Legal Memorandum
Published by The Heritage Foundation

No. 12
June 21, 2004

Biometric Technologies: Security, Legal, and Policy Implications

Paul Rosenzweig, Alane Kochems, and Ari Schwartz

Since September 11, 2001, there has been a great deal of interest in using biometrics for verification of identity.[1] The interest is particularly acute in the areas of visa and immigration documentation and government-issued identification card programs.[2] Unlike typical identification methods, which require a person to have something—an identification card, a personal identification number (PIN), or password—biometric information is part of a person. Since biometrics are so closely bound to a person, they are thought to be more reliable and not easily forgotten, lost, stolen, falsified, or guessed. This is because a biometric identifier relies on unique biological information about a person. This might be, for example, a 3-D image of the individual's hand, a scan of the person's iris, a fingerprint, or a voice print.

Biometrics can be used in two ways: for verification or for identification. When a biometric is used to verify whether a person is who he or she claims to be, that verification is frequently referred to as "one-to-one" matching. Almost all systems can determine whether there is a match between the person's presented biometric and biometric templates in a database in under one second.

Identification, by contrast, is known as "one-to-many" matching. In identification, a person's presented biometric is compared with all of the biometric templates within a database. There are two types of identification systems: positive and negative. Positive systems expect there to be a match between the biometric presented and the template. These systems are designed to make sure that a person is in the database. Negative systems are set up to make sure that a person is not in

Talking Points

- Advanced technology is a competitive advantage for the United States, and it must be used if the country is to win its war on terrorism.
- Biometric technologies—such as iris recognition, hand geometry, finger recognition, facial recognition, and voice recognition—have substantial potential to improve national security by providing a means to identify and verify people in many contexts.
- Although there is legitimate public concern over possible misuse, the technologies can and should be designed with appropriate protocols to ensure privacy.
- Appropriate protocols should include transparency, decentralization, voluntariness, and auditing to the extent practicable.

This paper, in its entirety, can be found at:
www.heritage.org/research/homelanddefense/lm12.cfm

Produced by the Center for Legal and Judicial Studies

Published by The Heritage Foundation
214 Massachusetts Ave., NE
Washington, DC 20002–4999
(202) 546-4400 heritage.org

Nothing written here is to be construed as legal advice on any matter, as an attempt to create an attorney-client relationship, or as an attempt to aid or hinder the passage of any bill before Congress.

the system. Negative identification can also take the form of a watch list, where a match triggers a notice to the appropriate authority for action.

Neither verification systems nor identification systems generate perfect matches. Instead, each comparison generates a score of how close the presented biometric is to the stored template. The systems compare the score with a predefined number or with algorithms to determine whether the presented biometric and template are sufficiently close to be considered a match.

Most biometric systems require an enrollment process in which a sample biometric is captured, extracted, and encoded as a biometric template. This template is then stored in a database against which future comparisons will be made. When the biometric is used for verification (e.g., access control), the biometric system confirms the validity of the claimed identity. When used for identification, the biometric technology compares a specific person's biometric with all of the stored biometric records to see if there is a match. For biometric technology to be effective, the database must be accurate and reasonably comprehensive.

This paper first considers some of the leading biometric technologies currently available—iris recognition, hand geometry, finger recognition, facial recognition, and voice recognition—and assesses their practical utility. It also describes match-on-card technology and the hazardous materials safety and security operation test, both of which integrate multiple biometric technologies into a system to provide additional security. The paper then examines the legal and political implications of using these technologies to provide security in a post-9/11 world.

Functionality and Effectiveness of Biometrics

Biometric technologies appear to be useful tools for identification and verification in security initiatives. Before implementing these technologies, one must consider whether biometric systems really work, whether they are sufficiently advanced to provide their touted capabilities, and their effectiveness. Accuracy, the possibility for deception, and user acceptance issues are also important considerations. It should be noted that the technologies can be difficult to compare—especially their cost—because they are often created for use in very different types of projects.

