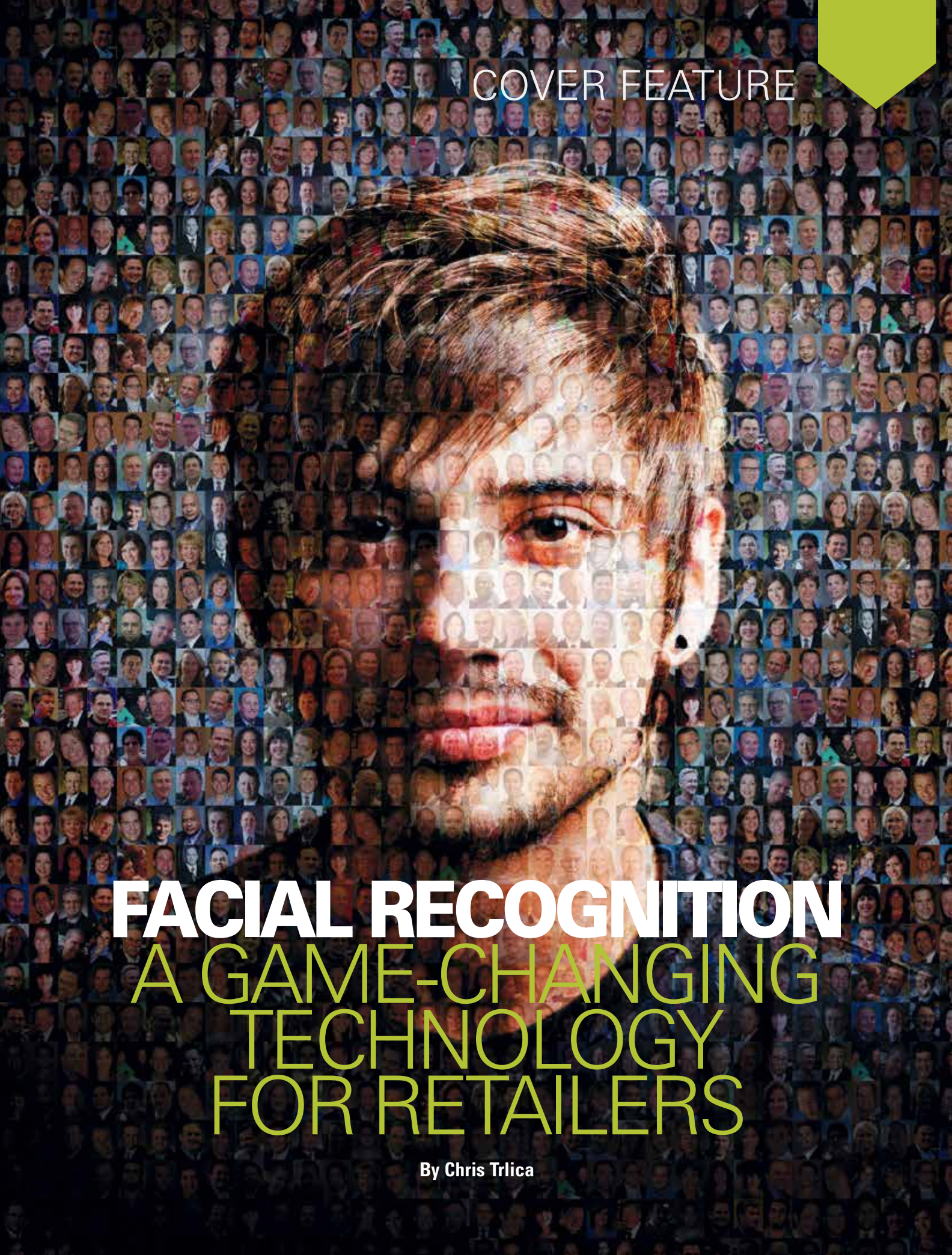


# FACIAL RECOGNITION
## A GAME-CHANGING TECHNOLOGY FOR RETAILERS

By Chris Trlica

*EDITOR'S NOTE: This article is based on the experiences of a well-known retailer who is currently implementing a facial-recognition system. Because of the potential value of this technology to the retail industry as well as the critical issues surrounding its deployment, the executive who leads this initiative approached the magazine to offer his insights on the condition of anonymity. Therefore, the names of the individual and the company have been changed.*

"We're seeing shoplifters—known shoplifters—come up to us and ask permission to buy something." Is this some kind of LP *Twilight Zone*, or the delusions of a loss prevention associate who has spent too many hours watching surveillance video? No, this is everyday life in stores at a leading retailer who has recently deployed a facial-recognition system. And it's just one of the changes that have led the company's head of loss prevention to call facial recognition a game-changing technology.

