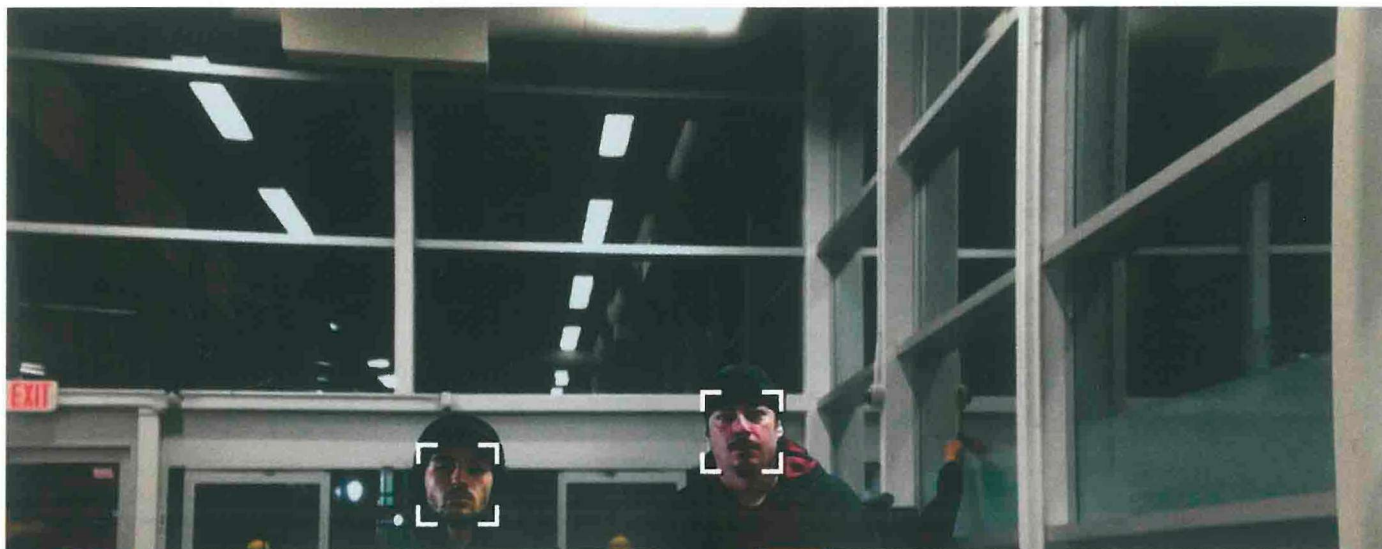


Nice to See You Again

Facial recognition is becoming a competitive tool in the fight against fraud








Mark Devlin

OBSERVE

4 visits across 2 locations.
Last visit: 13 days ago.
Prior shoplifting conviction.

- Organized Retail Crime (ORC)
- [see more details](#)

Dmitri Ivanov

OBSERVE

7 visits across 3 locations.
Last visit: 8 days ago.
Prior shoplifting conviction.

- Organized Retail Crime (ORC)
- [see more details](#)

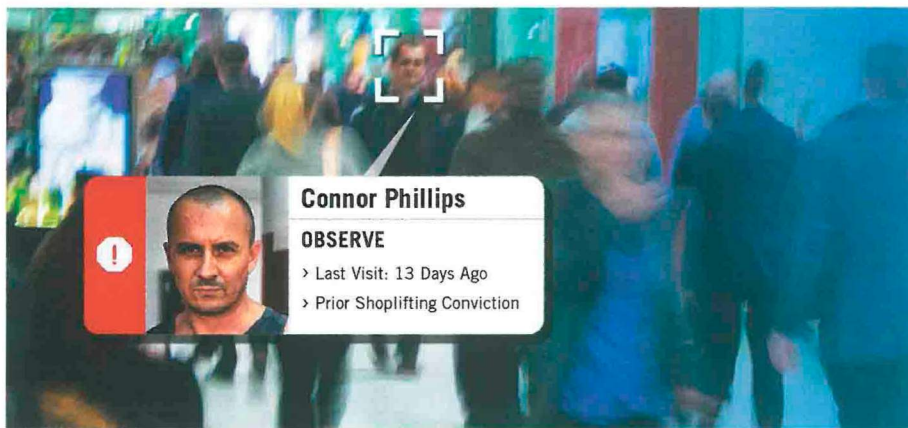
by DAVID SCHULZ



Return policies are coming back to haunt some retailers. Customers — and some people who are not customers — seem to have an insatiable appetite for bringing goods into a store and asking about credit for returned merchandise.

Even venerable L.L.Bean was forced to modify its generous “lifetime” return policy earlier this year because people were doing things like buying the company’s merchandise at yard sales and sending the items to L.L.Bean looking for a refund.

More recently, a man in Yuma, Ariz., was charged with making \$1.3 million worth of fraudulent returns at Walmart stores across the country.

In some cases of fraud, merchandise presented for returned isn’t even purchased in that store. It may not have been purchased anywhere but shoplifted



Connor Phillips

OBSERVE

> Last Visit: 13 Days Ago
> Prior Shoplifting Conviction

or otherwise stolen. The challenge for retailers is to separate legitimate customers returning goods from thieves and scammers.

