data usage rights and consent.
- Types of data:
  - Critical safety data (*e.g.*, event data recorders);
  - Non-safety critical data (*e.g.*, consumer preferences);
  - Both (geolocation).
- Uses: For the functionality, maintenance and support of the connected product? To improve product performance? For other business purposes?
- Anonymization and de-identification may be impossible.

Technology and Technology Currency

- Understand the use of Open Source Licenses in connected product:
  - 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?
  - Representations and warranties as to Open Source.
- Allocate responsibilities in patching/updating and related integration problems.
- Address end-of-life issues:
  - How long will devices be supported?
  - Notice period before support ends.

Incident Response; Risk Allocation

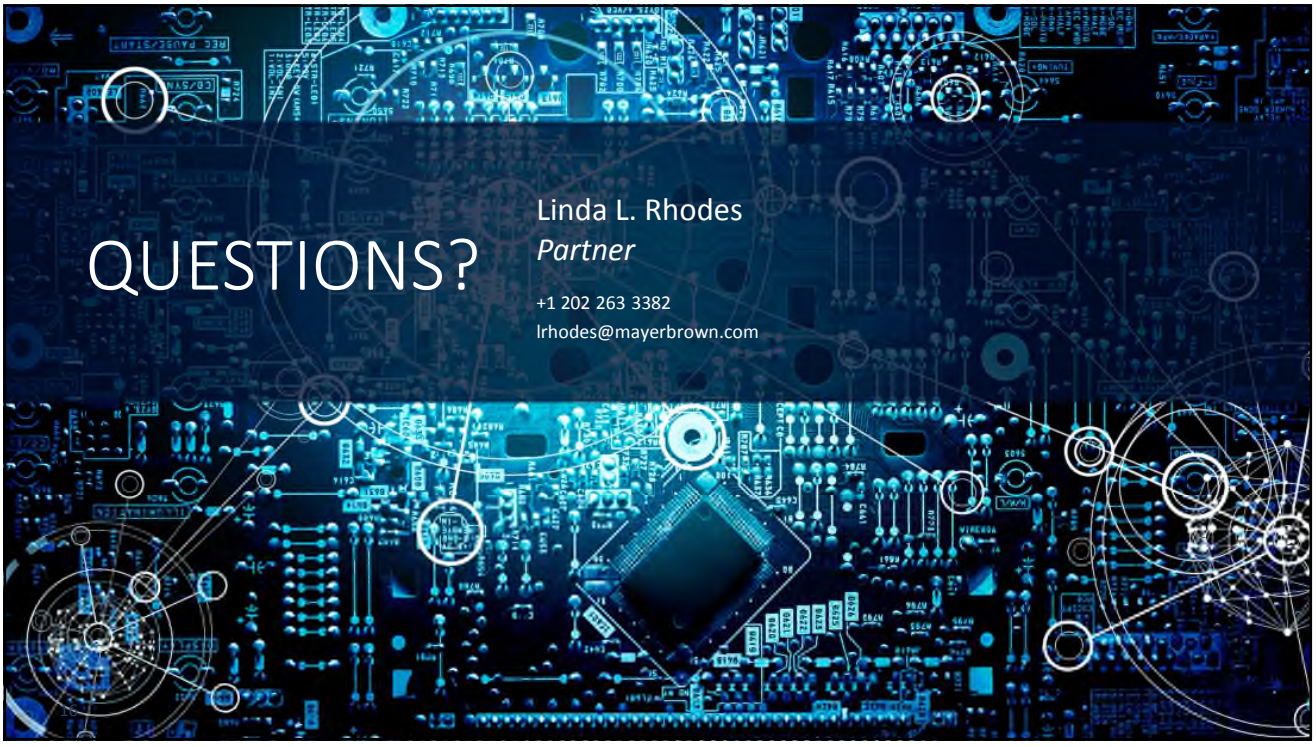
- Incident Response
  - Allocate responsibilities for root cause analysis.
  - Was the incident the result of supplier's defective products? Problems arising from integrated systems? A combination of both?
  - Outage and security incident response plans must account for multiple providers.
- Technology companies new to regulated industries may not be accustomed to bearing the responsibility for, nor indemnifying against, personal injury claims and regulatory remedies that arise out of functionality defects or security vulnerabilities in their technology.

Ownership and Licenses

- Allocate ownership in work product and product developments. Consider advantages and disadvantages associated with which party owns the IP.
  - Suppliers want to own developments to continue to develop their technologies.
  - Customers desire to own developments to protect competitively sensitive material.
  - Balance the need to incentivize suppliers to improve the products against the Customer's desire to own developments.
  - Consider exclusive licenses to protect competitive advantage.
- Obtain licenses to Supplier IP, including rights in background IP incorporated into owned work product, and rights necessary for support and maintenance and remedying safety issues and security breaches.

Contracting Summary

- Contracting for connected products is becoming more complex with the growth of safety and cybersecurity risks, the tremendous complexities of interconnected systems, the application of security safeguards and protocols to product risks, the proliferation of guidance and the inclusion of new supplier types.
- Customers can successfully contract for developing, implementing and/or utilizing connected technology and software through an understanding of the changing landscape and related challenges, combined with a diligent, thoughtful and creative approach to documenting contract requirements, allocating responsibilities and rights and managing risks to account for the new landscape.



MAYER·BROWN