Super Bowl Surveillance

Facing Up to Biometrics

By
John D. Woodward, Jr.

RAND
ARROYO CENTER

For more information on RAND Arroyo Center, contact the Director of Operations (telephone 310-393-0411, extension 6500; FAX 310-451-6952; e-mail donnab@rand.org), or visit the Arroyo Center's Web site at http://www.rand.org/organization/ard/.

May 2001

RAND

1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138

1200 South Hayes Street, Arlington, VA 22202-5050

201 North Craig Street, Suite 102, Pittsburgh, PA 15213-1516

A large spectator event like the Super Bowl presents a prime target for terrorists. Fearing the potential for such an attack or other serious criminal incident, law enforcement officials in Tampa, Florida turned for help to a new technology: biometrics, the use of a person's physical characteristics or personal traits for human recognition. Digitized fingerprints, voiceprints, iris and retinal scans, hand geometry, and keystroke dynamics are all examples of this technology. The biometric system used at Super Bowl XXXV relied on facial recognition. Specifically, surveillance cameras surreptitiously scanned spectators' faces to capture images. Algorithms then measured facial features from these images—such as the distances and angles between geometric points on the face like the mouth extremities, nostrils, and eye corners—to produce a "faceprint." This faceprint was then instantly searched against a computerized database of suspected terrorists and known criminals to recognize a specific individual. A match would have alerted police to the presence of a potential threat.[1]

Should we be concerned about the government's use of this technology? One could argue that "facial recognition" is a standard identification technique and that it raises no special concerns. After all, we look at each other's faces to recognize one another. Police regularly use mugshots to identify criminals. And we think nothing of being asked to display "photo ID" to confirm our identity. On the other hand, the use of a biometric facial recognition system such as that employed at the Super Bowl is different in certain respects from these more familiar uses, and it has the

potential to present greater risks as well as greater advantages.

This issue paper describes the concerns raised by the use of biometric facial recognition, and it discusses how the technology could potentially threaten our right to privacy. The paper also discusses the technology's countervailing benefits to national security and law enforcement, and it concludes by offering policy recommendations to help maximize the technology's utility while minimizing its threat to our privacy.

Privacy Concerns of Current Uses

Biometric technologies may seem exotic, but their use is becoming increasingly common, and in 2001 *MIT Technology Review* named biometrics as one of the "top ten emerging technologies that will change the world." Biometric facial recognition, although it is far from foolproof and not yet technically perfected, is being used in a wide array of applications. For example, it is being used to control access to computers and facilities, replacing badges and passwords. The gaming industry relies on facial recognition as part of casino security to identify "card counters" and other undesirables. Check-cashing operations, traditionally plagued with high rates of fraud, are using facial recognition. Since 1998, the West Virginia Department of Motor Vehicles has been using the technology to check for duplicate and false driver's license registrations. The British use it to fight crime in places like Newham, England and to combat hooliganism at soccer games. The Israeli government uses facial recognition to automate the border-crossing process for workers entering Israel from Palestine. And in 1999, the Mexican government deployed a facial recognition system to eliminate duplicate voter regis-

tration in the presidential election. As the technology improves and becomes more cost-effective, its uses will expand.

Although the concept of recognizing someone from facial features is intuitive, facial recognition, as a biometric, makes human recognition a more automated, computerized process. It is this aspect of the use of biometrics that raises the fear that we are losing our ability to control information about ourselves—that we are losing our right to privacy.

Does the use of this technology violate legally protected privacy rights? Legal rights to privacy may be found in three sources: federal and state constitutions (if the entity invading your rights is a government actor), the common law of torts (if the entity invading your rights is a private actor), and statutory law.

Although the word "privacy" does not appear in the U.S. Constitution, the concern with protecting citizens against government intrusions into their private sphere is reflected in many of its provisions. For example, the First Amendment protects freedom of expression and association as well as the free exercise of religion, the Third Amendment prohibits the quartering of soldiers in one's home, the Fourth Amendment protects against unreasonable searches and seizures, the Fifth Amendment protects against self-incrimination, and the Due Process Clause of the Fourteenth Amendment protects certain fundamental "personal decisions relating to marriage, procreation, contraception, family relationship, child rearing, and education."[2] The constitutional "right to privacy" therefore reflects concerns not only for one's physical privacy—the idea that government agents cannot barge into one's home—

Does the use of this technology violate legally protected privacy rights?

but also for less tangible interests—the idea that citizens should be able to control certain information about themselves and to make certain decisions free of government compulsion. And the Supreme Court has cautioned that it is "not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[3]