"We now know within seconds of a person walking in the store if they've previously been caught stealing from us," says Tom Smith, vice president of loss prevention for Store-Mart. "We now know which hours of the day see the most shoplifter activity. We now know that 26 percent of the people we detain, we see again in the brand within one month, on average 13 days later. We never had a way of knowing things like this before. This is stuff that LP associates will salivate over. It's going to be a game changer."

Suppose Johnny Johnson is caught shoplifting at a Store-Mart branch. He's detained, photographed, and given a barring notice. Johnson's photo is entered into Store-Mart's database of known shoplifters, becoming an "enrollee" in the system.

Three weeks later, Johnson walks into Store-Mart again. Within five seconds, the system has captured his image from the store security cameras, compared it against every photo enrolled in Store-Mart's database, found a match, and sent an alert to the in-store LP associate's (LPA) smartphone. The LPA looks at his phone, and Johnson's name, photo, and detention history with Store-Mart pops up. The LPA verifies that the photo in the alert actually matches the person who just walked in. Then the associate approaches and says, "Mr. Johnson, you've previously been given a barring notice from Store-Mart. You're not allowed to be here. Please leave." And Johnson walks back out. So, within a minute or so of walking in, a known shoplifter has left the store, empty-handed.

Facial-recognition systems made the leap from sci-fi to reality around a decade ago, but until the past year or two, they never really worked. Governments were the first adopters, targeting fugitives, terrorists, spies, and other high-priority targets. Retailers have had their eyes on the technology for some time, but until very recently, the price point was simply too high to justify.

Now that the detection algorithms have been refined to enable higher identification accuracy, and solutions providers have lowered prices to a range accessible to retailers, facial-recognition technologies are poised to surge into the retail world. And with megapixel IP cameras now standard, many stores are already equipped with the necessary hardware. All that's left to do is plug them into the system.

## How the System Actually Works

First, a database is populated with the enrollees' facial biometric information. Photos of known shoplifters are analyzed for identifying biometrics, such as length of the nose, distance between the eyes, and that mole beside the left nostril. Biometric profiles consisting of anywhere from tens of thousands to millions of these identifying parameters are compiled for each enrollee and linked to their name, photo, and detention history. Only people who are known to have committed criminal activity in the store are enrolled; average customers aren't ever brought into the equation.

After that, it's just a matter of connecting the database and the detection algorithms to the store's cameras. Joe Rosenkrantz, CEO of FaceFirst, a leading biometrics platform provider, describes the process. "A server in the store detects and tracks faces on every frame of video at 30 frames per second. So, we have a very complex scene of people walking in the front door, and we detect every face on every frame of

**Facial recognition has the potential to change the rules of retail. It could lower shrink, revolutionize in-store marketing, and, ultimately, more efficiently deliver products to consumers, thereby reducing costs for everyone involved—a win-win situation. But as usual, there's a catch. If deployed without careful, deliberate forethought, the technology could easily be abused, either intentionally or by poor planning, with far-reaching consequences.**

video," Rosenkrantz explains. "The system isolates the best representation of each person. We analyze each frame for lighting conditions, pitch, and yaw. We might get 50 pictures of a person, and the system, in near real time, analyzes every one to get the best representation." Each image is scored and the best one has its biometric profile extracted and compared against each profile in the shoplifter database. If no match is found, the image is immediately deleted. If there is a match, an alert message is sent to the designated store associate's smartphone.

Attached to the alert message is the original photo used to enroll the shoplifter in the system, so the store associate can verify that the person who just walked in the store really is the same person as the one in the database. The retailer can choose to set different kinds of alerts for different enrollees. Smith has created several.