Iris Recognition

Iris recognition technology relies on the distinctly colored ring that surrounds the pupil of the eye. Irises have approximately 266 distinctive characteristics, including a trabecular meshwork, striations, rings, furrows, a corona, and freckles. Typically, about 173 of these distinctive characteristics are used in creating the template. Irises form during the eighth month of pregnancy and are thought to remain stable throughout an individual's life, barring injury.

These systems usually use a small camera to take a black-and-white, high-resolution image of the iris. Algorithms then define the boundaries of the iris and create a coordinate grid over the image. All the selected characteristics within the zones are then stored in a database as the individual's biometric template.

Iris recognition units—typically used to authorize physical access to a place—cost about $2,000 per unit. Putting together a comprehensive iris recognition system would cost far more, and involves hardware, software, and licensing costs.

Iris recognition technology is relatively easy to use and can process large numbers of people quickly. It is also only minimally intrusive. However, colored or bifocal contact lenses may hinder the effectiveness of the iris recognition system, as may strong eyeglasses. Glare or reflections can also be problematic for the cameras. In addition, people with poor eyesight occasionally have difficulty aligning their

[1] This paper is based on presentations given at a March 5, 2004, roundtable event of the same name sponsored by the Center for Democracy and Technology and The Heritage Foundation. For a detailed report on using biometrics for border security, see U.S. General Accounting Office (GAO), *Technology Assessment: Using Biometrics for Border Security* (GAO-03-174) (Nov. 14, 2002).

[2] *See* "Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism," Hearing before the Subcommittee on Technology, Terrorism and Government Information of the Senate Committee on the Judiciary, 107th Cong. 1st Sess. (Nov. 14, 2001).

eyes correctly with the camera. Finally, people who have glaucoma or cataracts may not be able to reliably use iris recognition technology.

The United Arab Emirates (UAE) has found iris recognition to be an effective overt security means for preventing expelled foreigners from re-entering the country. The UAE faced a situation in which an expelled foreigner would return to his or her home country and legally change his/her name, date of birth, and address—all descriptors traditionally used to screen individuals entering the country. Since the new identity would not be on any of the traditionally maintained, name-dependent lists, government agents would admit the banned individual to the UAE.

To counter this problem, the UAE began developing a biometric system that could be used to scan all individuals arriving in the country and determine whether the person is banned from entering. The UAE's specifications for the system included using a biometric that did not change over time; could be quickly acquired; was easy to use; could be used in real time; is safe and non-invasive; and which could be scaled in the millions. The UAE determined that iris recognition technology was the only technology that produced a single-person match in a sufficiently short period of time to meet its needs.

As of March 4, 2004, the UAE had enrolled 355,000 irises. It enrolls approximately 600 new irises per day. Over 6,220 expelled foreigners have been caught trying to re-enter the UAE, which averages to about 30 individuals caught per day. There have been over 1,613,000 searches of the database so far, with no false matches. A statistical analysis of the program suggests that the likelihood of a false positive match is less than 1 in 80 billion—in other words, effectively impossible.

The UAE has found iris recognition technology easy to use. There have been no failures to acquire an iris scan; the system is regularly used by people unfamiliar with or unskilled in the technology, and in transit areas. The UAE is now considering creating a unified Arab list. The country is also considering a similar system to identify all individuals. Currently, the UAE identity cards are smart cards that contain fingerprints, and the UAE is considering including a person's iris code in the near future. Iris codes may also be placed on passports. The UAE's experience with iris recognition technology is that biometrics enhance the nation's security.

Hand Geometry

Hand geometry relies on measurements of the width, height, and length of the fingers, distances between joints, and the shape of knuckles. Using optical cameras and light-emitting diodes that have mirrors and reflectors, two orthogonal, two-dimension images of the back and the sides of the hand are taken. Based on these images, 96 measurements are then calculated and a template created. Most hand readers have pins to help position the hand properly. These pins help with consistent hand placement and template repeatability, so there is a low false positive rate and a low failure to match rate.

Hand geometry readers usually cost between $2,000 and $4,000. Hand geometry is a mature technology primarily used for high-volume time-and-attendance and access control. For instance, both Krispy Kreme and McDonald's rely on hand geometry to record staff time and attendance. Hand geometry works well when many people need to be processed in a short period of time, so long as it is one-to-one matching. Although people's hands differ, they are not individually distinct. As a result, hand geometry technology cannot be used for one-to-many matching.

