BUSINESS

Big Brother at the Mall

The privacy debate moves beyond e-commerce as magic mirrors and beacons log shoppers' data in bricks-and-mortar stores

By John D. McKinnon
April 13, 2019 12:00 am ET

WASHINGTON—The battle to protect consumer data is moving from cyberspace to shopping malls, as Congress scrutinizes how advanced technology increasingly follows shoppers around bricks-and-mortar stores.

Retailers including cosmetics chain Sephora use electronic Bluetooth beacons to detect customers' smartphones as they enter the store, allowing them to ping shoppers with promotions as they browse —and see where they linger.

In the fitting rooms at Rebecca Minkoff apparel stores, shoppers can tap on interactive mirrors to see how a top might match with other garments, with each choice being fed into the shopper's online profile.

Meanwhile, facial-recognition technology is being marketed to retailers as a way to flag people who have previously shoplifted or sought refunds for stolen merchandise. For now, many retailers are apprehensive but use of the technology is starting to make its way into real-world commerce, including retail. Walmart Stores Inc., Lowe's Co s. and Target Stores Inc. say they have tested facial-recognition systems but currently don't use the technology.

Retailers say new technologies are largely aimed at improving the shopping experience, helping old-fashioned stores stay competitive with online merchants. In-store tracking helps alert customers to sale items, for example, and facial recognition can let shoppers breeze through checkout stands by speeding up the payment process.

Stores say they've been forced to adopt high-tech data collection tools like beacons to remain viable as consumers do more shopping online. But in-store beacons haven't been as impactful as hoped, often sending promo messages only to customers who have the store app open, for example. So while there is trepidation, there's also strong interest among retailers in moving to the next stages of technology, particularly facial recognition.

At Rebecca Minkoff stores, customers can tap on mirrors for other sizes or to get suggestions, with their choices logged in their profiles. PHOTO: REBECCA MINKOFF

Privacy advocates, however, say the risks of abuse from in-store tracking of customers are as high as online.

Risk of Abuse

"Technology is rapidly erasing any differences between how precisely people can be tracked online and in a physical space," said Jay Stanley, a senior policy analyst for the American Civil Liberties Union. "So we're going to need all the same protections offline that we do online."

The data-privacy debate in Congress has largely taken aim at online social media and e-commerce companies, but key committee leaders in both the House and Senate are vowing to include bricks-and-mortar retailers in any legislation.

SHARE YOUR THOUGHTS

Should consent be required for facial recognition in stores? What about sensors on shopping carts that detect heart rate or monitors that detect eye movements? Is a sign in the store sufficient? Join the conversation below.

"It is clear to me that we need a strong, national privacy law that provides baseline data protections [and] applies equally to business entities—both online and offline," said Senate Commerce Chairman Roger Wicker, a Republican from Mississippi, at a recent hearing.

Facial-recognition systems are being marketed as a means to monitor customers or employees, said Joseph Jerome, policy counsel at the Center for Democracy and Technology. That raises the

likelihood that unregulated data-sharing cooperatives would emerge among retailers, he said -- as well as accuracy concerns and the risk of unfair blacklisting.

“It has serious impacts for how you go about your life,” he said.

The inclusion of bricks-and-mortar stores in privacy legislation is supported by online companies like Amazon.com Inc., where executives are concerned that internet businesses could be singled out for restrictions. But it’s drawing concern from traditional retailers who worry that their cutting-edge technologies could be banned or disrupted if they are included under the privacy law.

Retailers also fret that uniform privacy rules could limit their ability to use longstanding data-collection techniques such as customer-loyalty programs. A landmark privacy law passed by California last year prohibits discrimination against shoppers who decline to share certain personal information. That could restrict businesses’ use of loyalty programs and leave stores vulnerable to litigation, retail groups say.

SHOPPER SURVEILLANCE

Online retailers have a wealth of data, on customers, including on shopping history, payment and email. Traditional retailers are finding their own high-tech ways to fight back.

- Magic Mirrors—Some retailers including women’s-apparel company Rebecca Minkoff gather data through interactive mirrors and other devices in fitting rooms or on counters.
- Smartphone Tracking—Some retailers use beacons to detect customers’ smartphone apps as they enter stores, allowing them to ping shoppers with promotions as they browse the aisles. Retailers also can get location information from other apps. Shoppers can also be tracked if they sign up for in-store Wi-Fi.
- Facial Recognition—A few big chains have tested facial-recognition software, mainly to identify people previously caught shoplifting. But many retailers remain wary of blowback from shoppers, even as the broader use of facial recognition grows.

