Keeping One's Public Face Private

By John M. McNichols, *Litigation News* Contributing Editor

© Scharfsinn86 /Getty Images

Given the widespread mask-wearing caused by the COVID-19 pandemic, 2020 will likely be remembered as a year of covered faces. But it was also a year of profound attention to faces. Social unrest and civil disturbances gave rise to efforts by law enforcement and private citizens to identify the persons involved—both peaceful activists and violent criminals. Persons reviewing the footage of such incidents were in some instances aided by facial recognition technology, a form of artificial intelligence capable of comparing photographic images of human faces and identifying potential matches.

Although not as reliable as other biometric matching techniques, such as iris scans or fingerprints, facial recognition technology has the critical advantage of its ability to function without the cooperation or even awareness of the person under analysis. Given the near-ubiquitous presence of cameras and the vast reservoir of electronic images available for cross-reference—everything from mug shots to Instagram selfies—the technology provides an invaluable tool to law enforcement and national security officials seeking to identify suspected criminals or terrorists. But for the very same reasons, the use of facial recognition technology raises concerns among privacy activists and civil libertarians who see in it the potential for abuse.

Facial Recognition Technology

Facial recognition technology is a relatively new type of software capable of analyzing human facial features in a still photograph or video. Initially developed in the 1960s, it relies on machine-learning algorithms to teach computers to appreciate the distinctive features of a face and to distinguish it from other objects, including other faces. The technology first came into widespread use in the 1990s, when state driver's license bureaus began using it to prevent applicants from obtaining multiple licenses under different names. More recently, it helped confirm the death of Osama bin Laden.

By no means has facial recognition technology been limited to government use. Personal-device manufacturers offer it as an enhanced security feature, allowing a user to unlock a device by presenting his or her face. Airlines and sporting arenas have employed it to assist in security screening, and retailers have experimented with it to track shoplifters. Nor have all of its private-sector uses focused on personal security. Social media companies employ a form of facial recognition technology through programs that allow users to sort and group personal photographs by the persons who appear in them.

Legal Controversies and Responses

Concerns that the widespread use of biometric technology would infringe on personal privacy elicited a legal reaction. In 2008, Illinois enacted the Biometric Information Privacy Act (BIPA), becoming the first state to require notice and consent before collecting or using private citizens' biometric information, including "facial geometry." California followed suit in 2018 with its Consumer Privacy Act, which requires certain businesses to disclose when they collect a person's "faceprint" or other biometric information. Similar bills regulating or even banning the use of facial recognition technology have since been introduced in nearly a dozen states. In October 2020, Vermont became the newest state to legislate on the issue, enacting a broad ban on the use of the technology by law enforcement.

Several major municipalities, including San Francisco and Boston, similarly banned facial recognition technology for law enforcement use. These municipal bans were motivated not merely by privacy concerns but also by the fact that the technology can have a disproportionate impact on minority communities through false identifications. As commentators noted, an algorithm's ability to distinguish among faces is only as good as the sample set that it learns from. If a sample predominantly comprises white men, software based on that sample will have a lower degree of accuracy when applied to other demographics. Based on these concerns—as well as the possibility that the technology might be used to target peaceful protesters against police abuses—several major facial recognition vendors recently imposed voluntary moratoriums on the sale of their software to law enforcement.

There is currently no federal law in the United States governing the collection of biometric information in general or facial recognition technology in particular. That may soon change. In February 2020, Senators Corey Booker and Jeff Merkley introduced the Ethical Use of Facial Recognition Act, which would prohibit federal law enforcement from using the technology without a warrant and disallow the use of federal funds for facial recognition technology by state and local governments. In light of the heightened sensitivity over the use of the technology arising from the protests during the summer of 2020, the 117th Congress is expected to take up the legislation anew.

For the same reasons that facial recognition technology is an invaluable tool for law enforcement, it raises concerns among privacy activists and civil libertarians.

Private Use and First Amendment Implications

Since the passage of BIPA in 2008, Illinois courts have seen multiple class action lawsuits against private companies based on their collection of imagery for use in facial recognition databases. One such lawsuit, filed by the American Civil Liberties Union against Clearview AI in May 2020, made headlines when it alleged that the defendant had compiled its database through the "scraping" of photos from internet sources such as social media accounts, which the plaintiffs claimed amounted to the unconsented use of personal information.

In its defense, Clearview argued that its actions are protected by the U.S. Constitution and, in particular, the First Amendment right of public access. Specifically, the company asserted that the imagery it collects is not taken from private, secure, or proprietary sources, but rather exclusively from public-facing internet pages and postings, information that is in the public domain and thus fair game for anyone's use. Although the merits of this defense have yet to be decided, it is difficult to draw a principled line between a company's right to use publicly posted images and (for example) a paparazzo's right to take photographs of celebrities on the Hollywood Walk of Fame. On a more practical level, facial recognition technology companies have also asserted that their review of photographs from across the internet enables them to notify customers when photographs featuring their faces are uploaded—irrespective of whether the customer is "tagged" by the uploader—enhancing rather than diminishing the customer's awareness and control over personal imagery.

Going Beyond Recognition

Facial recognition technology may have applications going beyond mere recognition and identification of particular persons. In a recently published study, researchers led by Michal Kosinski of Stanford Business School claimed that computerized facial analysis is also capable of determining a subject's political persuasion. To emphasize the privacy implications of existing technology, Professor Kosinski's study did not employ software specially designed to uncover political persuasion, but rather an "open-source facial-recognition algorithm." According to the study, based on a data set of more than a million faces—one-third of whom were nonwhite—the algorithm was able to correctly classify a participant as "liberal" or "conservative" with 70 percent accuracy, as compared with 55 percent for unassisted human guessing.

As commentators observed, the ability of technology to discern personality traits could enable some forms of prohibited discrimination by making it more subtle, allowing employers to use an algorithm rather than invasive interview questions to distinguish among job applicants. Whether or not one accepts that outward appearance may convey information about personality, one should expect legal controversies on this issue to arise as the enabling technology becomes both more available and more sophisticated.

RESOURCES

- NIST, U.S. Dep't. of Commerce Interagency/Internal Report No. 8280, *Face Recognition Vendor Test Part 3: Demographic Effects* (2019).
- Thorin Klosowski, "Facial Recognition Is Everywhere. Here's What We Can Do About It," *Wirecutter* (July 15, 2020).
- Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *N.Y. Times* (Jan. 18, 2020), at A1.
- Kristin L. Burge, "Growing Patchwork of Biometric Privacy Laws," *Litigation News* (Summer 2019).
- Michal Kosinski, "Facial Recognition Technology Can Expose Political Orientation from Naturalistic Facial Images," *Sci. Reps* (2021).
- Alfred Ng, "Clearview AI Says the First Amendment Lets It Scrape the Internet. Lawyers Disagree," *CNET.com* (Feb. 6, 2020).
- *ACLU et al. v. Clearview AI, Inc.*, No. 9337839 (Ill. Cir. Ct. filed May 28, 2020).
- Ethical Use of Facial Recognition Act, S. 3284, 116th Congress (2020).