Hand geometry is perceived as very accurate and has been used in a variety of industries to regulate access control for more than 30 years. It is useful in identifying who is permitted somewhere or to do something and who is not. It is very difficult to spoof someone's hand shadow without the person's cooperation. The necessary information is not left behind physically (as, by contrast, a fingerprint often is), so that it is quite difficult to create a fake hand that would work on the unit without the enrolled person's knowledge. The technology is relatively stable—units placed in the field in 1991 are still working. The main change over the years has been in cost reduction. A wide variety of places rely on hand geometry for access. The San Francisco airport uses it for access to the tarmac; the port of Rotterdam, Scott Air Force Base, and a sorority at the University of Oklahoma also rely on it.

Most people are comfortable using the technology. Since it is an image of a hand as opposed to something more intrusive, most people consent to enrollment in the program. In addition, it is no less hygienic than touching a doorknob. (Indeed, acceptance of the technology by users has been made relatively easy by describing the hand geometry reader as a funny-looking doorknob.) Furthermore, people's unwillingness to accept hand geometry technology can be overcome if the individuals can see that they will get something in return. For instance, Gold's Gym uses the units for access, which allows its members to avoid the hassle of carrying keys or cards; the University of Georgia employs the technology for tracking meal plans. In the near future, Sea World annual pass holders will use hand geometry to enter the park. It is also used in approximately 15,000 banking applications.

Fingerprint Recognition

Fingerprint recognition technology is probably the most widely used and well-known biometric. Fingerprint recognition relies on features found in the impressions made by distinct ridges on the fingertips. There are two types of fingerprints: flat or rolled. Flat prints are an impression of only the central area of the finger pad while rolled prints capture ridges on the sides of the finger as well as the central portion between the tip and first knuckle.

Fingerprint images are scanned, enhanced, and then converted into templates. These templates are saved in a database for future comparisons using optical, silicon, or ultrasound scanners. Ultrasound appears to be the most accurate, but is rarely used. Optical scanners are the most commonly used.

According to a report by the U.S. General Accounting Office, fingerprint readers for physical access control cost approximately $1,000 to $3,000. There are also additional software licensing expenses of about $4/user. Smaller fingerprint scanners also have maintenance costs of 15 to 18 percent of their purchase price. The larger live-scan, 10-print readers run about $25,000 and have upkeep costs of about 14 percent of the reader's cost.[3]

Only a small percentage of people cannot be enrolled because their finger ridges have become dry, worn with age, or worn from using corrosive chemicals. There are, in addition, some people who are uncomfortable with this technology because of its relationship to forensic fingerprinting—certain cultures, for example, equate the taking of a fingerprint with identification as a criminal and resist its use as a biometric. There is also concern that fingerprints collected for one purpose could be used to track an individual's activities elsewhere. People occasionally complain about touching a scanner that many other people have touched, thinking it unhygienic. In addition, fingerprint biometric systems do not work everywhere; they are inappropriate, for example, in gloved environments like operating rooms in hospitals.

One area where fingerprint biometrics has been used is for identity and access management in health care (e.g., VA and teaching hospitals). The biometric technology is used to solve the challenge of how hospitals can give access to users and yet maintain security levels that provide confidence and comfort. This is a critical challenge, since greater security usually decreases access. There have been very few complaints about the technology in hospitals. People seemed comfortable with having their fingerprints stored in a database, since it was stored as a string of numbers rather than the actual digital image.

Facial Recognition

Face recognition technology identifies individuals by analyzing certain facial features such as the upper outlines of the eye sockets or sides of the mouth. Typically, facial recognition compares a live person with a stored template, but it has also been used for comparison between static images and templates. This technology works for both verification and identification. In addition, it is the only biometric system that can routinely be used in a covert manner, for surveillance, since a person's face is easily captured by video technology.

