Professor weighs benefit vs. risk of facial recognition technology

9 May 2013

Phys.org — Many states are using the technology to scan driver's licenses to prevent identity fraud. It led to the arrest of a suspected arsonist in New York. And while facial recognition technology could not identify the Boston Marathon bombing suspects, police used the software in their search.

These recent headlines illustrate the benefits this technology provides for law enforcement agencies in an investigation. Not surprisingly, many businesses also see an advantage in using facial recognition, not for crime-fighting, but to reach customers. However, Brian Mennecke, an associate professor of information systems at Iowa State University, questions whether customers are ready for it.

"It's beneficial for a company to have more information about you because it allows them to customize their service and products as well as their advertising. And it's certainly beneficial to the customer because they don't have to waste time essentially relaying that information," Mennecke said. "But the other side of this story is really the privacy aspect."

Retailers have collected data on customer preferences and demographics for years, but biometrics takes it to a new level. Facial recognition software is already used in social media applications, like Facebook's "tag suggestions." The technology scans uploaded images and then matches the biometrics to names and faces "tagged" in other photos in its database.

It may seem like a cool feature, except the users cannot control or modify this profile, Mennecke said. In fact, they give Facebook permission to create and maintain a profile database as part of the "terms of service" they agree to when signing up for Facebook.

Business applications

Intel is also using facial recognition software in its digital signage displays, Mennecke explained in a study published online in the journal Business Horizons. The displays use touch screens to interact with the customer and feature everything from video and graphics to Internet sites and broadcast clips.

The technology also identifies general characteristics like gender, age and race and tracks how customers use the display and for how long. Mennecke says the Intel system promises anonymity as it builds a digital customer profile that includes physical characteristics. It's what Mennecke calls a "marketing avatar" or "mavatar."

Businesses want that personalized information to provide better customer service and to make the most of advertising dollars by directly targeting consumers with specific, detailed information.

"If you watch people as they walk around public places, like the mall, people mostly ignore signs and billboards. This is because we are bombarded..."
with so many irrelevant ads and displays. The more relevant the ad, the more likely that someone will look at it. So if ads can be targeted, retailers can do a better job of grabbing your attention," Mennecke said.

A price for privacy

Facial recognition technology promises benefits for consumers if they are willing to sacrifice some privacy. Mennecke says retailers could use the software in digital kiosks or smart phone applications to identify and collect consumer information. However, he believes it will still be a few years before that happens because people are hesitant to opt into a service that uses a biometric scan of their face.

To make it work, Mennecke says businesses will have to offer incentives to get customers to sign up for and use the service. The concept is similar to businesses that offer free Wi-Fi service as a courtesy in exchange for the right to identify and track where customers go online.

"I'm convinced we're all willing to sell our privacy to a degree, if the service is right and I'm getting something worthwhile out of it," Mennecke said. "In return, companies will pay you through loyalty points or better service to opt in to some of these types of services, which we've been doing for 30 years with credit cards."

In addition to privacy concerns, there are also ethical questions to consider. Mennecke fears that facial recognition technology could result in more cases of identity theft as well as stalking, if the information falls into the wrong hands. Issues that both businesses and consumers must consider, Mennecke says, before embracing the technology.

The recent launch of Google Glass is already sparking a debate over privacy and could create a slippery slope, Mennecke said. The person wearing the glasses can discreetly snap a photo with a simple wink of the eye. He offers the following example as a reason to exercise caution.

"If someone can use Google Glass or his cell phone to take a picture of you and use it to search for you in Facebook or on Google, then he could dig out all kinds of personal information about you while you are shopping or driving down the street," Mennecke said.

While this is technically feasible, Mennecke thinks it will probably be sometime before there is an app for smart phones to allow this type of scanning. Search engines, like Google, will be reluctant to support these types of applications, he said.

Mennecke recommends businesses clearly explain to customers how the technology will be used and guarantee that individuals have input as to how their "mavatars" are created and used. By addressing these issues now, Mennecke hopes it will limit problems once the use of facial recognition software is more widespread.


Provided by Iowa State University