Most enrollees generate approach alerts, in which case the LPA addresses the person by name, reminds them that they signed a barring notice, and asks them to leave. If a person has been definitively observed shoplifting, but was not able to be detained, they may be enrolled using a good photo of them from the CCTV footage, and an observe alert will be issued. In this case they won't be approached, but will be watched carefully. A person known to be associated with ORC will have an ORC alert issued, leaving it to the discretion of the LPA as to whether they should make an approach or call the police. In addition, there are alerts advising the LPA to immediately call the police. Smith says, "We already have one guy who's a 911 alert. We had approached this person three times, and the fourth time, he had already started stealing after being in there for 20 seconds. When we approached him, he physically assaulted our agent and ran out of the store. So, we converted him to a 911 alert."

## The Value of a Photograph

What the technology does is dramatically increase the value of a digital photograph of a shoplifter. Information that has been filed and forgotten can suddenly be put directly into the hands of the person best equipped to act on that information. And it happens entirely automatically, and at precisely the time that information will be most useful.

Retailers who have been diligently photographing each shoplifter they detain may be sitting on a digital gold mine, since enrolling these photos into the system effectively extends the value of the original detention. Suppose a person is detained for a $50 theft and enrolled. Now every time they are recognized and approached, that's another potential $50 savings—residual value from the original detention.

And the savings extends beyond just the value of the merchandise. There is also substantial savings of store associates' time. "Just think," Smith says, "of the LPA who gets an alert, makes the approach on a shoplifter, and tells him, 'You gotta get out of here.' That takes about three minutes total. Before, they may have watched that person for 20 minutes until they stole something. And if they had detained that person and processed the paperwork, that's another 45 minutes. What was going on

in your store for those 45 minutes? Now, those efforts can be redeployed onto observing and detaining other individuals."

LP organizations may even start valuing a photograph more than a prosecution. "The value of a photo is so much," Smith says, "that I may change the approach for a detention in the store to something less aggressive. We may train agents to approach someone they just saw stealing and say 'Look, give me back the product, let's go back to the office, do some paperwork, I'll take a picture of you, give you a barring notice, and then you're out of here. I'm not going to call the police.'"

Retailers may also be able to reap benefits from photos of other retailers' shoplifters. A national shoplifter database similar to the Stores Mutual Association model is already in the works. This would mean that each additional retailer who adopts the technology and starts sharing will incrementally increase the value of the system for all members.

## The Importance of Statistics

Despite how useful the system is in enforcing barring notices, the greatest LP benefit of facial recognition may be the quality of data the system makes available. Having solid statistics about which individual thieves enter which stores and the distribution of peak shoplifter activity over the course of a day or a month can be extremely powerful in informing management decisions.

in eventual reduction of man-hours necessary to operate an LP organization," says Rosenkrantz. "It's a combination of force multiplication effects and the incredibly valuable statistics." Of course, the system only detects shoplifters in the database. LPAs will still need to keep a lookout for new enrollees. And some high-risk stores need as many eyes on the floor as they can get.

Rather than threaten LP jobs, the technology will likely aid in the evolving shift in LP responsibilities. "What I'm expecting," says David Guttadauro, CEO of leading facial-recognition provider Digital Signal Corporation, "is that loss prevention people will be following a trend I've seen in the intelligence community, government, and law enforcement, in which the traditional role of the detective is changing into the role of the analyst. Data and technology are really going to be how the LP industry is going to be run moving forward. You look at your risks from the standpoint of data and event patterns, and then you analyze those risks to end up taking more informed, evidence-driven action."

## Limitations of the Technology

Determining whether two images of a face match is not a simple yes-or-no question. The system works based on how probable it is that the face on the store camera matches the face in the database. The retailer must set an acceptance

**Facial-recognition systems made the leap from sci-fi to reality around a decade ago, but until the past year or two, they never really worked. Governments were the first adopters, targeting fugitives, terrorists, spies, and other high-priority targets. Retailers have had their eyes on the technology for some time, but until very recently the price point was simply too high to justify.**

Rosenkrantz says, "Let's say you have a store and an LP associate is there the entire day. What if the system tells you that 90 percent of the theft is happening during certain hours of the day, and you're able to adjust the schedule accordingly?" Better data will enable LP departments to optimize the deployment of LPAs to work where and when they're needed most.