The use of biometric facial recognition potentially implicates both types of privacy interests. Nevertheless, law enforcement's use of the technique at the Super Bowl does not appear to run afoul of the protections afforded by the U.S. Constitution.[4] Some civil libertarians argue that the sort of mass, dragnet scanning that took place at the Super Bowl is improper, and that law enforcement must have individualized, reasonable suspicion that criminal activity is afoot before it can "search" a subject's face to see if it matches that of a wanted individual in its database. Under current law, however, the type of facial recognition used at the Super Bowl would almost certainly be constitutional. The Supreme Court has explained that government action constitutes a search when it invades a person's reasonable expectation of privacy. But the Court has also found that a person does not have a reasonable expectation of privacy with regard to physical characteristics that are constantly exposed to the public, such as one's facial features, voice, and handwriting.[5] So although the Fourth Amendment requires that a search conducted by government actors be "reasonable," which generally means that there must be some degree of suspicion that the person to be searched is engaged in wrongdoing, the scan of spectators' facial

Some civil libertarians argue that the sort of mass, dragnet scanning that took place at the Super Bowl is improper.

characteristics at the Super Bowl did not constitute a search. And with respect to concerns about information privacy, if law enforcement officials limited their actions to simply comparing scanned images of people entering the stadium with their computer database of suspected terrorists and known criminals, then information privacy concerns would probably not arise so long as no information about individuals were retained, disclosed, or linked to any other database.

Potential Privacy Concerns as the Technology Advances

As the technology advances, however, particularly to the point that many facial recognition or other biometric databases become interlinked, then the threat to information privacy has the potential to increase significantly. With biometric facial recognition, the loss of information privacy essentially takes two forms: fears of tracking and clandestine capture. Tracking refers to the ability to monitor an individual's actions in real time or over a period of time. In its most extreme incarnation, tracking could become a kind of "super surveillance" that lets the tracker "follow" a person today as well as search databases to learn where he was months ago.

For example, suppose the authorities place me in their "watch list" database. As I go about my many daily tasks, surveillance cameras could capture my faceprint and digitally transmit this biometric information for instantaneous searching against the watch list. As I board the subway on my way to work, enter and exit my office building, stop by the ATM, make purchases in stores, visit my doctor, or attend a political rally, my faceprint will be matched with information in the database, allowing the surveiller to track

my movements. Similarly, the authorities can enter on their watch list the biometric information—the faceprints—of all those who attended the political rally with me. The authorities could then "reverse engineer" the identity of these individuals, by searching the database for their previous movements. If such a system were established, it would become possible to compile a comprehensive profile of an individual's movements and activities.

The theoretical possibility that the government could compile such massive databases, and that such databases could be used by law enforcement, raises the specter of "Big Brother" tracking its citizens' every move. The clandestine capture of biometric data increases these fears. As the above example makes clear, facial recognition systems can surreptitiously track individuals without their knowledge or permission. Moreover, the information from tracking can be combined with other personal data, acquired by other means (through, for example, a social security number), to provide even more insight into an individual's private life.

With biometric facial recognition, the loss of information privacy essentially takes two forms: fears of tracking and clandestine capture.

Whether such technological advances as the capability for "super surveillance" could render certain applications of this technology unconstitutional remains to be seen. If the compilation of information in these databases had a significant chilling effect on First Amendment rights, such as attending a political rally, if it impinged on fundamental rights of decisional privacy, or if the information were insufficiently safeguarded against unauthorized disclosure, then the

maintenance of such databases could potentially run afoul of the law.[6]

Given these potential concerns, civil libertarians are correct that we should be mindful of emerging technologies that may invade our privacy, and it is wise to monitor their development to forestall potential abuses. We should, however, also ensure that perceived or potential threats to our privacy do not blind us to the positive uses of biometric technologies like facial recognition.

Benefits of the Technology

At the Super Bowl, law enforcement used facial recognition as part of its efforts to prevent a terrorist act or other serious criminal incident. Although no suspected terrorists were apprehended, the authorities took prudent steps to identify them if they had chosen to show their faces. The national security community also understands the need for such precautions, and it believes that biometric facial recognition can help identify and protect against terrorist threats to U.S. forces and our embassies abroad.