Facial recognition technology usually has a very low failure to enroll rate. However, reports the GAO, "the performance of facial recognition technology appears to depend on the operational setting and specific application. Pilots of facial recognition surveillance at airports have resulted in [failure to match rates] between 0.3 percent and 5 percent and [failure

[3] GAO, *supra* note 1, at 72.

to not match rates] between 5 percent and 45 percent."[4] Environmental factors have a great impact on these rates because variations in camera performance, facial position, expression, or features may hinder the algorithms when trying to match the presented face to a template. The age of the template can further degrade the ability for a correct match.

Facial recognition technologies can be very expensive. "A facial recognition server controlling access at a facility with up to 30,000 persons would cost about $15,000. Depending on the number of entrances installed with facial recognition devices, the cost of software licenses would range from about $650 to $4,500."[5] As the database size and number of attempted matches increases, so does the system's cost. In cases where closed-circuit television (CCTV) surveillance is used in conjunction with the facial recognition software, the costs for the CCTV range between $10,000 and $200,000 depending on the entrance size and the type of monitoring required. Additional CCTV cameras run between $125 and $500, reaching up to $2,300 for cameras with advanced features.

Voice Recognition

Voice recognition technology identifies people based on the differences in the voice resulting from physiological differences and learned speaking habits. When an individual is enrolled, the system captures samples of the person's speech as the individual says certain scripted information into a microphone or telephone multiple times. This information is known as a "pass phrase." (There are also biometric systems available that can distinguish between people's voices without requiring a predefined phrase.) The pass phrase is then converted to a digital format and distinctive characteristics (e.g., pitch, cadence, tone) are extracted to create a template for the speaker. Voice recognition templates require the most data space of all the biometric templates. Voice recognition technology can be used for both identification and verification.

Voice recognition technology requires minimal training for those involved. It is also fairly inexpensive and is very non-intrusive. The biggest disadvantage with the technology is that it can be unreliable and does not work well in noisy environments (like points of entry).

One example of where voice recognition systems might be used is the US-VISIT program. As one company has conceived in its proposal, an individual would be enrolled in a U.S.-managed database when applying for a visa at a U.S. consulate. The person would record his or her name and pass phrase then. Later, in the United States, local, state, or federal employees could use a telephone, cell phone, or the Web to verify if the individual is who he or she claims to be. Since visa holders would have gone through the process once when they received their visas, it should not be too difficult for them to repeat the process in the United States, even if they are not English speakers.

Biometric Match-on-Card Technology

Match-on-card technology can be used with virtually any biometric and usually takes the form of a smart card. The card has a biometric template (for example, a digitized and encoded fingerprint) stored in a computer chip. A live version of the fingerprint is then compared with the stored template for verification purposes. The technology's advantage is that it can be used as part of a network where the presented biometric is compared to a centralized database (e.g., the US-VISIT program), for comparison with local databases, or for an offline comparison between the presented biometric and the stored template on the card itself. Smart cards essentially act as the "issuer's security agent in the hands of the

[4] GAO, *supra* note 1, at 70. There are three main performance metrics when evaluating biometric technologies. They are false match rates (FMR), false nonmatch rates (FNMR), and failure to enroll rates (FTER). A false match means that the technology has incorrectly matched an identity to a presented biometric, and the FMR is the probability of the incorrect matches. Incorrect matches in a positive identification system mean that unauthorized people could gain access to resources or places to which they are not allowed. False nonmatches happen when the technology rejects a valid presented biometric. False nonmatches could mean that an authorized person is denied access to a place, where he or she is, in actuality, permitted. The FTER is the probability that an individual will not be able to be entered into the database. These failures can occur for different reasons including the inability to capture a sufficiently distinct sample or from system designs that inhibit consistent readings.

[5] GAO, *supra* note 1, at 71.

user." In addition, the security levels available are scalable. One could use the card and biometric, cards combined with PINs, cards with biometric templates used in conjunction with PINs. The proposed E-passport system now under development worldwide is a form of match-on-card technology.[6]

Biometrics for Securing Hazardous Material Transportation

The Department of Transportation has sponsored a project to examine commercially available technologies to protect transported hazardous materials from terrorist attack.[7] The test involves 100 trucks outfitted with an assortment of technologies, including biometric ones. The project will test whether these technologies can verify drivers; track vehicles and loads; alert the appropriate organizations and individuals about off-route or stolen vehicles, cargo tampering, and driver distress; and provide remote vehicle disabling in the event that terrorists successfully capture the vehicle.

