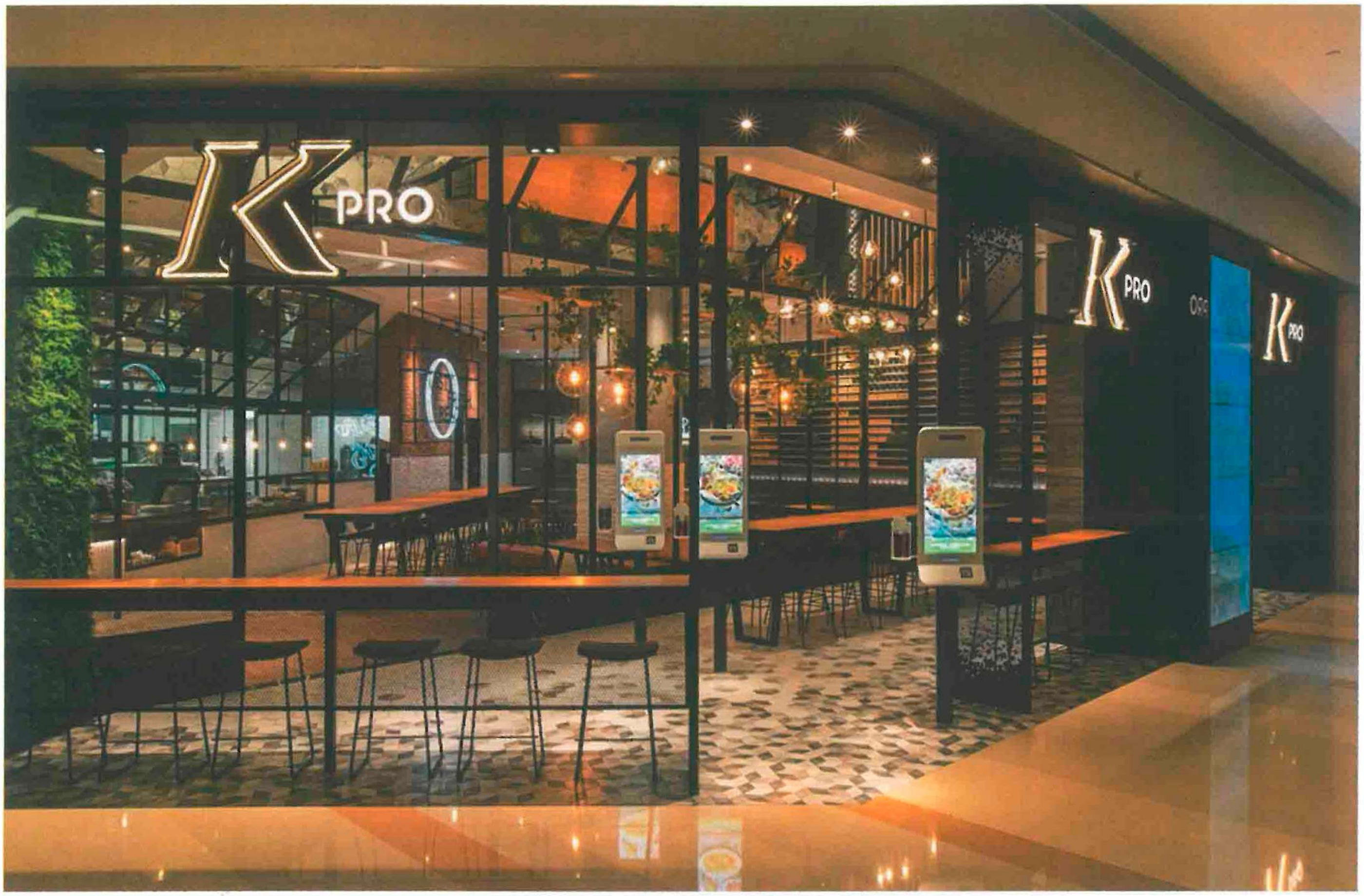
Face Value

Previously the realm of science fiction, facial recognition technology today is science fact



by LEN LEWIS

Imagine a customer strolling through a store when their phone rings and a cheery voice on the other end says, "Hi, Susan. We just got more of those T-shirts you liked in new colors. Come over and check them out."

