PROTECTING PRIVACY

AS **DATA MINING** BECOMES MORE SOPHISTICATED, HOW DO CONSUMERS FEEL ABOUT **USE OF THEIR PERSONAL INFORMATION**? > By Brenda Porter-Rockwell

Retailers are embracing an ever-increasing array of technologies to improve loyalty programs that maximize the customer experience. But the data collection that comes along with these programs has raised concerns about individual privacy.

As information-gathering techniques become more sophisticated (think in-store facial recognition software), retailers are pushing the boundaries, to the point where programs are becoming more invasive and data security and privacy are of increasing concern.

"Our customers tell us, 'We want to be rewarded; we want to be recognized; we want to earn those points.' But we have to be very, very careful about how we do that. Otherwise, we run the risk of crossing over from the cool to the creepy continuum very quickly," says Fatemeh Khatibloo, senior analyst at research firm Forrester, during a webinar titled, "Big Data: Gold Rush or Illusion?"

But if done right, intelligent and respectful approaches to data gathering can offer greater insights to customer needs and reignite loyalty to a particular retailer or brand.

ASK, DON'T TELL

In "Retailer Loyalty Programs–US" released by Mintel in August 2013, research reaffirmed continued customer interest in loyalty programs. However, the report's authors reminded retailers that so-called "loyalty" rests on thin ice, which could easily crack or even break should they overreach in their quest to know their shoppers intimately.

Mintel found that consumer concerns about privacy are growing as consumers weigh whether to sign up for a loyalty program. About 32 percent of Americans said the privacy of their personal information is an important attribute of a loyalty program.

In response to customer concerns about loyalty program data, retailers have doubled down on their commitment to keep the data safe and secure, says analyst Bill Bishop, chief architect of Barrington, Ill.-based Brick Meets Click.

According to recent data gleaned from Brick Meets Click's study of the use of big data in retailing, "How the Game is Changing: Big Data in Retail," retailers are taking action to ensure that commitment is kept before government regulations force their hand.

In Europe, regulators are currently tackling the issue of protecting citizens' personal data—any information a citizen didn't willingly offer up. The general data protection regulation aims to apply certain measures to foreign companies who collect and mine the personal data of EU citizens. Violations could result in hefty fines. Big companies and national officials are still hashing out the details. To date there is no such monitoring by the U.S. federal government, but consumers are on edge due to recent data security breaches at Target and Nieman Marcus.

As a retailer, it's imperative to offer an opt-in/opt-out program, says Deena Amato, retail analyst for the Aberdeen Group.

"Shoppers should also have access to a retailer's privacy policy at the time they sign up for a program, or the chance to read it later via e-mail or direct mail. Retailers that don't offer this option run the risk of not only losing a loyalty program member, but a loyal shopper, to a competitor that is on the ball," she explains.

HORSE TRADING?

There's nothing original about exchanging personal information for the benefit of getting a good deal at just the right time. It's the basis of loyalty programs. Montreal-based loyalty management company Aimia's research shows that customers are willing to share information as long as there is a "clear and explicit value exchange," says Stephanie Swain, Aimia VP of retail.

"The digitization of everyday life means that consumers are now having to release more and more of their personal data to more and more suppliers, risking the overuse and even potentially misuse of this data," Swain says.

Bishop says he is skeptical about this kind of "horse trading," calling it a slippery slope.

"There's a lot of interest in making this tradeoff, but not much appreciation for what the downside of sharing could be," Bishop says. "I think the enthusiasm will subside somewhat as the problems become better known."

But Swain thinks the give-and-take will go on as long as it's done carefully and with respect.

"We will find that only companies that treat their customers' data with respect and reward them for its use will continue to enjoy access to it," she says. Swain recommends that new technology be used "to do things for and with consumers, not to them. It is this customer-centric approach that will ensure we are using all of the new sources of customer data and new channels to build real long-term relationships, not just short-term deal-based noise."

GENERATION GAP

There is one caveat around this give-and-take model. The rules for sharing appear to differ among the generations.