Terrorist attacks have extracted a painful toll. For example, in Saudi Arabia in 1996, terrorists exploded a truck bomb near Building 131 of Khobar Towers. Nineteen service members died. Hundreds were injured. More recently, truck bomb attacks destroyed the U.S. embassies in Kenya and Tanzania, taking 224 lives and wounding some 4,600 others. And on October 12, 2000, a terrorist attack on the U.S.S. *Cole* in the Yemeni port of Aden killed 17 sailors and injured 42 more.

In the wake of the Khobar Towers terrorist attack, the Defense Advanced Research Projects Agency

(DARPA) embarked on a $50 million initiative known as "Human ID at a Distance," a major component of which is facial recognition. DARPA's ambitious goal is to help develop biometric technologies, like facial recognition, that can be deployed to identify a known terrorist before he closes on his target. In this way, lives can perhaps be saved.

The nation's political leadership has also recognized the potential of biometric technologies. Public Law 106-246, signed by President Clinton on July 13, 2000, included a provision making the Army "the Executive Agent to lead, consolidate, and coordinate all biometrics information assurance programs of the Department of Defense." On this basis, Deputy Secretary of Defense Rudy de Leon issued a memorandum on December 27, 2000, consolidating oversight and management of biometric technology under the recently created DoD Biometrics Management Office.

Similarly, while facial recognition did not lead to any arrests at the Super Bowl, there is evidence that using such a system can help deter crime. In Newham, England, the crime rate fell after police installed 300 surveillance cameras and incorporated facial recognition technology. While it is possible that the criminals only shifted their efforts to other locales, crime in Newham at least was deterred.

Moreover, the facial recognition system used at the Super Bowl was not physically invasive or intrusive for spectators. In fact, it was much less invasive than a metal detector at a public building or an inauguration parade checkpoint. In this sense, facial recognition helped to protect the privacy of individuals, who otherwise might have to endure more individualized police attention. One potential criticism is that the known criminals placed in the database may face

heightened police scrutiny once they are identified in a public setting, despite the fact that they have "paid their debt to society." One response to this concern is that known criminals already face heightened police scrutiny. For example, a prior criminal record has long been a standard screening tool when police are developing a list of suspects, and law enforcement routinely checks latent fingerprints found at a crime scene against databases containing fingerprints of those with prior criminal histories. In 1924, Congress authorized the Department of Justice to collect fingerprint and criminal record information from the states. The FBI's Criminal Justice Information Services Division currently has file holdings of fingerprint cards totaling over 219 million.

While there is also the danger that the biometric facial recognition system will make an incorrect match, that danger exists whether one is using facial recognition or traditional methods of identification such as comparing mugshots. Moreover, the potential for error is reduced when matches made by biometric facial recognition must subsequently be confirmed by law enforcement professionals. And as facial recognition technology improves, such misidentifications will most likely become rarer.

Facial recognition helped to protect the privacy of individuals, who otherwise might have to endure more individualized police attention.

The technological impartiality of facial recognition also offers significant benefit for society. While humans are adept at recognizing facial features, we also have prejudices and preconceptions. The controversy surrounding racial profiling is a leading example. Law enforcement officials searching for an African

American male sometimes stop far too many members of that group. Facial recognition systems do not focus on a person's skin color, hairstyle, or manner of dress, and they do not rely on racial stereotypes. On the contrary, a typical system uses objectively measurable facial features, such as the distances and angles between geometric points on the face, to recognize a specific individual. With biometrics, human recognition can become relatively "human-free" and therefore free from many human flaws.

Our efforts should focus on identifying potential dangers and addressing those concerns with specific safeguards.

While realizing that facial recognition has the potential to be misused in ways that could erode individual privacy, we must also acknowledge that this biometric technology has many positive uses as well. Super Bowl XXXV showcased its potential to help prevent terrorist acts and criminal incidents at high-profile events. Facial recognition can also have beneficial uses closer to home. As just one example, many parents would most likely feel safer knowing their children's elementary school had a facial recognition system to ensure that convicted child molesters were not granted access to school grounds.

Policy Recommendations

So while we must remain alert to potential abuses, it would be ill advised to decry the technology's use under all circumstances. Instead, our efforts should focus on identifying potential dangers and addressing those concerns with specific safeguards. As the above discussion demonstrates, one potential danger is function creep; that is, databases individually designed for a specific purpose, such as screening for suspected

terrorists at a large sporting event, could easily be interlinked with databases designed for other purposes, such as locating those who are delinquent on child support payments or have overdue library books. The interlinking and interoperability of massive databases could lead to several problems. The most serious of these potential problems is that much more private information is collected and revealed to the government entity than is necessary to achieve the purpose of the surveillance. And as a consequence, the damage caused by inadvertent disclosure or unauthorized access to the database is much greater.