“The nondiscrimination clause in California would invite lawyers to sue every store that has a loyalty program,” said Paul Martino, vice president of the National Retail Federation. Many retailers worry that imposing privacy rules designed for the online world could disrupt the customer experience—for example, by requiring cumbersome opt-in.

Retailers are also apprehensive about giving customers so much control over their data that they could simply move it from one business to a rival, Brian Dodge, chief operating officer of the Retail Industry Leaders Association, said in recent testimony to the Senate Commerce Committee.

Some retailers privately fear that Amazon, with its expanding market clout, could buy up their hard-won data on the cheap. Amazon and e-commerce companies, meanwhile, argue that the rules should be uniform for all retailers. One concern for online retailers is that many bricks-and-mortar retailers have been feeding the busy wholesale trade in consumer data for years, but haven't come in for the kind of scrutiny that Facebook and other internet giants have endured in recent months.

"Americans should have consistent experiences and expectations across state lines and industries —regardless of whether they're interacting with a company online or offline," Michael Beckerman, president of the Internet Association, said at the Senate hearing. Internet Association members include Amazon, Alphabet Inc. 's Google unit, Facebook Inc., eBay Inc., Uber Technologies Inc., Airbnb Inc. and others.

Common in-store tools such as cameras, Bluetooth monitors and other types of beacons scattered around stores can be used for relatively straightforward purposes—for example to generate traffic counts without identifying individual customers. But some used in conjunction with a smartphone app or other technologies can identify customers or their accounts individually and even offer to charge them for items they select from shelves, as Amazon has begun to do at its Amazon Go stores.

Courtney Marin, a 22-year-old New Yorker coming out of Sephora's Times Square store in Manhattan, said she doesn't mind that the retailer sends her in-store promos. "Sometimes they have brands there that are having an event," she said. Another customer, Rosy Jerez, 23, said that when she goes to a store she already knows what she wants. "For today I needed a concealer, so in and out, I went for a concealer. But I know people that are so into makeup that that would be something they'll use a lot."

The ACLU's Mr. Stanley said that with tomorrow's technology likely to include in-store sensors to detect shoppers' mood, eye movements and heart rate, the need for privacy protections is getting more urgent. "As the sensors get better and artificial intelligence gets smarter, the limits of information that can be collected are the limits of the human imagination," he said.

A Sensitive Issue

An emerging industry of companies sell facial-recognition systems, including Ayonix Face Technologies Inc. of Richmond, Va. The company declined to identify clients, but said it had systems in place at several stores.

"We are monitoring return visits of people that are trying to scam the store," said Mike Broggie, Ayonix's chief executive officer.

The issue is a sensitive one for companies. When the ACLU surveyed 20 of the country's largest retailers last year to determine if they use facial recognition, all except two declined to answer. Several said the information was proprietary or raised competitive concerns. Of the two that responded, a grocery chain said it wasn't using it and Lowe's told the ACLU it might use the technology to prevent shoplifting. Lowe's told The Wall Street Journal it has since decided against using the technology after testing it in three stores.

A spokeswoman for Target said the company tested facial recognition last summer as a way to deter theft and fraud in a small number of stores but isn't using it now. "We'll continue to test and learn from new technologies that have the potential to keep our guests and team members safe," she said.

A Walmart spokesman said there was "a brief facial recognition test a few years ago in a handful of stores for loss prevention, but that was ended." He said the company was still "actively exploring how the technology could be used to benefit customers."

One reason for retailers' reluctance is the potential for blowback from customers. Another is the concern that facial-recognition software might make mistakes in identifying people.

For privacy advocates, another set of concerns revolves around how the data is used. Would one incident of teenage shoplifting lead to someone being barred from stores for life? Could merchants share data? Studies also show that facial recognition is less accurate for people of color; what happens in cases of mistaken identity?

A federal Commerce Department effort to craft voluntary standards for the use of facial recognition fell apart in 2015 as big companies and trade associations resisted agreement on any scenarios where facial recognition could only be used with consent from people subjected to it.

A flurry of privacy bills—including one by Sens. Roy Blunt (R., Mo.) and Brian Schatz (D., Hawaii) that would bar commercial users of facial recognition from tracking consumers without their consent—have been introduced in anticipation that the Senate will eventually consider a broad privacy bill.

"We need guardrails to ensure that, as this technology continues to develop, it is implemented responsibly," Mr. Blunt said.

Ms. Jerez, the Sephora shopper, was skeptical about the prospect of facial recognition being used in retail stores. "I have facial recognition for my iPhone but it makes more sense because it's something personally for me, you know? But if a store is using my face, what else are they going to use it for? You don't know."

—Laine Higgins in New York contributed to this article.

Write to John McKinnon at john.mckinnon@wsj.com

Appeared in the April 13, 2019, print edition.