This project uses biometric technologies for driver authentication. Smart cards and biometrics are used to confirm drivers' identities to shippers, consignees, and the drivers' vehicles. Smart cards holding predetermined, driver-specific information will be used in conjunction with fingerprint scanners to validate drivers' identities. These technologies will also record drop-off, pickup, and truck start-up events. This bio-login in the truck alerts dispatchers if an unauthorized person tries to operate the truck. Biometric and smart card technologies are also used to secure the shipping manifest system so that only authorized users can create or view the documentation for shipping the hazardous cargo or to access the loads themselves.

There have been only two device failures thus far. The biggest problem has been with driver impatience with some of the authentication procedures relying on information passed through satellites, which can be slow during heavy load periods.

Emerging Technologies

In addition to the mature technologies discussed above, researchers are also looking for other useful biometrics. Some of these emerging technologies include vein scans, facial thermography, DNA matching, odor sensing, blood pulse measurements, skin pattern recognition, nailbed identification, gait recognition, and ear shape recognition. Some of these biometrics, like vein scanning, are just becoming commercially available, while others, such as ear shape recognition, are recently started research projects.

Any organization interested in biometric safeguards must look carefully at its requirements and then choose the biometric and the relevant safeguards that meet those requirements. The organization must choose the level of security based on the threat. The more security used to prevent people from fooling the system, the greater the potential for false positives. For instance, if an organization wants to use a biometric for time and attendance, it is unlikely to care about whether the sample is alive. The threat is too minor for such security guards.

Legal and Political Implications

As the foregoing review suggests, the use of biometric technologies poses a host of interrelated policy questions, some of which are of general applicability to all biometric systems and others of which are technology- or use-specific. Among the questions one might ask are: Can the biometric system be narrowly tailored to its task? Who will oversee the program? What alternatives are there to biometric technologies? What information will be stored and in what form? To what facility/location will the biometric give access? Will the original biometric material be retained? Will biometric data be kept separately from other identifying personal information? Who will have access to the information? How will access to the information be controlled? How will the system ensure accuracy? Will data be aggregated across databases? If information is stored in a database, how will it be protected? Who will make sure that program administrators are responsive to privacy concerns? Can people remove themselves from a database voluntarily—in effect, can they "unenroll"? How will consistency between data

[6] *See* Ha Nguyen, Paul Rosenzweig & James Jay Carafano, "E-Passports: A Strategy for Long-Term Success," Heritage Foundation *Executive Memorandum* No. 921 April 13, 2004.

[7] *See www.safehazmat.com* or *www.fmcsa.dot.gov/safetprogs/fot/index.htm* for more information on the Hazardous Materials Safety and Security Operational Test.

collected at multiple sites be maintained? If there is a choice, will people be informed of optional versus mandatory enrollment alternatives?

These are difficult questions—ones that a paper of this nature cannot comprehensively answer. We offer, however, the following preliminary thoughts as a framework for answering these questions.

First, and foremost, we are convinced of the utility of biometric identification as a general matter. Biometric technologies have substantial potential to improve national security by providing a means to identify and verify people in many contexts. In many circumstances they will provide a substantially higher level of security beyond current means of identification. This will be of especial utility in controlling access to areas where security risks are especially high—airport tarmacs, critical infrastructure facilities, and the like.

At the same time, however, as with any other new technology, there is the potential for abuse. Thus, there is legitimate public concern that biometric technology can be misused to invade or violate personal privacy or other civil liberties. Some of the fears surrounding biometric information include that it will be gathered without permission, knowledge, or clearly defined reasons; used for a multitude of purposes other than the one for which it was initially gathered (function creep); disseminated without explicit permission; used to help to create a complete picture about people for surveillance or social control purposes. There are also concerns about tracking, which is real-time or near–real-time surveillance of an individual, and profiling, where a person's past activities are reconstructed; both of these would destroy a person's anonymity.[8] There are also concerns about identity fraud.