And when an LPA isn't on duty, they just hand off the smartphone to the store manager. "In the past month, about 20 percent of our approaches have been done by management," Smith says, "and they love it. They know when a crook walks in their store, and they just walk up to them." The system puts more power back into the hands of the store manager, giving them a greater degree of personal control over external shrink.

Could this reduce the need for in-store LP professionals? "I think the most major impact to the industry as a whole will be

probability threshold, which can be a delicate balancing act.

On the one hand, if the threshold for a match is set too low, many ordinary customers could be identified as shoplifters. This high false-acceptance rate risks alienating customers, wasting the time of the store associates, and generally lowering users' confidence in the system. "That's a scary part for me," says Smith, "the false alert; the boy who cried wolf. But so far it's low enough—about six out of a hundred alerts—that it hasn't gotten to that stage. We've always been able to use the photo to see that it wasn't the right person."

On the other hand, if the threshold for a match is set too high, someone who's enrolled in the system might not trigger an alert, just because the cameras weren't able to get a perfect photo of him as he walked in the store. Enrollment photos are usually like driver's license photos, taken straight-on with

even lighting. It's rare to capture these same conditions on in-store cameras, and any deviation will marginally reduce the probability of a match. "The less that you see of the face, the lower the probability of a match there'll be," says Rosenkrantz, "so when our system sees eyeglasses on a person, it actually removes them and makes some assumptions about what's behind them. We are able to detect people with high match rate who are wearing hoodies, parkas, or scarves, or where the person is looking at their phone or never looking quite at the camera. These things just lower the probability of a match."

While there are limitations, the system is expected to become ever more accurate as the technology matures. And in the instances that the system does fail, what's at stake? "The government uses a lot of facial ID that's very sophisticated," says Smith, "but they're trying to find terrorists. We're just trying to ID a shoplifter or two. People have asked me what happens if it misses one. Who cares? I'm just trying to catch shoplifters. I'm not trying to catch an international terrorist. I don't need the most sophisticated system in the world. I just need one that pays for itself."

## Marketing and the Problem of Privacy

"The initial cost justification that drives the purchase of the system comes from loss prevention," says Rosenkrantz, "because the numbers are a lot more tangible and you can gain empirical evidence of what your savings are. But retailers are exploring future uses for marketing purposes."

There is widespread speculation about what will happen after LP departments have given the system a test drive and marketing departments get hold of it. The possible applications are breathtaking in scope. Dynamic advertisements could be targeted very precisely on a customer-by-customer basis. Sales associates with knowledge of customers' brand, aesthetic, and price preferences could very efficiently guide them to more personally appealing products. Stores could track not only what customers bought, but also what they looked at and didn't buy. Biometric-linked credit cards could enable cashier-less purchasing.

"I see it becoming extremely pervasive," says Rosenkrantz. "It's already being used for digital signage for personalized advertisements. It can identify gender and age ranges with about a 90 percent accuracy. I think that the technology will become incredibly pervasive really in the next five to six years."

Guttadauro agrees. "In five years you'll see the technology in almost every retail store," he predicts. "The price point of the technology is going to come down so that it's affordable based on ROI to almost every retailer. You're talking about a game-changing technology that has sales, marketing, and transaction benefits."

Facial recognition has the potential to change the rules of retail. It could lower shrink, revolutionize in-store marketing, and, ultimately, more efficiently deliver products to consumers, thereby reducing costs for everyone involved—a win-win situation. But as usual, there's a catch. If deployed without careful, deliberate forethought,

the technology could easily be abused, either intentionally or by poor planning, with far-reaching consequences.

The way they're presently deployed for LP purposes, facial-recognition systems are designed to be very conservative. There is little privacy threat and limited potential for abuse. The system immediately discards images of anybody who isn't a match to a known shoplifter. Compare this to ubiquitous archiving of CCTV footage of everyone who enters a store. Surely facial-recognition systems are less intrusive than standard video archiving?

