When convenience meets surveillance: AI at the corner store

July 5 2019, by Melissa Hellmann, The Seattle Times

Jacksons Food Store customer Denise Diharce was surprised to learn that the Tacoma location she frequents for odds and ends is testing a high-tech system that, prior to entry, will compare her to images of previous crime suspects.

Before patrons can enter the basic convenience store at the corner of South 38th Street and Pacific Avenue, a camera under a red awning will take a picture and use artificial intelligence (AI) to decide whether the image matches any in a database of known robbers and shoplifters at that location.

"That's a privacy violation because you should be notified about it," Diharce said on a recent morning. "They should have a sign to notify you that they're comparing it to photos of criminals."

Jacksons spokesperson Russ Stoddard said that when fully functional, the system will operate from 8 p.m.-6 a.m. It's now deactivated after a recent test, but when it's turned back on, a sign at the front of the store will notify customers that facial recognition technology is in use, and a speaker will ask customers to look at the camera. The door won't unlock if someone is wearing a mask or if the person has been previously flagged for criminal activity by in-store camera footage.

A customer named May, who asked that her surname not be used, said she had no issue with the surveillance tool, but questioned its purpose in a corner store.
"It's a little store—I don't see why they need something like that," May said as she stood in the Jacksons parking lot.

The testing at Jacksons, first reported by KIRO 7, is part of a larger trend in which retailers, as well as governments, are turning to AI cameras to combat criminal activity and to observe people's habits for other purposes. It's a development that has privacy advocates wondering if the anti-crime efforts outweigh the civil liberty risks.

Big box retailers such as Target, Walmart and Lowes have also used AI cameras to prevent criminal activity, and a recent report by research firm CB Insights found stores are not always forthcoming about their use of the technology. AI cameras may watch more than just shoplifters: At a Long Island Walmart, The Associated Press reported, thousands of high-resolution cameras were recently installed to monitor inventory on shelves and even the ripeness of fruit.

Civil liberties groups worry that if it goes unregulated, the increased use of facial recognition software in stores and elsewhere could perpetuate biases and lead to mass surveillance.

The facial recognition software at Jacksons is created by Blue Line Technology, a Fenton, Mo.-based company that partners with Dell and Axis to provide the video security system.

The platform is not connected to a criminal database, so a store manager must flag a suspected shoplifter's image to receive a notification when the person approaches the store again. Names and personal data aren't gathered by the system, and the company recommends its users only store images of nonflagged customers for 24-48 hours, while suspected shoplifters are kept in the database.

Retail can be a dangerous line of work: According to industry
Blue Line Technology senior partner Tom Sawyer said the more than 20 retail companies that use its software platform throughout the nation have reported a 95% reduction in police service calls, and shoplifting theft is cut in half.

A video of an attempted robbery last summer showed two masked people run from view after they were denied entry into a Yakima AMPM store that uses Blue Line's system.

"We understand the stigma behind facial recognition," said Sawyer. "All we want to do is stop robbers."

The Jacksons in Tacoma is the Idaho-based company's second location to install the video surveillance system, said Vice President of Operations Jill Linville in an email. Another Jacksons in Portland, Ore., has used the technology for about a year, and company spokesperson Stoddard said criminal activity has greatly dropped thanks to the system.

Once it's fully installed at the Tacoma store, the AI security system will serve as a testing ground for use in its other locations in five Western states, although Linville said it would not be deployed in all the nearly 245 stores.

Blue Line Technology's security platform takes the limited action of locking a door on suspected shoplifters, which differs from systems that strive to analyze what people are doing in real time, sometimes called video analytics.

Another AI security camera startup, Austin, Texas-based Athena Security, uses video analytics to detect guns or criminal activity at businesses, schools and places of worship, then alerts law enforcement to
the potential danger.

The company says it seeks to prevent racial profiling and the collection of personal information by blurring out subject faces before the AI system analyzes the video. Last month, the startup installed its AI-powered cameras at the Al-Noor mosque in Christchurch, New Zealand, following the murder of 50 worshippers at two mosques there in March.

"The core A.I. brain that powers Athena Security is just scratching the surface of what it's capable of to mitigate crime and save lives, but the road map is also full of evil potholes that we'll need to size up and take the right course," Chris Ciabarra, CTO and co-founder of Athena Security, said in an email.

A new ACLU report detailing concerns about intelligent video surveillance technology finds that AI security systems are becoming more commonplace because it's getting easier and faster to build systems that recognize people and analyze images. The amount of time it takes to train an artificially intelligent machine to recognize objects in images has decreased from an hour to a few minutes, according to a Stanford University report.

The proliferation of AI surveillance technology could usher in "a society where everyone's public movements and behavior are subject to constant and comprehensive evaluation and judgment by agents of authority—in short, a society where everyone is watched," warned Jay Stanley, the report author and senior policy analyst with the ACLU Speech, Privacy, and Technology Project.

Blue Line Technology software footage is only accessed by law enforcement if store management chooses to share it. Amazon's smart doorbell company Ring, on the other hand, uses an app called Neighbors to share neighborhood surveillance videos and tips with law enforcement.
agencies.

Jake Laperruque, senior counsel at the D.C.-based nonprofit Project on Government Oversight, says more retail stores are using surveillance technology to observe shopper habits and curb shoplifting, although he called Jacksons use of AI-technology to allow entry "a little extreme."

Another instance of AI use in retail is to monitor merchandise. The ACLU report cited Target's use of AI video analytics to notify store security when customers spend an extensive amount of time in front of certain items.

Target told The Seattle Times it stopped using the video analytics system in the one store where it was piloted; the retail giant also discontinued testing facial recognition software to prevent fraud and theft in a small number of stores last year.

"As we always do, we'll continue to test and learn from new technologies that have the potential to keep our guests and team members safe," Target spokesperson Danielle Schumann wrote in an emailed statement.

Lowe's also decided not to use facial recognition technology for any purpose after conducting a three-month test at three stores four years ago, said company spokeswoman Maureen Wallace.

Aside from security systems, video analytics are used in a range of machines for commercial or governmental reasons, such as to power autonomous cars or robots.

The unprecedented potential for mass surveillance calls on policymakers to strike a delicate balance between the constitutional right to privacy and freedom of expression when creating regulations, says Stanley.
To prevent widespread misuse of video analytics systems, Stanley recommends that governmental agencies should openly discuss the use of the technology prior to implementing it. Video analytics should only be used in necessary situations, he suggests, and not to make decisions that could alter people's lives without their approval. Nor should private companies use video analytics to collect customer data for marketing reasons.

Laperruque from the Project on Government Oversight expressed concern about the lack of regulation over the use of facial recognition in retail settings. Facial surveillance technology has been shown to misidentify women and darker skinned people at a higher rate than lighter skinned males.

Although Blue Line Technology spokesperson Sawyer said the software has never misidentified anyone, Laperruque said its use at Jacksons "doesn't seem to be a good thing for anything other than a discrimination lawsuit."

©2019 The Seattle Times
Distributed by Tribune Content Agency, LLC.

Citation: When convenience meets surveillance: AI at the corner store (2019, July 5) retrieved 1 August 2024 from https://phys.org/news/2019-07-convenience-surveillance-ai-corner.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.