In light of these and other similar fears, some conclude that the technology should not be developed at all. But given the very serious terrorist threat that we face, if biometric technology is proved to enhance security in a particular context and appropriate safeguards can be put in place, we believe it is worth pursuing.

Some critics of biometrics believe that liberty derives from anonymity,[9] while supporters are of the view that proper security is dependent on complete identification and that liberty would in no way be put at risk.[10] Yet, instead of depending solely on anonymity or full identification, Americans would be better served by a range of authentication solutions that fit the context of the interaction between government and individual.

Anonymous political speech remains an important ideal for maintaining liberty, yet—outside of this specific realm—anonymity is a different, and possibly weaker, form of liberty. The American understanding of liberty interests necessarily acknowledges that the personal data of those who have not committed any criminal offense (such as biometric data) can be collected for legitimate governmental purposes. On the other extreme, liberty could be put at risk if biometric data were required for even the smallest interaction with the government, such as using a government public Web site.

It is important to note that between complete anonymity and full identity there are gradations. Many transactions with government can be accomplished without requiring detailed personal information, though they would not be completely anonymous. In fact, we already have the beginning of a graduated understanding of identification; there is a spectrum of authentication and personal identification solutions available to the government.[11] In a transaction where no identifying information about the individual is necessary, but actual authentication is needed—for example, for use in an ongoing govern-

[8] *See,* for instance, Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society* (Washington, D.C.: ACLU Technology and Liberty Program, Jan. 2003).

[9] *See* Phillip Kurland, "The private I," *The University of Chicago Magazine*, Autumn 1976, p. 8 (characterizing three facets of privacy, broadly characterized as anonymity, secrecy, and autonomy), *quoted in Whalen v. Roe*, 429 U.S. 589, 599 n. 24 (1977).

[10] *See* Alan Dershowitz "Why Fear National ID Cards?" *The New York Times,* Op-Ed, October 18, 2001.

[11] The General Services Administration recently recognized this fact when establishing "Levels of Trust" for E-Authentication. Importantly, the GSA levels include the ability for government to allow individuals to be authenticated pseudonymously. *See* OMB Memo 04-04 to Federal Agencies *http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf*

ment research study—a lower level of authentication will be required. By contrast, in cases where the actual identity is not important, but identifying information is necessary—for example, in accepting online regulatory compliance filings from a company— a higher level will be needed.

What these examples demonstrate is not so much that our conception of liberty is based upon absolute privacy expectations,[12] but rather that any government impingement on our liberty will occur only with good cause. We must be able to voice controversial political viewpoints with the expectation that the government will only investigate those that truly may threaten national interests. When a criminal or terror investigation is underway, we must be able to expect that the spotlight of scrutiny will not turn upon us individually without some good reason. However, most interactions with the government fall somewhere in between expectations of complete anonymity and a detailed investigation. We must be able to continue to expect that government will ensure that any possible impingement on liberty is commensurate to the interaction with the individual and that the government has the technological tools to achieve this. If there is no true spectrum of authentication choices (from anonymity to pseudonymity to full identity) for use, all expectations of privacy will erode simply because government will be forced to treat every interaction as investigative.

In many ways, the implementation of new laws and systems to combat terror are not an unalloyed diminution of privacy. Rather, the laws and practices can substitute one privacy intrusion (for example, a search of electronic biometric data about an individual) for another privacy intrusion (the physical intrusiveness of body searches before entry into a facility). But this means that legal analysts cannot make broad value judgments—each person weighs the utility of their own privacy by a different metric. For many Americans, the price of a little less biometric privacy might not be too great if it resulted in a little more physical privacy in certain circumstances; for others, the opposite result might hold in that same instance. Reasonable people can disagree about when biometric technology should be used, but taking a position that any use of biometric technology is privacy invasive is like suggesting that biometrics should be used in every transaction. The true policy challenge is in finding the most effective uses of the specific biometric technology—both for liberty and security—not in labeling it as universally good or evil.

