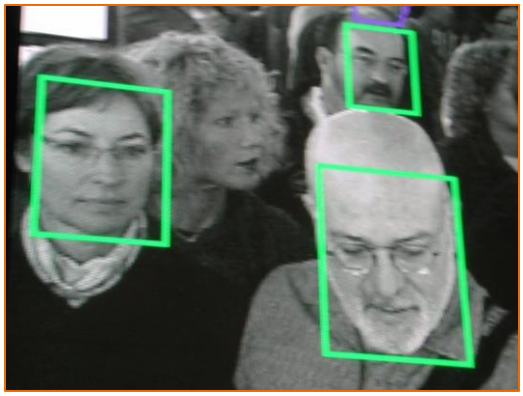
Facing the Challenges of Next Generation Identification: Biometrics, Data, and Privacy



Kent K. Barnes / CC BY 2.0

In 2011, the FBI signed a contract with the military developer Lockheed Martin to launch a pilot program called "Next Generation Identification" (NGI). This program was designed to utilize biometric data to assist the investigations of local and federal law enforcement agencies as part of anti-terrorism, anti-fraud, and national security programs. By late 2014, the program's facial recognition sector became fully operational and was used regularly by the FBI and other law enforcement agencies to aid in the identification of persons of interest in open investigations. This program compares visuals from surveillance cameras or other imaging devices with the world's largest database of photographs to find similarities in facial details and provide identification. When the program was first introduced, the FBI used biometric data from known and convicted criminals to compile the database. However, the database has since been expanded through a program run by the FBI's Criminal Justice Information Services (CJIS) called FACE (facial analysis, comparison, and evaluation), and now includes driver license photos from individuals that have been issued a photo ID from participating states.

Objections to the inclusion of driver license photos of law abiding citizens have been raised by many organizations, including the Government Accountability Office, the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center. This controversy primarily stems from the perceived lack of disclosure by the FBI over the specifics of the NGI and FACE programs, or the ability for citizens to agree to, or opt-out of, the use of their images. Senior Staff Attorney for the EFF, Jennifer Lynch, raised concerns about the implications of such technology, as well as its legal validity. She notes that "data that's being collected for one purpose is being used for a very different purpose." Lynch argues that due to facial recognition technologies, "Americans cannot easily take precautions against the covert, remote, and mass capture of their images," especially if they are not made aware that such capture and retention is taking place in the first place. These organizations argue that this goes against federal law (The Privacy Act of 1974) that states that images of faces are protected personal information and alters "the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant to show he is not who the system identifies him to be."

Those who are not worried about the NGI program or the inclusion of law-abiding citizens' photographs in the database say that biometric data, including a person's face, is no different than collecting a person's fingerprints, and that this information is crucial for national security. Such information has gained a renewed importance in light of recent terror attacks,

both domestically and abroad. Stephen Morris, the assistant director of the CJIS, states that "new high-tech tools like facial recognition are in the best interests of national security" and argues that it aids law enforcement officials in identifying and capturing terrorists and other criminals. The FBI also "maintains that it searches only against criminal databases" and that requests can be made to include other outside databases, such as various state and federal databases (including state driver license photo databases, and the Department of Defense passport photo database) if and when the FBI deems it necessary for a specific criminal investigation. This highlights the fact that facial recognition technology cannot be considered independently of the databases it uses in its search for more information about imaged persons of interest. Against those that call for more human oversight across database requests integral to facial recognition technology, Morris argues that those who think that "collecting biometrics is an invasion of folks' privacy" should instead be concerned with how to best "identify…the right person." How will our society face the conflicting interests at stake in the collection and use of biometric data in maintaining public safety and national security?

Discussion Questions:

1. What are the ethical values or interests at stake in the debate over using photo databases in the NGI program?
2. Do you believe the government can use databases not intended for biometric identification purposes? If so, what limits would you place on these uses?
3. As facial recognition technology gets more advanced, what sort of ethical limitations should we place on its use by government or private entities?
4. What would the ethical challenges be to using extremely advanced facial recognition technology in situations not concerning national security—such as online image searches?

Further Information:

Rebecca Boyle, "Anti-Fraud Facial Recognition System revokes the Wrong Person's License." *Popular Science*, July 18, 2011. Available at: www.popsci.com/gadgets/article/2011-07/anti-fraud-facial-recognition-system-generates-false-positives-revoking-wrong-persons-license

Eric Markowitz, "The FBI Now has the Largest Biometric Database in the World. Will it lead to more Surveillance?" *International Business Times*, April 23, 2016. Available at: www.ibtimes.com/fbi-now-has-largest-biometric-database-world-will-it-lead-more-surveillance-2345062

Sam Thielman, "FBI using Vast Public Photo Data and Iffy Facial Recognition Tech to find Criminals." *The Guardian*, June 15, 2016. Available at: www.theguardian.com/us-news/2016/jun/15/fbi-facial-recognition-software-photo-database-privacy

Authors:

Jason Head & Scott R. Stroud, Ph.D.
Media Ethics Initiative
University of Texas at Austin
April 17, 2018

www.mediaethicsinitiative.org