CBA Report
Cincinnati Bar Association
December 2011

Privacy Face Off

Facial Recognition:

The End of Privacy or a Precursor for New Laws?

By Craig A. Hoffman

Do you feel compelled to wear a Richard Nixon mask or a baseball hat equipped with infrared signal emitters on the brim when you leave the house? If so, you may be trying to prevent a passerby on the street from guessing your name, interests, Social Security number, or credit score using only a pair of face-scanning glasses and an iPhone. This is not science fiction — law enforcement has been using facial recognition technology for years. Through advances in facial recognition software and the convergence of the vast amount of personal information on social networks (especially photographs), smartphones, the power of cloud computing, and statistical re-identification, the use of this technology has the potential to become widespread. The potential ubiquitous use of facial recognition technology raises critical concerns regarding privacy, security, and basic freedom.

Rooted in 1960's

Facial recognition technology traces its origin to government-funded research in the 1960s. The technology works by using an algorithm to create a unique numerical code from distinguishable landmarks on faces, sometimes called nodal points. The technology measures approximately 80 nodal points, such as the distance between eyes, nose width, eye socket depth, and jaw line length. The unique code or "biometric template" created by facial recognition software from a photograph can be stored in a database and later compared to other photographs to create a match.

There are several applications of facial recognition technology in law enforcement that most would agree are useful. Police in Tampa, Fla., have made over 500 arrests after identifying suspects by taking photographs at a traffic stop and comparing the images to a mugshot database. In 2010, the Massachusetts state police obtained over 100 arrest warrants for creating false identities and revoked 1,860 licenses using facial recognition software against the state's driver's license registry. In Britain, Scotland Yard is using facial recognition software to identify suspects from the recent riots in London.

Facial recognition can also provide modern convenience. Since 2002, Australians have been able to use self-processing e-passports at airport customs checkpoints. Advertisers have generated more relevant billboard advertisements based on the age and gender of passers-by. Even Facebook uses facial recognition to suggest the identity of friends to tag in a photo, and programs like iPhoto and Picassa allow users to organize photographs by faces.

The technology is not foolproof, and there are other applications that are outright alarming. The ability to successfully identify a person by matching two photographs is dependent on the quality of the images. If the person in the photograph is not directly facing the camera with open eyes and in front of a plain, light-colored background, the performance of the facial recognition software declines. Thus, while you can obtain a high-quality picture from a driver's license database, pictures taken without the cooperation of the subject (e.g. through surveillance cameras) rarely meet the ideal standard. Although the technology has improved over the last 10 years, there is an inherent error rate because it is reliant on statistics. Accordingly, either matches that should be made do not occur or false identifications happen.

False ID's

A driver in Boston recently had his license revoked because his picture closely matched the picture of another driver. Although his license was returned, it took days of wrangling for him to prove his identity. At least 34 other states are using similar technology. There are no current reported statistics on the number of false positives, but Massachusetts alone issues 1,500 suspension letters per day using the system.

On August 4, 2011, researchers from Carnegie Mellon's CyLab presented the results of three experiments from which they concluded that it is possible to use facial recognition software to identify strangers and then determine sensitive information about that person, including their Social Security number.

In one experiment, the researchers were able to identify members of Match.com, who used pseudonyms on the dating site to protect their identities, by comparing their profile photograph to photographs on Facebook.

In the second experiment, they took photographs of college students that they were able to successfully match one-third of the time to the student's Facebook profile (in less than three seconds).

In the third experiment, the research- »

ers used a custom iPhone application to predict a stranger's Social Security number (generally just the first five digits) by matching a photograph to a Facebook profile picture in conjunction with information about the stranger's state and year of birth gathered online. The lead researcher, Alessandro Acquisiti, said: "A person's face is the veritable link between their offline and online identities."

What About Personal Liberty?

In addition to the obvious privacy concerns, there are security and personal liberty concerns. According to a report, one in 750 passengers scanned at an international airport in the United States is falsely identified, and some of the falsely identified individuals may have been temporarily detained by the FBI. In locations where biometric data like facial recognition is used to gain entry to a secured area or through customs, the failure of those institutions to safeguard that data in a computer system can lead to unauthorized persons gaining access.

Although it is not yet possible to consistently and accurately identify all of the faces in a crowd, the technological limitations are likely to continue to fade. The billions of images tagged on social networking sites and associated data provide an easily accessible source of personal information to match with other offline data collected by data aggregators, which can be turned into detailed personal profiles and sold to companies for use in behavioral advertising targeted directly to you through your smartphone or cable box. It may become possible to search for a person online using an image of their face just as easily as it is now to enter a name in a search engine. On the law enforcement side, the FBI will begin testing its Next Generation Identification facial recognition system in January 2012 in four states. The system, which will also use biometric indicators (e.g. iris scans and voice recordings) to identify suspects, will match a photo of an unknown person against mug shots.

Facial recognition technology has not gone unnoticed by lawmakers and regulators. The FTC is hosting a workshop to explore beneficial uses of the technology and the associated privacy and security concerns on December 8, 2011. And U.S. Senator John Rockefeller has asked the FTC to provide a report on the findings from its workshop to his Commerce Committee.

The applications of facial recognition technology may force a paradigm shift in how we view privacy. Will we enact laws to increase our privacy rights in the face of emerging technology, or will we accept that "privacy is dead" and "deal with it" as some social networking sites and privacy experts have suggested?

Hoffman is an associate at Baker Hostetler LLP where he focuses his practice on complex business disputes, as well as data privacy, information security and social media. He has also represented companies in class action litigation arising from data breaches and alleged violations of federal privacy laws and regulations. His is the editor of the firm's Data Privacy Monitor blog, providing commentary on developments in data privacy, security, social media and behavioral advertising.