MAYER | BROWN

How Smart, Connected Products are Transforming Business

By Marjorie Loeb, Linda Rhodes, Riley Moore, Dean Won

Connected products are now ubiquitous, and their use is projected to dramatically increase in the foreseeable future. An estimated 8.4 billion connected "things" were used in 2017, the vast majority of which were consumer products and applications.[1] The prevalence of these connected products is projected to double between now and 2020.

While bringing significant benefits to consumers and businesses through enhanced functionality, convenience and customization, connected products also raise important considerations for technology transactions. In particular, connected products require the integration of complex technologies, creating challenges for achieving the interoperability required for functionality. In addition, this connectivity can unintentionally open multiple cybersecurity attack points with respect to which security measures and safeguards must be implemented and maintained. The fast-paced growth in this area will result in exponential growth in data collection, raising issues with respect to data usage rights and consent. Connected products are already used prominently in regulated industries, where the implications of regulatory compliance and consumer safety are key contracting considerations. Customers must be confident that their products work as intended and understand the technology and licensing restrictions and requirements of the technologies enabling the product functionality.

Accordingly products must be secure from unauthorized access or manipulation, must collect and use data consistent with applicable privacy and security laws, and must comply with other applicable regulations and industry standards governing functionality. Contracts between suppliers and customers for technology to build connected products must define responsibilities and allocate risk in support of these fundamental objectives.

Legal and Regulatory Landscape

In the United States, the legal and regulatory landscape is still developing, as legislators begin to propose and consider laws addressing the new issues raised by connected products, and existing regulatory bodies, including the Federal Trade Commission, seek to adapt policy and guidance to new circumstances.

CYBERSECURITY AND CONSUMER SAFETY

Connected products are highly networked, and access to one device opens up access to other devices connected to that network. For hackers looking to access either the broader network of a business or multiple devices of an individual, connected products are an attractive point of entry. In addition to the risks associated with general data breaches, connected products can present particular cybersecurity risks for consumers and companies alike. Specifically, with products

like smart medical devices and connected cars, a security breach of the network on which those products rely could result in real-time death and bodily injury to end users.

Consumers have brought claims against businesses for transmission of product performance and use data, as well as consumer data, via unsecured transmissions.[2] While decisions have varied as to the standing of plaintiffs where no actual harm occurs, the DC Circuit held that, in a case brought for data breach involving credit card and social security numbers, a substantial risk of harm existed simply by virtue of the data breach and the nature of the data stolen, even if there were no allegations that harm (in this case, identity theft) had occurred.[3] This same principal, that a substantial risk of harm is enough, has been supported in the context of regulated devices. For example, NHTSA required the recall of vehicles to address security vulnerabilities even without a showing that anyone had tried to exploit the vulnerability.

Lawmakers are contemplating these issues and are beginning to set the groundwork for legislation. In September of 2017, for example, the US House of Representatives unanimously passed the SELF DRIVE Act (H.R. 3388 (115th)), a bill giving federal regulators the power to regulate self-driving vehicles. The bill includes a requirement for vehicle manufactures to develop a "written cybersecurity policy with respect to the practices…for detecting and responding to cyber attacks or unauthorized intrusions."[4]

DATA COLLECTION AND DATA PRIVACY

Data collection (both direct and incidental) through connected devices means providers of such technology must comply with increasingly stringent privacy requirements. In 2014, 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. Vizio was required to delete the data it collected and put a privacy program in place to evaluate Vizio's practices and its partners.[5] In addition, Vizio must now disclose its data collection methods and receive consumers' express consent to collect this information.[6] The FTC applied established consumer protection principles grounded in transparency and consent and released best practice guidance that companies should follow when collecting data via connected products: (1) explain your data collection practices up front; (2) get consumers' consent before you collect and share highly specific information about their entertainment preferences; and (3) make it easy for consumers to exercise options.

Numerous additional privacy issues are raised by connected products. For example, many connected consumer devices are portable, requiring consideration of privacy laws in multiple jurisdictions relating to geolocation and other data protection issues.

Contractual Implications

To build successful supplier relationships for the design, creation, sale and maintenance of connected products and solutions, customers and suppliers will need to consider the risks associated with the connected products and allocate those risks in their supply agreements. Connected products may be used for business purposes or sold as consumer products, and the risks should be considered in relation to the context in which the products will be used.

That allocation of risk may be very different from more traditional technology acquisitions. One key difference is in the area of product liability, a concept that has not been a critical focus in traditional technology transactions. For example, contracts for the supply of software and services have limits on liability for warranty or other breaches and exclusions

of damages that are typical to the technology industry but which sharply contrast with the warranty provisions and assumption of liability often expected by manufacturers from component suppliers in the sales of goods and services under purchase orders governed by the Uniform Commercial Code.