"Age is strongly related to the type of loyalty program to which people belong. While supermarket loyalty program memberships are likely to be cited by individuals aged 35 and older, 18- to 34-year-olds tend to enroll in foodservice, mass merchandiser, online retailer, convenience stores or fuel or dollar discount store programs. Club store memberships are also popular among younger age groups," says Ika Erwina, Mintel's retail, apparel and technology analyst. "Given millennials' strong propensity toward environmental and social responsibility, retailers may need to incorporate social issues into the program to improve awareness and participation."

"There's a lot of interest in making this tradeoff, but not much appreciation for what the downside of sharing could be. I think the enthusiasm will subside somewhat as the problems become better known."

— BILL BISHOP, *Click Meets Brick*

"Shoppers should also have access to a retailer's privacy policy at the time they sign up for a program, or the chance to read it later via e-mail or direct mail."

—DEENA AMATO, *Aberdeen Group*

Interestingly, Aimia's research found that millennials are less concerned about data privacy than other cohorts. Of all of the named marketing channels in the survey, loyalty and reward programs were perceived as the most privacy-friendly by millennials, and only 14 percent of millennial loyalty program members said they were concerned about sharing personal information to participate in these programs. About 47 percent of them agree that they're more likely to share personal details with a brand that offers loyalty and reward incentives.

As digital capabilities increase, and as these programs are increasingly shifted from loyalty cards onto smartphones, the potential for invasiveness increases.

Brick Meets Click's survey found that item-level movement data—point-of-sale and data and market basket data—is still recognized most broadly as the type of information that will improve supply-side performance, but tracking in-store shopper behavior and shopper feedback are not far behind.

The loyalty card was once retailers' top choice to capture shopper data. "It tracked everything they needed to know in terms of their preferences, brand loyalty and buying patterns. What it lacked was a way to see *how* they shopped. What were their navigation patterns like? What aisles did they spend the most time in?" Amato says.

This is where smartphones and related apps can add dimension to the data. Using integrated GPS systems, retailers are able to obtain these details and more. In fact, snack food manufacturer Mondelez International is rolling out a pilot program called Smart Shelf in grocery stores.

Utilizing technology from Microsoft's Kinect controller, the goal is to provide targeted promotions to shoppers by scanning and reading their faces. If the shelf's weight sensor signals that they've picked up a given item, it will make recommendations for complementary items.

Along similar lines, UK grocer Tesco is installing cameras that determine how long shoppers look at an in-store ad, while scanning their facial features to determine their gender and approximate age.

Kevin Permenter, analyst at Aberdeen Group, says retailers also are integrating social media into their programs.

"The advent of social shopping will also play a role, as many consumers are not shopping alone. They are taking their friends and family in the dressing room with them, so to speak," Permenter says. "Consumers are utilizing their network of friends and family to influence the buying decision. This is relevant to privacy because there is a growing number of companies that are using the social sphere to monitor buying habits and shopping preferences."

WHAT LIES AHEAD

Forester's Khatibloo says that going forward, retailers will need to be very careful not only about how they gather data, but in how they use it.

"It's all about establishing trust and not hindering it," Khatibloo says.

Swain says she sees a growing divide between what marketers want to do with customer data and what value consumers expect to receive from sharing it. That "could mean a world where data brokers or regulators help consumers seize control of their data, and where marketers are forced to pay a premium to collect it," she says. "Unless there's a better value exchange."

Perceived relevance of customer data, as well as transparency, will be key to fostering an environment where consumers willingly share personal information.

"In this new world where customers are taking more control of their data, they can choose which brands to listen to and which to turn off," Swain says. "Technology needs to be architected differently to respond to this trend by putting the customer experience at the center, giving them control of what channels are used to talk to them and who can access their data."

It's likely that companies will start pushing the boundaries even further, making use of every selfie, every tweet, every pin and more in shoppers' social networks.

Permenter recounted a recent discussion with a large North American fashion retailer that indicated that in the near future it will rely almost primarily on social networks for creating customer profiles.

"This social 'data mining' blurs the line between personalization and data privacy even further," he says. **RL**