Deloitte.

SkiftX CREATIVE STUDIO

How security, privacy, and trust can help travel brands offer a more human experience

Utilizing data is an integral part of how travel brands can offer a better customer experience. But securing this data, protecting customer privacy, and building trust can be equally essential to supporting both the human experience and the bottom line.

To deliver the richer, more fulfilling experiences that travelers crave, travel brands depend on a growing cache of customer data. More data can mean more opportunities to deliver an elevated human experience, personalized to each traveler's needs and wants. But many brands are opaque about just what data they are collecting, and customers often don't have any way to know how it may be used, how well it is secured, and what, if any, control they have over their personal information. Hence, the trust that travelers place in the industry is at risk, which ultimately could impact their travel choices.

"This is a challenge for the hospitality industry," said Linda Walsh, Cyber Risk managing director at Deloitte & Touche LLP. "Guests desire more targeted and relevant experiences, but not at the risk of losing their privacy. Companies must establish security and trust as basic pillars of the human experience."

On the one hand, 61 percent of Americans say they'll share more data with a company to get customized communications from them, according to research from Smart Communications. On the other hand, the 2019 Edelman Trust Barometer Special Report found that only 34 percent of consumers trust most of the brands they use or purchase from. The challenge: Brands are often asking customers to take a leap of faith without providing the necessary assurances.

"At the heart of the issue for many customers is that they don't know in advance how their data will be used to market to them, and opting-out is frequently not an easy option," said Dorsey McGlone, managing director of Deloitte Consulting LLP's Customer & Marketing practice. Security is also a major concern. SmarterHQ reports that while 72 percent of consumers are highly likely to buy from brands who personalize their messages, 86 percent are also concerned about data privacy. With the Federal Trade Commission reporting consumers losing nearly $1.48 billion to fraud in 2018, worries about security are highly valid.

A key element of alleviating those worries is looking at the entire customer experience through a human lens and providing transparency and clarity on how the data will be used, stored, and secured. That way, travel brands can balance seemingly opposing customer needs: "know me well" and "protect my privacy."

Balancing personalization and trust

Travel brands have a lot of historical data on each customer which supports critical personalization initiatives. This data often includes sensitive information, such as credit card details, locations and dates of travel, and personal preferences, that makes these customer profiles valuable to marketers but also more attractive targets for criminals.

Recent Deloitte research shows that customers are aware of—and are

comfortable with—brands collecting data on them. For example, 75 percent of those surveyed expect brands to know why they purchased a product, and 52 percent expect the brand to know how satisfied they are with it. At the same time, 35 percent say they do not want brands to track their browsing history for similar products. The implications are clear: most customers will allow brands to collect data, but only if the customer feels it is relevant to their relationship with the brand. They also want to have a choice in what data is captured and how it is used.

Achieving both personalization and trust can come down to two essential factors: transparency and control. "A user may have already given the brand permission to build a profile but may not be aware of all the additional data being collected," said Vikram Kunchala, Cyber Risk principal at Deloitte & Touche LLP. "This additional data collection should be made clear, and there should be a simple, one-click way to delete any and all data."

McGlone agrees and says that providing that clarity shouldn't take a five-page agreement, but just a few bullet points in a simple communication. She suggests that once brands explain what they intend to collect, they should "give users choices to customize what is permissible and make it easy for them to change their minds so they feel in control."

Securing the entire value chain

"When you're booking travel, there are a host of third-party companies behind the travel vendor that the customer never sees," Kunchala said. "Hotels, for example, operate heavily on a franchise basis. But franchisees may not have the resources or the appetite to implement the appropriate controls to meet the franchisor's data security and privacy standards and policies."

Having security lapses in the franchisee's systems can put the franchisor's brand reputation at risk. It can therefore be critical to ensure that all access points across the entire value chain (made up of partners and service providers with access to the data) are also secure. Kunchala gave an example of one way that Deloitte has helped brands with this issue: by developing a package of security services that is typically more cost-effective than sourcing individual solutions. Additionally, travel brands can work to conduct security assessments more effectively. "Like a credit rating, there are solutions to provide a 'cyber hygiene' rating," Kunchala said. "If that rating falls below a certain level, the brand can mandate changes for their franchisees."

Another way to help secure the value chain could be to reduce the attack surface by centralizing data collection, storage, and access. "By using cloud technology, for example, the franchisee does not store the data on site and centralizes storage," Kunchala said. "That way, if a chain has 6,000 hotels, there won't be 6,000 access points to the data, limiting vulnerability."

But travel brands should also be prepared with technical and communication responses in case of a breach. "The longer you wait, the worse the news gets," Kunchala said. "How simply a customer can access resources in those situations is a differentiator for cultivating loyalty."

Customer-centric means privacy-centric

An increasing number of customers will expect to be in control of their data. Growing concerns about privacy, similar to those that led to the General Data Protection Regulation (GDPR) in the European Union, are beginning to take off in the U.S. The new California Consumer Privacy Act, for example, states that consumers must consent to data capture, have the right to ask for all of the data a company has on them, and have the data deleted if they so desire. Other states are launching similar initiatives. "Implementing these regulations pose a challenge for companies. Not only will it take time and investment to build the right infrastructure, but customers will ultimately be in control of their privacy demands. If a customer believes their data will be misused or even if they simply don't want to share it, companies will be legally required to capitulate to the customer," Walsh said.

But security is about more than meeting regulations. Companies should provide greater transparency into their practices. "That transparency means allowing users to share only what they choose. It also involves being open about what opting-out really means," McGlone said. "Organizations will no longer be able to hide behind 'legalese.' Customers should clearly understand what is and isn't covered by that agreement, and what they gain by sharing their personal information."

Transparency starts at the top

"From the standpoint of delivering a more human experience, many companies are being rewarded for being transparent," said Ashley Reichheld, principal at Deloitte Consulting LLP. "One study showed that 94 percent of consumers agree that transparency is the number one factor in brand loyalty, and three-quarters of them would pay more for those brands."

But making transparency a part of a company's DNA often requires commitment and buy-in at every level of the organization, including the C-suite leaders. "This priority needs to be agreed from the top down," Reichheld said. "There must be guiding principles, a data strategy, and a dedication to being customer and privacy-centric."

While organizations need customer data to improve their performance, customers want to be confident that their data is being collected and used for the right reasons. They also should know just what data is being captured, how it is being used, and if it is being handled securely. Initiating transparent and secure data handling practices is a business imperative as regulations and pressure from travelers drives the industry to be more responsible. Starting now can give organizations time to define processes and policies and earn their customers' trust.

This content was created collaboratively by Deloitte and Skift's branded content studio, SkiftX.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional adviser.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, "Deloitte" means Deloitte & Touche LLP, which provides audit, assurance, and risk, and financial advisory services; and Deloitte Consulting LLP, which provides strategy, operations, technology, systems, outsourcing, and human capital consulting services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of Deloitte's legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2020 Deloitte Development LLC. All rights reserved.