Or, they're walking down the street in front of a store when they're accosted by police who tell them, "Sir, you've been identified as a shoplifter. Please come with us."

Welcome to what could become the new world order, where facial recognition replaces the chip in credit cards, where likes and dislikes are analyzed by complex biometric algorithms, where individualized pricing could be the norm — and where the system could go wrong, identifying even Mother Teresa as part of a vast criminal conspiracy.

'POTENTIAL FOR MISUSE'

To some futurists and techno-geeks, facial recognition is the dawning of a new age — albeit an early dawn — in customer analytics, personalized advertising marketing and an enhanced shopper experience.

Despite its technological cachet, facial recognition has a deep dark side. Personal privacy — already under assault — could become a myth with the ability to track people as they walk down the street. In legal terms, reading people's faces without their permission could conceivably constitute an invasion of privacy and result in lawsuits ranging from simple harassment to constitutional issues.

But what makes facial recognition the Wild West is that it is virtually unregulated. Best practices have been developed but are merely guidelines without the rule of law. Moreover, hacking and identity theft could become even more pervasive since account numbers and passwords can be changed but faces can't.

In 2015, the federal General Accounting Office issued a 54-page report on the commercial uses of facial recognition technology and the inherent privacy issues. The agency made no specific recommendations, suggesting that Congress consider strengthening the consumer privacy framework to reflect changes in technology and the marketplace. The report was sent to the Department of Commerce, Federal Trade Commission and appropriate congressional committees for review but little action has taken place since.

The National Retail Federation has not taken a position on facial recognition technology. But NRF has argued for years that regulation of technology should focus on any abuses rather than banning it outright. NRF has also opposed restrictions on new technology that stand in the way of innovation that can help retailers better serve their customers.

"This is a very powerful technology, and it's not to say there aren't good uses for this tool," says Jay Stanley, senior policy analyst with the American Civil Liberties Union. "But there's a lot of potential for misuse in monitoring and tracking individuals as they go about their daily lives.

"The first rule has to be transparency and letting people know it's being used," Stanley says. "If stores don't think customers will mind, then tell them. Why keep it a secret? If they do mind and you don't tell them, you're getting into an area that may be unethical."

ENHANCING LOYALTY PROGRAMS

While adoption of facial recognition software will be a long road, some interesting and relevant tests are taking place.

Last year, California-based fast food chain CaliBurger piloted an artificial intelligence-enabled self-ordering kiosk that uses NEC's NeoFace software to identify customers and access their loyalty accounts and past order preferences. The system is expected to be modified later this year to enable customers to pay for orders using their faces.

"Face-based loyalty significantly reduces the friction associated with loyalty program registration and use," Cali Group Chairman and CEO John Miller says. "Further, it enables a restaurant chain like CaliBurger to provide a customized, one-on-one interactive experience at the ordering kiosk."

In 2014, Facebook was one of the early adopters of facial verification in the digital world with DeepFace, a program that recognizes when two images portray the same face. The system also includes a security feature that lets users know when someone else has uploaded a picture of them as a profile picture, intended to prevent people from impersonating others.

> In China, Yum Brands is targeting young consumers with KPRO, a pilot store that enables people to pay for their meals by scanning their face at a kiosk.

Amazon's Rekognition program provides highly accurate facial analysis and recognition which also allows a retailer, for example, to track people through a video even when their faces are not visible or when they go in and out of a scene. The system has a wide variety of uses, including cataloging, people counting and public safety. Rekognition is based on the same deep learning technology developed by Amazon's computer vision scientists to analyze billions of images and videos daily, the company said.

The technology is not just for the digital giants. Lolli & Pops, a candy store chain with nearly 50 locations, is rolling out Intel facial recognition technology that identifies customers when they enter the store and ties together data from online customers and its loyalty program.

In China, Yum Brands is targeting young consumers with KPRO, a pilot store that enables people to pay for their meals by scanning their face at a kiosk and entering a telephone number to avoid fraud.

Walmart has also dipped a toe into facial recognition: In 2012, the chain filed an application for a patent on a system that would detect unhappy customers so it could dispatch store employees to quickly solve any problems. Walmart also said it could use facial expressions to analyze changes in purchasing patterns due to dissatisfaction.

On a more conventional level, Walmart also considered using facial recognition to identify suspected shoplifters. The application never got off the ground, according to published reports.

