RFID JOURNAL

Give Customers Control of Their Data or Risk Incurring Their Wrath

EXPERT VIEWS

BY JIM KASKADE

As product managers rush to deliver a new multichannel experience, customers will need increased control of their personal data—even more so than in the context of traditional mobile-app surfing, shopping and the like.

TAGS ▸ INTERNET OF THINGS | PRIVACY | RETAIL

Nov 13, 2017 Figures vary, but analysts agree that Internet of Things (IoT) devices will proliferate exponentially during the coming years, and IoT-oriented products and services will likewise explode. As product managers rush to deliver a new multichannel experience that potentially adds dozens of "things" to the usual Web and mobile access points, they must understand this very important difference in the IoT consumer journey: customers will need increased control of their personal data—even more so than in the context of traditional mobile-app surfing, shopping and the like—thanks to the convergence of the following five forces:

Security Threats Are More Personal—Has Your Webcam Been Compromised?

Although identity theft, phishing attacks, spoofing and other tactics designed to pilfer personally identifiable information (PII) have seemingly been around as long as the Internet itself, IoT breaches have resulted in unprecedented levels of invasiveness. You should check to see if your webcam has been hacked. Each baby-monitor hack, smart TV spying incident and teddy bear account heist is making end users squeamish. Are their devices secure, and can they trust that their personal information is safe? Users will demand control of their digital identities and associated personal information in response to the increased number of identity breaches. Control over what data is in a company's hands obviously won't eliminate cybercrime, but it may provide a little peace of mind.

The IoT Is Driving Changes in Customer Relationship Dynamics

As connected refrigerators begin to inform people that they need to restock the milk, and as personalized discounts for products start showing up on public devices in far-flung places, customers may get that "Big-Brother" feeling. They may want more transparency around how their data is being used to ultimately serve up a coupon for salsa when they reach for tortilla chips at a supermarket. If you own an Amazon Echo, you probably know that the device not only listens to but records a lot of what you say. Behind that dark tower, Amazon is storing a vast trove of recordings inside your home. Your voice—your friends' voices—are all being analyzed. Well, now a consumer can listen to every command they've ever given their Echo with the Alexa app on their smartphone or tablet. If it creeps you out that your requests, and other things you may have said, have been stored in a database, you can delete them.

Consumers Are Starting to Exercise Their Power

Consumers are fighting back against uninvited communication via Web or mobile device more and more with each passing year, as is evidenced by the rise in ad blocking. Data shows that 78 percent of consumers are much more likely to engage deeply with a company when they have a say in which channels those organizations use to communicate with them (e.g., text, email, etc.). Moreover, 71 percent are more open to unhanding PII when they have assurances that their personal details aren't shared with third parties, while 62 percent will release their data if they are confident they aren't being used as a conduit for marketing to friends in their network. Again, the IoT will only accelerate this proclivity, given its potential for new depths in personalization.

Regulators Will Mandate This Change

The European Union (EU)'s General Data Protection Regulation (GDPR), which will go into effect next May, will potentially penalize companies €20 million or 4 percent of global revenue if they fail to follow the 99 articles, including requirements such as obtaining explicit consent for specific customer communications purposes, or granting customers the ability to review and revoke permissions at any time, among many other requirements. Since GDPR applies to any company serving EU residents, many organizations around the world will have to bake consumer empowerment into the design of their IoT offerings—or pay a steep price in cash and reputation.

Technology Is Evolving to Give Consumers Control

Inspired in part by GDPR, fine-grained consents, permissions and consumer controls will be required in all enterprise and mobile apps deployed in the EU. Customers will soon expect to know which items they have agreed to share (e.g., email address, mailing address, birthday, etc.) and for what purpose. Any desired changes at the surface may be as easy as checking and unchecking boxes. However, enterprises will need to take that consent data and propagate it to all downstream information systems. The IoT will only intensify this need with its vast number of customer touchpoints.

Brands will be tempted to have a ubiquitous presence around end users, given the IoT's promise of deeper insights and fine-targeted customer relations. Customers having control of their data will keep organizations on the right side of the line separating customization from creepy.

Jim Kaskade is the CEO of Janrain, where he leads the company's vision, strategy and worldwide operations. He is a seasoned entrepreneur with more than 31 years of experience in complex enterprise technology, including 10 years as a startup CEO leading companies from their founding to acquisition. He has built multiple technology businesses in cloud computing, enterprise software, software-as-a-service (SaaS), online and mobile digital media, online and mobile advertising and semiconductors. Prior to Janrain, Jim was the VP and general manager of digital applications at Computer Sciences Corp., where he led the formation of its largest line of commercial business. You can contact him via Twitter or LinkedIn.