Updates
December 05, 2018

Managing the Privacy and Data Security Risks of IoT This Holiday Season

As brick-and-mortar retailers seek effective ways of competing with the perceived convenience of online shopping, more and more are turning to the Internet of Things (IoT) to enhance customer engagement, in-store experience, and administrative and personnel efficiencies. As with the adoption of many new technologies, however, IoT use is not without its data privacy and security risks.

What Is IoT and How Is It Relevant to Retail?

For the uninitiated, IoT generally refers to physical devices that connect to the internet and collect, transmit and receive information (sometimes called "smart devices" or "smart technology"). Retailers in the United States and elsewhere have adopted a myriad of IoT technologies, from the use of targeted discounts and Bluetooth beacons that drive customer engagement and enhance the in-store experience, to investment in smart shelves and Radio-Frequency Identification (RFID) chips to manage and control inventory, thus maximizing employee effectiveness.

As a practical example, picture a customer who searches your website for a replacement printer cartridge, has downloaded your app and goes to your store to purchase it. Upon her arrival, she receives a smartphone notification that opens to a map of the store, directs her to the printer cartridge aisle, offers a discount for the brand of cartridge viewed online and provides an up-to-date inventory for the cartridges. As the customer walks towards the printer section, Bluetooth beacons from other aisles send messages regarding other products and sale items she may want to consider. After the customer picks out the right cartridge and removes it from the shelf, the IoT enabled smart shelf notifies your inventory software, while RFID chips on the remaining cartridges help you monitor their shelf life.

IoT Data Privacy Risks

One of the obvious purposes of implementing IoT technology is to increase the bottom line. However, retailers should be mindful of the data privacy regulatory issues associated with retailers' implementation and management of IoT technology. Does the customer know that the retailer is tracking her internet use while on the retailer's website, her location in the store and her purchases? Does she know what information the retailer's app is collecting? What is the retailer doing with that information? Will it be shared externally with other vendors or otherwise monetized downstream? Will it be used for any other purpose? Will it be retained and, if so, for how long? What happens in the event of a data breach? These are some of the questions retailers should

consider in deciding whether to take advantage of the benefits and power of the interconnected world offered by IoT.

The data privacy risks inherent in the three modalities of website, app and in-store IoT experiences are interrelated. To avoid running afoul of data privacy and security regulations, including the EU's General Data Protection Regulation, the recently enacted but not yet effective California Consumer Privacy Act and California Senate Bill No. 327 (requiring reasonable security features on "connected devices"), among others, retailers should: (1) have a comprehensive understanding of how they are collecting, using, tracking, sharing and storing customer data, *including* data collected by IoT devices; (2) consider how data privacy regulations may be implicated by the retailers' customer data practices; and (3) if applicable, provide customers with full and clear notice of such practices in, for example, the retailer's privacy policies and terms of service, which should be easily accessible and comprehendible (e.g., minimize legalese). In short, prior to rolling out an IoT strategy, it is critical that retailers carefully and thoroughly review their customer data policies and terms to ensure compliance with applicable privacy regulations, and to guard against consumer complaints and potential lawsuits.

IoT Data Security Risks

The adoption of IoT technologies carries the potential for increased data security vulnerabilities and risks due to: (1) the frequent reliance on third-party software and devices, some of which may be relatively new and insufficiently "bug" tested; and (2) the creation of additional network access points. Accordingly, retailers who are considering the use of IoT devices should understand the cybersecurity risks associated with such devices (both general risks, as well as device/technology specific), and prepare a mitigation strategy in advance of taking their IoT strategy online.

Preparing a data security risk mitigation strategy relating to IoT is, in general, a process similar to that required for general retailer data security preparedness. The tone should be set from the top of the organization that reflects a commitment to investing adequate resources and support to the effort to protect customers from breach or other leakage. Those with ownership of the information technology and/or security programs should be aware of applicable cybersecurity risks to the retailer's customer data security infrastructure, and ensure that clear, enforced and updated policies that govern the storage and handling of such data are in place.

To mitigate the legal, customer confidence, and other consequences associated with a breach, the retailer should have and exercise a comprehensive cyber incident response plan, which includes the buy-in and participation of stakeholders from across the organization such as legal, IT, risk management, corporate communications and customer service, to name a few. The retailer should also have a plan for complying with breach notification laws, as well as have considered in advance when to involve and, if applicable, who to contact within law enforcement. These preparations and practices are necessary to help ensure that the implementation of IoT does not have more downsides than benefits for retailers.

Conclusion

The use of IoT is an important and valuable tool that can aid brick-and-mortar retailers with enhancing customers' in-store experiences, while reducing administrative and personnel costs and increasing profitability. However, retailers who are planning to or already use IoT technology should be mindful of the evolving privacy and cybersecurity risks associated with IoT-related data collection, use, sharing and retention. To assist with preparing for and responding to the data privacy and security risks associated with IoT technology, and to minimize the impact of such risks while maximizing the potential rewards, retailers should consider early involvement by legal counsel in any IoT strategy.

Authors

Debra R. Bernard

Of Counsel
DBernard@perkinscoie.com 312.324.8559

Explore more in

Retail & Consumer Products

Related insights

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights

Update

FDA Food Import and Export Updates for Industry