To prevent the unnecessary growth and interlinking of databases, specific protocols should be established to govern what information is authorized to reside in the database. At a minimum, the government entity maintaining the database should provide an articulable reason why the information is needed, how long it needs to be retained in the database, and under what conditions the information may be disseminated or shared with others. To ensure the accuracy of the information compiled in the database, a clear set of standards should set forth the criteria for placing someone on a watch list, and the data should be reviewed periodically to purge outdated or inaccurate information.

To prevent unauthorized disclosures, strict controls to safeguard information should be required. The database should be made secure, access to it should be restricted, encryption and other technical measures should be used to thwart threats, records should be made of when, by whom, and for what purpose the database is accessed, and stiff criminal penalties should be available for unauthorized disclosure.

In addition to regulatory controls, it might be useful to explore less traditional methods to monitor this

technology. For example, as with any new technology, public understanding of its operation and uses may mitigate many of the fears about Big Brother. To that end, the government should be encouraged to use the technology openly, rather than clandestinely. Moreover, the government entity using biometric facial recognition should provide as much information as possible to the public about the technology's purposes and capabilities. Finally, some form of active oversight, either government only or a cooperative effort between government officials and private citizens, such as citizen oversight committees, would be useful not only to quell fears about the technology's use but also to ensure that it will not be abused.

As with any new technology, public understanding of its operation and uses may mitigate many of the fears about Big Brother.

Conclusion

Biometric facial recognition can provide significant benefits to society. At the same time, the rapid growth and improvement in the technology could threaten individual privacy rights. The concern with balancing the privacy of the citizen against the government interest occurs with almost all law enforcement techniques, however, and we should not let the fear of potential but inchoate threats to privacy, such as super surveillance, deter us from using facial recognition where it can produce positive benefits.

Biometric facial recognition is by no means a perfect technology, and much technical work has to be done before it becomes a truly viable tool to counter

terrorism and crime. But the technology is getting better and there is no denying its tremendous potential. In the meantime, we, as a society, have time to decide how we want to use this new technology. By implementing reasonable safeguards, we can harness its power to maximize its benefits while minimizing the intrusion on individual privacy.

NOTES

[1]See, for example, "And Now, the Good Side of Facial Profiling," by John D. Woodward, Jr., *Washington Post*, February 4, 2001; "Criminal Faces in the Crowd Still Elude Hidden ID Cameras," by Charles Piller et al., *Los Angeles Times*, February 2, 2001; "Super Day for Big Brother," *Los Angeles Times*, February 2, 2001; "Call It Super Bowl Face Scan I," by Declan McCullagh, *Wired News*, February 2, 2001; "Police Video Cameras Taped Football Fans," by Peter Slevin, *Washington Post*, February 1, 2001; and "Cameras Scanned Fans for Criminals," by Robert Trigaux, *St. Petersburg Times*, January 31, 2001. See also Thomas J. Colatosti, President and CEO, Viisage Technology, "Welcome to the 21st Century," speech delivered at Cyberposium 2001 TechShow, Harvard Business School, Boston, Massachusetts, February 10, 2001; Thomas J. Colatosti, "Computer Freedom and Privacy Conference 2001 Speech," delivered at Computer Freedom and Privacy Conference, Cambridge, Massachusetts, March 9, 2001; and "When Your Mole Betrays You," by Julia Scheeres, *Wired News*, March 14, 2001. (Tampa authorities used Viisage's facial recognition technology at the Super Bowl.)

[2]*Planned Parenthood of Southeastern Pennsylvania* v. *Casey*, 505 U.S. 833, 851 (1992).

[3]*Whalen* v. *Roe*, 429 U.S. 589, 605 (1977).

[4]States are free to provide greater privacy protections in their own state constitutions than those afforded in the U.S. Constitution. When evaluating the use of a specific biometric system, therefore, its legality must be analyzed under state constitutional provisions as well.

[5]*United States* v. *Dionisio*, 410 U.S. 1, 14 (1973).

[6]Given that constitutional protections are available only against actions by government agents, if this hypothetical "super surveillance" technology were used by a private entity—for example, a market research firm—then legal recourse could be sought under one of the common law privacy rights, such as the tort of intrusion upon seclusion or the tort of public disclosure of private facts. Under the scenario described here, in which surveillance would only track the location and activities of individuals in public, such surveillance would not appear to violate either of these common law privacy rights. Congress, however, could pass legislation aimed at directly regulating such practices.