BEST PRACTICES

As enthusiastic as some observers are about the potential of facial recognition, others have misgivings about gathering databases of "faceprints" — one of the last vestiges of anonymity and privacy.

Currently, no federal laws govern the use of facial recognition; given the congressional agenda, it's unlikely to come up any time soon, according to industry observers. Three states — Illinois, Texas and Washington — have enacted laws restricting use of the technology without people's consent. Montana, Connecticut, New Hampshire and Alaska have reportedly considered statutes.

The Illinois law seems to have the most teeth and could be problematic for retailers, according to privacy and cybersecurity law firm Hunton & Williams. Federal judges have declined to dismiss cases brought against Facebook, Google and Shutterfly under the statute.

"Recent judicial interpretations of the Illinois Biometric Information Privacy Act present potential litigation risks for retailers who employ biometric capture technology such as facial recognition, retina scan and fingerprint software," the firm said in a report last October.

"Retailers who use biometric data for security, loss prevention or marketing purposes may also become litigation targets as federal judges decline to narrow the statute's applicability and additional states consider passing copycat statutes."

For the past three years, the Commerce Department's National Telecommunications and Information Administration, which advises the White House on technology privacy issues, has acted as a mediator for privacy advocates and retailers developing best practices for using facial recognition. The recommendations, which would exempt government agencies and law enforcement, are voluntary, however, and some privacy advocates have reportedly criticized the process or even walked away due to the lack of stronger guidelines.

The best practices encourage companies that collect, store or process facial data to take steps including:

Connecting with Ecommerce

Customer engagement remains one of the most important aspects of bricks-and-mortar retailing. Facial recognition is getting the lion's share of technological buzz these days. But many are concerned about privacy issues and customers getting "creeped out" by being followed.

The alternative to following customers electronically is using technology to connect associates with customers. That is the crux of Hello Customer, a new feature in Mad Mobile's Concierge system that alerts associates when specific customers enter a store.

"We don't follow customers through the stores. We want to connect them to associates and work with them to find products that may or may not be in the store," says Mad Mobile President Greg Schmitzer.

The system, now being used by retailers including Talbots and Helzberg Diamonds, lets associates connect with people when they walk in a store. If customers are in the store's database and come within about 100 feet of an associate, the system maps their mobile number and gives the associate profile information and what that customer is most likely in the store to buy.

There's also a check-in process where customers can plug into the retail system. This alerts associates on what has been purchased in the past and enhances the customer's shopping experience, Schmitzer says.

"We're also closing the loop on what's happening in the store by sharing the customer information with ecommerce," he says. "This has been a real blind spot for retailers. They don't know who came in the store and went to the dressing room to try things on but didn't buy. We can now capture that information, then remarket it to customers when they go back to the website."

- Disclose their practices to consumers.
- Consider factors including types of non-facial sensitive data captured and how it would be stored and used.
- Give people the opportunity to control sharing of facial data with unaffiliated third parties.
- Protect data by implementing a program with "reasonable" administrative, technical and physical safeguards.
- Take "reasonable steps" to maintain the integrity of facial data.
- Provide a process for consumers to contact the entity regarding the use of facial data.

"The best practices are intended to provide a flexible and evolving approach to the use of facial recognition technology, designed to keep pace with the dynamic marketplace surrounding these technologies," NTIA said.

However, the ACLU's Stanley says the guidelines don't address legal issues that are likely to crop up.

"This technology is so new, the law hasn't caught up with it yet," Stanley says. "I wouldn't be surprised to see some lawsuits with courts trying to figure out how existing older laws apply to this new technology, which gets to the heart of what it means to be a citizen and our relationship to the government.

"Most people would get a restraining order if they were being followed around 24/7. But now it can be done virtually, and my face is recognized in every store, every aisle I walk down and every item I look at. I'm not sure most Americans would be comfortable with that," he says.

"And if [a store] combines its data with that of other companies, you can get a pretty robust picture of what I'm doing all day. It has the potential to be the human version of license plate readers." **STORES**

Len Lewis is a veteran journalist and author covering the retail industry in the U.S., Canada, Europe and South America.

> "Face-based loyalty significantly reduces the friction associated with loyalty program registration and use."
> **— John Miller, Cali Group**