"I would actually agree that, if the system is truly set up like that, it's definitely less intrusive than holding onto security camera footage," says Jennifer Lynch, a staff attorney with the Electronic Frontier Foundation, an international digital rights organization. "A system that is designed to look only for people who have been convicted of shoplifting in the past is not going to be a threat to privacy for the vast majority of shoppers."

The conservative design of Smith's system is the result of long, hard thought about the privacy and process issues he needs to address. But will every retailer be so careful? For loss prevention the only people enrolled are shoplifters. LP doesn't need to identify and track average customers. But marketing is frothing at the mouth at the prospect. And when average customers are enrolled is when potential problems set in.

"The real privacy issue for marketing is how stores are holding on to the data," emphasizes Lynch. "Are they using a system that just detects a person's gender or age range, then forgets their image? Or do they collect identifying information about specifically who that person is and then track that person every time they walk in the store? In that situation it's a huge impact on privacy. And stores may be tempted to go even further and sell the information, and that's a huge problem as well. In the online world and the offline world, it's very easy for data to be collected and then combined with other data so that marketers have a very distinct picture of a person that people would never know about."

## The Risks of Ignoring Privacy

Imagine a retailer that identifies and tracks every customer that enters the store. Imagine they scour Internet image databases, housing records, Facebook and LinkedIn profiles, until they know not just your name, age, address, birth date, and brand preferences, but also income bracket, credit score, social circle, work schedule, and the number and approximate age of your children. Imagine the retailer sells this information—to other retailers, lenders, government agencies, or whoever has the money. Imagine there is a database out there with an incredibly detailed profile of what you like, what you do, and who you are. And you can't change it, delete it, dispute it, or even see it. You might not even know it's there.

These are the sorts of possibilities worrying both privacy advocates as well as forward-thinking retail executives; the possibilities that are ripe for abuse, which would likely result in a consumer backlash. For retailers the potential cost of consumers becoming alienated and eventually rejecting

continued on page 22

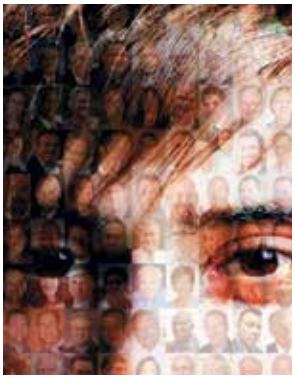
continued from page 20

the technology is enormous, even beyond the loss of a tool as valuable as facial recognition. The PR nightmare and consumer pushback resulting from the wrong sort of publicity could do serious damage to a brand.

The storage and protection of biometric databases presents a further risk. Even very tightly secured credit card databases have been compromised multiple times in recent years, allowing hackers access to hundreds of millions of customers' credit cards and other sensitive information, and costing companies billions. For consumers having credit card information stolen is usually more inconvenience than danger; they simply replace their cards. But it's much more difficult to get a new face.

Who is liable if a biometric profile is stolen? What new crimes are possible if criminals have access not only to the usual information stolen during identity theft, but also to information about a person's physical features and a complex profile of preferences and behavior patterns? If nothing had yet sparked consumer outrage at facial recognition, identity theft of biometrics is sure to.

Even if the vast majority of retailers use the system conscientiously, all it would take is one example of major abuse to jeopardize the use of the technology by all. The legal space surrounding the technology is very blurry. If major abuse came to light or a PR incident was handled poorly, there is a risk that legislation would be crafted too hastily and thoughtlessly, which could end up crippling the technology.



**Facial-recognition technologies, and the torrent of new data they bring, are poised to dramatically alter the LP landscape, changing the day-to-day life of LP professionals, informing top-level decision making, and shifting the way the industry as a whole operates. Soon after, the technology will set the stage for a radical paradigm shift in retail marketing and the retail customer experience.**

## Leading the Charge

Loss prevention professionals are the first adopters, leading the adaptation of this incredibly disruptive technology to the retail world. This leaves the LP industry with the opportunity to spearhead the adoption of privacy standards, process standards, and consumer protections, setting the tone for the impending adoption of the technology by other segments of the retail industry. By very careful, deliberate self-regulation, retailers may be able to avoid consumer pushback and knee-jerk over-regulation that could cripple the technology and deny the industry an incredibly powerful, potentially game-changing tool.