Some retailers use third-party services to monitor individuals returning merchandise, scoring them on factors such as whether a receipt is involved, the length of time between purchase and

return, value of the returned merchandise and whether the individual had returned too much merchandise within a short time span.

Other retailers are using facial recognition technology to combat returns fraud, comparing the facial image against a database of known shoplifters and fraudsters.

Merchandise returns cost retailers in the United States more than \$350 million in sales last year, including up to \$22.8 billion attributed directly to fraudulent returns and abuse, estimates data analytics firm Appriss.

“Fraud is such a big number in retail, one that largely goes unchecked,” says Peter Trepp, CEO of FaceFirst, a software firm that provides a security face recognition platform for use in industries including retail, air transportation, casinos, sports and event venues. The company recently unveiled Fraud-IQ, which it calls the first facial recognition product built specifically for use against retail return fraud.

“It’s hard to find tools to combat fraud,” Trepp says. “Part of this is because criminals have become so sophisticated. We think [facial recognition] is a contribution to battle this.”

The new Fraud-IQ works in two ways to assist retailers. “First, it can identify people entering the store without a package and then showing up at the return counter with goods to return,” Trepp says, “and the second works against repeat offenders.”

This latter involves patterns, analytics and software. “It arms retailers against previous offenders,” he says.

TRAINING THE ALGORITHM

Nobody likes being confronted as a potential thief or fraudulent returner of merchandise. “We train our clients to be customer-friendly, so their customers will come back and shop,” Trepp says. “But there are a lot of people trying to work the system.”

As a result, FaceFirst suggests that when an individual has been identified as a prior offender, they should be greeted by a manager or loss prevention associate with an innocuous but pleasant phrase such as, “How can we help you today?”

“The person will recognize they have been spotted and will be watched,” Trepp says. “Usually, they will leave the store.”

Facial recognition has been in the news recently, for its use at border crossings as well its ability to identify the suspect in

the Capital Express newspaper shootings in Annapolis, Md., that left five dead.

Still there are critics of the software. Among the most vocal have been those who maintain the technology makes a higher number of misidentifications when dealing with people of color, women and especially women of color.

“We do not see these issues with our customers,” Trepp says. By way of explanation, he notes that an algorithm is at the center of facial recognition technology. When faulty identifications based on gender or color are made, it means “these algorithms were not trained sufficiently,” he says.

At FaceFirst, after developing the algorithm, “We begin training the machine, giving it millions of images. Hundreds of thousands of images won’t do, it has to be millions,” he says. “If you don’t train with images of women, people of color, women of color,” the system is not well trained.

Another frequent criticism of facial recognition technology is its potential for invading privacy or otherwise not protecting consumers’ personal information.

“A number of things really matter, especially privacy. This influences the way we develop our software,” Trepp says. “We have a motto: ‘Privacy by Design,’ because everything we do is done with an eye toward handling people’s data. We are very, very careful with that.”

ADDITIONAL LP USES

The technology has the capability for multiple uses inside stores. “It absolutely can be of help” in combatting employee theft, Trepp says, because it can track how many times an employee leaves and re-enters the store during a work shift. It can also track how often a friend might visit an associate and buy a few things, not all of which are necessarily rung up, or how frequently friends are showing up in a store just around an employee’s quitting time.

When Fraud-IQ was launched in June, joining FaceFirst’s broader retail security facial recognition platform,

Trepp pointed out that shoplifting and in-store violence could be addressed as well as return fraud.

“A lot of people who are shoplifting are also ones that are prone to violence. Crime is trending down, but it is up in stores,” Trepp says. “Stopping people before going into the store is preferable to having surveillance cameras record the crime and let the shoplifter walk out with the merchandise. With facial recognition, they leave once they realize they’ve been spotted.”

FaceFirst maintains that its technology reduces shoplifting by an average of 34 percent and in-store violence by 91 percent.

“Retailers are under assault from organized retail crime and other dishonest customers,” Trepp says. “We’re seeing rapid face recognition adoption across big box, grocery and pharmacy retailers.”

He also sees facial recognition as a factor in facilitating seamless omnichannel retailing. “The lines between online and physical [retailing] will be blurred because of facial recognition,” he says. One example he offers: A shopper walks into a store, is immediately recognized as a regular customer and receives notices of specials, coupons via smartphone.

As for whether any of FaceFirst’s retail customers had run into any problems claiming the use of facial recognition had violated someone’s privacy, Trepp says, “No.”

“A big part of this is how we train customers,” he says. “People accuse facial recognition of things that don’t happen on a daily basis. If the system does recognize someone, nobody is put up against the wall and told to raise their hands. They are just greeted by someone.”

Amplifying his point about familiarizing users with facial recognition, “We rely heavily on this training,” Trepp says. “We view our relationship with retailers as a partnership.” **STORES**

David P. Schulz has been writing for STORES since 1982 and is the author of several non-fiction books.