INTERACTIVE SESSION TECHNOLOGY

Do You Know Who Is Using Your Face?

Facial recognition is an artificial intelligence application that can uniquely identify a person by analyzing patterns based on the person's facial textures and shape. Facial recognition systems can be used to identify people in photos, video, or real-time. A facial recognition system uses biometrics to map facial features from a photograph or video. It compares the information with a database of known faces to find a match. The face recognition system uses computer algorithms to highlight specific, distinctive details about a person's face, such as the distance between the eyes or the shape of the chin. (Some algorithms explicitly map the face, measuring the distances between the eyes, nose, and mouth and so on. Others map the face using more abstract features.) The system converts these details to a mathematical representation and compares them to data on other faces stored in a face recognition database. The data about a particular face is called a face template, and it can be compared to other templates on file. Facial recognition technology learns how to identify people by analyzing as many digital pictures as possible using neural networks, which are complex mathematical systems that require vast amounts of data to build pattern recognition.

Face recognition tools are now frequently used in routine policing. Police compare mugshots of arrestees to local, state, and federal face recognition databases. Law enforcement can query these mugshot databases to identify people in photos taken from social media, traffic cameras, and closed circuit television surveillance cameras in stores, parks, and other places. There are systems to compare faces in real-time with "hot lists" of people suspected of illegal activity. Face recognition has also been used in airports, border crossings, and events such as the Olympic games. The FBI spent more than a decade using such systems to compare driver's license and visa photos against the faces of suspected criminals.

Facial recognition systems can make products safer and more secure. For example, face authentication can ensure that only the right person gets access to sensitive information meant just for them. It can also be used for social good; there are nonprofits using facial recognition to combat trafficking of minors. However these systems also have limitations that can do harm as well.

Dozens of databases of people's faces are being compiled by companies and researchers, with many of the images then being shared around the world. The databases are pulled together with images from social networks, photo websites, dating services like OkCupid, and cameras placed in restaurants and on college quads. While there is no precise count of the data sets, privacy activists have pinpointed repositories that were built by Microsoft, Stanford University, and others, with one holding over 10 million images while another had more than two million. Georgetown University has estimated that photos of nearly half of all U.S. adults have been entered into at least one face recognition database.

Tech giants like Facebook and Google are reputed to have amassed the largest facial data sets, which they do not distribute, according to research papers. But other companies and universities have widely shared their image troves with researchers, governments, and private enterprises in Australia, China, India, Singapore, and Switzerland for training artificial intelligence, according to academics, activists, and public papers.

Startup Clearview AI created a powerful facial recognition app that enables the user to take a picture of a person, upload it, and be able to view public photos of that person, along with links to where those photos appeared. The system uses a database of more than three billion images that Clearview claims to have scraped from Facebook, YouTube, Venmo, and millions of other websites. Federal and state law enforcement officers have used the Clearview app to help solve shoplifting, identity theft, credit card fraud, murder, and child sexual exploitation cases.

Companies and labs have gathered facial images for more than a decade, and image databases are an essential component of facial recognition technology. But people often have no idea that their faces are in them. And although names are typically not attached to the photos, individuals can be recognized because each face is unique to a person. There is no oversight of these facial recognition data repositories.

Privacy advocates worry that facial recognition systems are being misused. A database called Brainwash was created by Stanford University researchers in 2014. The researchers captured over 10,000 images using a camera located in San Francisco's Brainwash Café (now closed). It is unclear whether the patrons knew their images were being captured and used for research. The Stanford

researchers shared Brainwash with Chinese academics associated with the National University of Defense Technology and Megvii, an AI company that provided surveillance technology for racial profiling of China's Uighur Muslim population. Brainwash was removed from its original website in mid-2019.

Using eight cameras on campus to collect images, Duke University researchers gathered more than 2 million video frames with images of over 2,700 people. The database, called Duke MTMC, was reported to have been used to train AI systems in the United States, Japan, China, and elsewhere. The cameras were identified with signs, which gave a phone number or email for people to opt out.

Moreover, facial recognition systems are not entirely accurate. Face recognition systems have varying ability to identify people under challenging conditions such as poor lighting, low-quality image resolution, and suboptimal angle of view, which might occur if a photograph was taken from above looking down on an unknown person.

Facial recognition software is poor at identifying African Americans and other ethnic minorities as well as women and young people. A 2012 study co-authored by the FBI reported that accuracy rates were lower for Afro-Americans than for other demographics. Although the FBI claims that its facial recognition system can find the correct candidate in the top 50 profiles 85 percent of the time, that's only when the true candidate exists in its gallery. If the candidate is not in the gallery, the system may still come up with one or more potential matches, creating false positive results. Those identified could then be targeted as suspects for crimes they didn't commit.

Face recognition becomes less accurate as the number of people in the database increases. Many people around the world look alike. As the likelihood of similar faces goes up, matching accuracy goes down.

Sources: "Face Recognition," www.eff.org, accessed April 21, 2020; Kashmir Hill, "The Secretive Company that Might End Privacy as We Know It," *New York Times*, January 18, 2020; Cade Metz, "Facial Recognition Tech Is Growing Stronger, Thanks to Your Face," *New York Times*, July 13, 2019; www.ai.google.com, accessed April 21, 2020.

CASE STUDY QUESTIONS

1. Explain the key technologies used in facial recognition systems.
2. What are the benefits of using facial recognition systems? How do they help organizations improve operations and decision making? What problems can they help solve?
3. Identify and describe the disadvantages of using facial recognition systems and facial databases.

TABLE 11.4 EXAMPLES OF NEURAL NETWORKS

FUNCTIONALITY	INPUTS	PROCESS	OUTPUTS/APPLICATION
Computer vision	Millions of digital images, videos, or sensors	Recognize patterns in images, and objects	Photo tagging; facial recognition; autonomous vehicles
Speech recognition	Digital soundtracks, voices	Recognize patterns and meaning in soundtracks and speech	Digital assistants, chatbots, help centers
Machine controls, diagnostics	Internet of Things: thousands of sensors	Identify operational status, patterns of failure	Preventive maintenance; quality control
Language translation	Millions of sentences in various languages	Identify patterns in multiple languages	Translate sentences from one language to another
Transaction analysis	Millions of loan applications, stock trades, phone calls	Identify patterns in financial and other transactions	Fraud control; theft of services; stock market predictions
Targeted online ads	Millions of browser histories	Identify clusters of consumers; preferences	Programmatic advertising