Guttadauro believes his company's technology is so powerful, he won't even sell it to retailers until the privacy and process goals have been adequately addressed. "I don't believe they've done enough work to protect the people on the other side of the camera," he says. "I wouldn't want to risk the market. We need to build a consortium between vendors, retailers, and consumer advocates to really build a foundation of standards."

To what degree consumers ultimately accept or reject the technology will be in large part dependent on the PR response to the first widespread public acknowledgement of the system and its capabilities. Having standards and customer protections already in place will be invaluable in convincing an already-skeptical public that the technology will help them more than threaten them.

Standards will need to address issues like enrollment and unenrollment procedures, data storage and protection, data sharing, transparency, and data ownership, among other things. Different standards may need to be developed for different purposes. For example, Smith says, "We let shoplifters know that we intend on approaching them and that we reserve the right to use biometric ID to identify them for the purposes of enforcing a barring notice." But when it comes to the general public, "We need to let customers know that they own their image and they're in control of their image," says Guttadauro. "If they want to be detected, they should be able to opt in for detection. And since it's your right to opt in, we should also guarantee that you can opt out."

A standards consortium could protect the industry moving forward, but only if it actually succeeds in protecting the consumer as well.

## Future Directions

As the technology evolves and becomes more widely adopted, there will be many challenges and many benefits to be gained if challenges are properly addressed. What else is on the horizon?

Industry experts are already predicting an ORC response. There may soon be blogs sharing tips about how to confront facial-recognition systems and listing which brands and which stores within each brand are known to use them. "When most

continued on page 24

continued from page 22

retailers in a certain geographic area adopt the technology," says Smith, "those who haven't could end up taking a disproportionate amount of ORC theft until they're on a level playing field. It's a mousetrap game. I think it puts us one mousetrap ahead of the people who are really burning us in ORC activity. I do think they'll catch up, figure out how to beat it, or go where it's not. But I think it eliminates, or close to eliminates, personal use theft in a store. And that's huge. Because all that's left is the new batch that comes in, and they don't show up at the same rate."

Meanwhile, the technology itself is only going to become more accurate and comprehensive. Current retail solutions leverage existing IP cameras, which generate a normal two-dimensional image. The most sophisticated facial-recognition solutions, used by governments and intelligence agencies and already nearing perfect accuracy, use special cameras to generate a three-dimensional model of the face. There is also research toward a mixed biometric approach, using gait recognition, earlobe recognition, skin-texture recognition, and other biometrics that could make it possible to identify a person without even needing to see the face.

The technology could also have positive effects that spread from the industry into greater society. "Take juvenile delinquency," says Guttadauro. "For a 15-year-old shoplifter, a conviction scars them. They get no financial aid, fewer job prospects. Retailers are literally creating a downward cycle of shoplifting by the way that we approach it as a whole. Using facial recognition, if we catch a 15-year-old shoplifting, we're not going to prosecute him, we're going to register him into the database, we're going to have his parents come down and sign a form saying 'Johnny will never shoplift again and I agree to let you use his image.' The next time he comes back into the store you say 'Welcome back to Store-Mart, Johnny. Please don't shoplift, or we're going to call your parents.' It'll have the same effect on shoplifting, but the kid doesn't end up with a criminal record, and the court costs are significantly less both for the retailer and the municipality."

Facial-recognition technologies, and the torrent of new data they bring, are poised to dramatically alter the LP landscape, changing the day-to-day life of LP professionals, informing top-level decision making, and shifting the way the industry as a whole operates. Soon after, the technology will set the stage for a radical paradigm shift in retail marketing and the retail customer experience. Like most disruptive technologies, facial recognition has the potential to bring considerable benefits as well as considerable abuse. It's in the hands of loss prevention leaders today to choose the course for the future and to blaze the path that takes us there. ■

CHRIS TRLICA is a business and technology analyst and researcher based in North Carolina. He is a new contributing writer to *LP Magazine* focusing on emerging technologies. He can be reached at chris.trlica@gmail.com.