PRODUCT FUNCTIONALITY

Connected devices can be almost anything, in the case of consumer products, from smart refrigerators and televisions, wearable clothing, medical monitoring and dosing devices and personal assistants, to, in the case of business use, devices that gather data about heavy machinery operation, or track manufacturing parts or shipments. Whether used in a consumer or a business context, connected products rely on integrated or external technology, data collection and analysis. The technology, data collection, data processing and analysis are likely to be provided by multiple suppliers, creating numerous integration points, and potential points of failure. Building a connected products offering means managing an ecosystem of relationships and integrating different technologies. Accordingly, incorporating detailed design standards and requiring adherence to protocols and best practices in supply contracts are key to developing products that work as intended and are compliant with industry standards governing functionality. Achieving and maintaining inter-operability among the components in the product ecosystem is critical to sustaining performance throughout the life of the product. In addition to determining product specifications for individual components, the parties will need to allocate responsibility for establishing and testing interfaces to integrate the necessary components and to test the functionality and security of the overall system.

The rapid pace of technology change necessitates the inclusion of contractual terms delineating responsibilities with respect to technical evolution and remotely delivering upgrades. The parties should consider a change management process to address both technology evolution and other necessary changes in one or more individual components or the potential need to substitute a supplier. An effective change management process will need to address the extent to which a supplier will be required to cooperate with the business customer, as well as other suppliers. In some cases, suppliers will need to share confidential and proprietary information with, or provide access to software code to facilitate the update by another supplier or the business customer, particularly in the case of a product comprised of many integrated components.

CYBERSECURITY

Businesses developing connected products and solutions need to build into their standards new approaches and requirements to address growing cybersecurity risks, pass through to suppliers the obligation to comply with these evolving standards and maintain flexibility to update standards during the contract term. External guidance and best practices related to cybersecurity are growing vastly. Technology contracts will need to consider the parties respective responsibilities for staying abreast of the same and build requirements for compliance with appropriate external standards into their contracts. Additionally, the parties will need to work through the tension between cybersecurity principles, premised on providing each supplier access to technology components only to the extent necessary to supply the particular component or service, and the benefits of open architecture with broader access to share responsibility for testing and integration and enhance product innovation in support of product functionality as described above.

Further, although customers may have experience negotiating for cybersecurity protections in enterprise systems, they will need to rethink their approach as they seek to build cybersecurity protections into their products intended for consumer use. There are fundamental differences between enterprise cybersecurity practices, which are largely aimed at protecting against business risks arising from unauthorized access to confidential and personal data, versus product cybersecurity practices, which will require protecting individuals from actual physical injury or death , and rely on product liability concepts, in addition to data security concepts.

In the case of consumer products, the parties need to consider product liability concepts, including thinking beyond the prescribed use of the product to reasonably anticipated use or even misuse. This includes anticipating connections to devices and data sources from outside of the eco-system which is the subject of the contract, with the result that the parties must consider how to allocate risk and responsibilities for mitigation procedures (e.g., authentication procedures, fall back modes) from external factors.

DATA PRIVACY, DATA RIGHTS AND DATA USE

As connected products collect large amounts of data, the parties need to understand the different types of data that will be collected, for example, safety critical data (e.g., crash event data), non-safety critical data (e.g., consumer preferences) or both (geolocation data) and the purposes for which the data is collected (product performance, product improvement, including through machine learning, and customer preferences and marketing). There may be instances where government compels a business to collect specific data, such as event data records. Other data may be helpful in maintaining and improving the product. The interests of the parties in the data may vary and the rights and uses of the data will need to be negotiated.

In the case of consumer products a threshold concern will be the need to gain consumer consent for the collection and use of the data, including ensuring consent is obtained as ownership of the connected products that are readily transferable changes. The contractual terms around use of data will be driven by the consent obtained. The contract will need to specify which party is responsible for obtaining consumer consents, and which party is responsible for maintaining compliance with changing privacy laws that impact the personal data collected (both directly and indirectly) through connected products.

REGULATORY COMPLIANCE AND CONSUMER SAFETY

With connected products, particularly those providing services or functionality that if incorrectly performed or misused may raise consumer safety issues, the parties will need to consider the appropriate allocation of risk in light of heightened product liability concerns and other contractual terms. Regulated companies of consumer products are accustomed to passing through to traditional component suppliers obligations necessary for regulatory compliance and allocating the risk associated with consumer safety. Technology companies may be unfamiliar with both the contractual requirements necessary for the customer's regulatory compliance and assuming risks associated with personal injury. The parties will need to work to bridge those gaps.

Contracting for connected product technologies is becoming more challenging with the growth of safety and cybersecurity risks, the vast increase in data collection, the tremendous complexities of interconnected systems and evolving laws and regulations. Customers can successfully contract for connected product technologies through an

understanding of these challenges and through the use of flexible contracting requirements that allow for constant adaptation of the technology, business requirements and compliance considerations in this area.

Endnotes

[1] https://www.gartner.com/newsroom/id/3598917

[2] In 2015, several automotive manufacturers were sued for manufacturing cars that transmitted car and owner data via unsecured transmissions. https://epic.org/amicus/cahen/Cahen-First-Amended-Complaint.pdf. The plaintiffs alleged that poor cybersecurity in the vehicle's wireless technology put drivers at risk of having their cars hacked and a hacker taking "control" of the cars. https://epic.org/amicus/cahen/Cahen-First-Amended-Complaint.pdf ¶ 33.

[3] CareFirst, Inc. v. Chantal Attias, No. 17-641.

[4] https://www.congress.gov/bill/115th-congress/house-bill/3388/text

[5] https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen

[6] https://www.ftc.gov/news-events/blogs/business-blog/2017/02/what-vizio-was-doing-behind-tv-screen