wiley

NEWSLETTER

New Issues Raised By Internet Of Things Payments

January 2019

Privacy in Focus®

The internet of things is a promising platform for all sorts of consumer services — and one coming fast is IoT payments. This holiday season, for example, Amazon reported huge sales of internet-connected home devices and a jump in consumers ordering products using those same kinds of devices. The development of IoT payments will bring great benefits to consumers, but just as with the move to mobile over the last decade, companies need to carefully think through implementation. How do existing laws apply to transactions executed using a wide range of connected devices? How should companies proactively address the attendant risks?

What Are IoT Payments?

IoT payments come in a range of forms. A person can order a product online through a smart home assistant, or set up a refrigerator to manage and order groceries. A consumer can use a wearable device like a watch to make an in-store contactless payment or even an in-app payment. Connected cars can search for nearby gas stations and pay automatically. These kinds of use cases will only grow as consumers increasingly rely on and become more comfortable with IoT devices — just as consumers shifted their habits from desktop computers to mobile devices over the last decade.

What New Issues Do They Raise?

Plenty of consumer laws and regulations apply to payments, and a key challenge is figuring out how they fit when payments are integrated into IoT devices — particularly given that these devices

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Practice Areas

Connected & Autonomous Vehicles
Internet of Things
Privacy, Cyber & Data Governance
Telecom, Media & Technology

may have small or no screens, or rely on voice interaction to operate. Here are a few issues to watch:

Getting Consent for Transactions

In the world of payments, eliminating user friction is an important goal. One of the advantages of IoT payments is that consumers don't need to re-enter payment credentials for every purchase. At the same time, consumers must provide some sort of authorization for the transaction. For example, a refrigerator may be smart enough to order groceries on its own, but its owner won't want it to get ahead of what he or she authorized. And both the fridge operator and owner may be wary that kids in the household will use the connected functionality to stock the fridge with their favorite treats.

The Federal Trade Commission has brought multiple actions against companies that it alleged had failed to take sufficient steps to gain authorization for transactions, under Section 5 of the FTC Act. In resolving those actions, the FTC has generally permitted companies to obtain advance consent for transactions, while requiring that the scope of that consent be clearly and conspicuously disclosed to consumers in connection with obtaining authorization. In the context of cases in which kids were alleged to have made unauthorized purchases, it has also required that the disclosures and consent mechanism be reasonably calculated to ensure that the person providing consent is the account holder. So, for example, in obtaining consent for future grocery purchases, a company will want to look closely at how it informs consumers what they're authorizing when they set up instructions for future orders. And companies will want to think through whether kids or other unauthorized individuals are likely to incur unauthorized charges on IoT devices — particularly those not under normal parental supervision — and what kinds of reasonable measures to take to verify an adult is behind the purchases.

For recurring purchases using IoT devices, an additional issue is compliance with the Restore Online Shoppers' Confidence Act, which prohibits companies from charging consumers for goods or services over the internet through a negative option feature (e.g., automatic renewal), without (1) clearly and conspicuously disclosing all material terms of the transaction before obtaining billing information; (2) obtaining the consumer's express informed consent before charging the consumer; and (3) providing "simple mechanisms" for a consumer to stop recurring charges. The FTC has not yet applied ROSCA in the IoT context, but the FTC has brought an action against an app developer for failing to disclose, before collecting billing information, the "simple mechanism" for stopping recurring charges, alleging that linking to a terms of service containing this information was insufficient. Communicating that kind of information can be challenging depending on a device's user interfaces.

Clarifying Payment Mechanisms and Dispute Rights

Different payment options — credit, debit and prepaid — have different statutory and regulatory protections if something goes wrong. (Prepaid account regulations will change when the CFPB's final prepaid rule goes into effect in early 2019). For example, liability for unauthorized use of a credit card is capped at $50 under Regulation Z, implementing the Truth in Lending Act. If a payment is linked to a debit card, however, a consumer must report the transaction within 2 business days to cap liability at $50, and could face greater

costs if reporting is further delayed, under Regulation E (implementing the Electronic Fund Transfer Act).

In the context of mobile payments, the FTC has flagged that consumers could potentially be confused about which funding source a consumer is using to make a payment and what liability protections they have. The FTC has not yet brought any enforcement actions based on this kind of confusion, which would require proof that consumers had been misled about a material fact of a transaction. But IoT payments may provide further challenges in this area. In a mobile payment, a consumer may see a screen that shows the card or account being used, while IoT payments may not involve a screen at all. If an IoT account — like many mobile accounts — is linked to multiple funding options, companies will want to think carefully about how to communicate any choices or defaults to consumers.

Communicating Privacy Choices

Both the federal government and states are actively evaluating whether and how to give consumers more control over use and disclosure of their personal data, including data that is collected in the course of payment transactions. This is a potential challenge for companies involved in IoT payments. In an online or mobile transaction, consumers can review privacy policies or disclosures, and make decisions about data use, on the same device — but that option may not be realistic with an IoT device.

In the case of financial or transaction data, there are guideposts in existing law. Under Section 5 of the FTC Act and similar state laws, privacy representations must be nondeceptive. The FTC has brought many cases where consumers thought they were keeping some information private, but in fact the data was shared — including one recent case involving transaction history on a mobile app. And a company involved in IoT payments will want to assess whether it qualifies as a "financial institution" under the Gramm-Leach-Bliley Act and is subject to the FTC's privacy rule. The FTC recently alleged, for example, that the operator of a peer-to-peer payment application qualified as a financial institution and that it violated the privacy rule by failing to provide a clear and conspicuous initial privacy notice, as required by the rule.

Over the next year, Congress, states and agencies like the FTC, the National Institute of Standards and Technology and National Telecommunications and Information Administration may all weigh in with further regulations or guidelines on consumer privacy that could impact the design and implementation of privacy choices in IoT transactions.

Security

Cybersecurity remains a top concern for IoT market participants, and payments add another layer of complexity. For one, using payment card information triggers the payment card industry's data security standard, or PCI DSS, requiring certain measures to protect cardholder data, including securing the entire cardholder data environment. Depending on the network architecture, that can include other internet-linked devices. Companies that fail to comply with PCI DSS requirements can face significant fines. Additionally, the risk of a breach includes payment card compromise or fraud that can result in even more financial exposure.

The FTC and, increasingly, states have also brought actions based on breaches — or even just vulnerabilities. For example, the New York attorney general recently announced a settlement with five companies whose mobile apps, it alleged, failed to properly authenticate SSL/TLS certificates, leaving them vulnerable to a so-called "man-in-the-middle" attack to obtain consumer credit card information. And the attorney general specifically noted that the office itself had tested the mobile apps to uncover security vulnerabilities, rather than responding to a complaint about stolen data. Industry participants have focused on cybersecurity issues in IoT in recent years, and will need to take account of device payment capabilities as well.

Conclusion

All signs point to payments growing in the IoT space in 2019 and beyond — a development that should bring benefits for consumers. As the numbers of IoT devices grow and their functionality expands into payments, industry participants will confront issues like the ones noted above in building out their products and services. Now is the time for companies to think through compliance as they scale up — to safeguard their own interests and benefit their customers.

This article was first published by Law360 on January 4, 2019 and is available here.