In properly determining how best to enhance both liberty and security, it is useful, therefore, to have some basic principles for assessing a particular biometric technology. Such a code of principles ought to include the following:

- Enrollment in biometric systems should be overt instead of covert. Before one is "enrolled" in a biometric program one should be made aware of that enrollment. Thus, we are skeptical of biometric programs, such as public facial recognition, that permit the surreptitious capture of biometric data.
- Biometric systems are better used for verification rather than identification. In general, that is, they are better suited for a one-to-one match assuring that the individual in question is who he says he is and has the requisite authorization to engage in the activity in question. Biometrics are both less practically useful, and more problematic as a matter of policy, when they are used in a one-to-many fashion to pierce an individual's anonymity without the justification inherent in, for example, seeking access to a particular location.
- Biometric systems should be designed to operate with local storage of the data (e.g., on-card templates) rather than with central storage. Centralized storage of biometric data raises privacy concerns and also tends to permit more ready mission creep.[13] Clearly for some technologies and applications local storage will not be feasible—but to the extent it is practicable, local storage should be preferred.
- Similarly, we should prefer biometric systems that are "opt in" and require a person to consent,

[12] *But cf. Lawrence v. Texas*, -- U.S. --. 123 S.Ct. 2472 (2003) (recognizing that certain intrusions into individual privacy are beyond governmental power).

[13] As a consequence, we also support the need for legislative authorization for many biometric uses. This additional requirement will serve as a bulwark against mission creep.

rather than those that are mandatory. By this we do not mean that requiring one to opt in cannot be made a condition of participation (e.g., if you want to enter the United States you must provide a biometric) since participation is ultimately voluntary. And we also recognize that certain biometric applications (e.g., DNA for convicted terrorists) may need to be mandatory. Again, however, this should be an exception to the general rule of voluntariness.

- For privacy and security reasons, one should prefer biometric systems that reduce the biometric to a template, rather than maintaining a stored image. Generically, templates are harder to falsify. Images, however, may be somewhat easier to encrypt. In the end, the choice will very much depend on the application.
- Similarly, where feasible, biometric systems should consider the use of forms of verified pseudonymity, where the authorization for use by the identified individual is conveyed while the identity is concealed unless and until suitable authorization for piercing the veil of anonymity is received.
- Any biometric system should have strong audit and oversight programs to prevent misuse. The Privacy Act of 1974 addresses some of these concerns since it limits the ability of federal agencies to collect, use, or disclose personal information like biometric data. There are, however, exceptions for national security and law enforcement purposes. Recourse to those exceptions should be well-documented and subject to periodic review.
- Any biometric system is only as strong as the initial enrollment system. An ideal way to evade biometric detection is to be improperly registered as a legitimate user. Thus, in conjunction with the deployment of any new biometric system, one must take care to monitor, audit, and periodically test the enrollment process. Enrolled data should also be subject to routine secondary review to identify those mistakenly enrolled in the first instance.
- Similarly, a biometric system is only as strong as its back-up alternative. The principle of layered security requires that those implementing biometric identification systems have in place a suitable secondary identification system for use when the primary biometric system fails or provides an inconclusive result, It will not do, for example, for the back-up to a biometric system to be a simple, insecure, signature verification.

In the end, biometric technologies can be privacy-neutral. They can and should be designed with appropriate protocols to ensure privacy before they are implemented. Those protocols can both be part of the hardware (and thus designed into the system) and enhanced through operational guidelines and systems oversight that address privacy concerns.

Advanced technology is a competitive advantage for the United States, and it must be used if the country is to win its war on terrorism. Indeed, resistance to new technology poses practical dangers. As the Congressional Joint Inquiry into the events of September 11 pointed out in noting systemic failures that played a role in the inability to prevent the terrorist attacks:

> 4. Finding: While technology remains one of this nation's greatest advantages, it has not been fully and most effectively applied in support of U.S. counterterrorism efforts. Persistent problems in this area included a lack of collaboration between Intelligence Community agencies [and] *a reluctance to develop and implement new technical capabilities aggressively* ....[14]

The development and implementation of biometric systems with appropriate safeguards will help avoid repeating this mistake.

Conclusion

The implementation of biometric technologies for increasing national security raises numerous practical and policy questions. It is critical that the right type of technology is chosen to meet the purpose and privacy requirements of a specific use. In order

[14] *Report of the Joint Inquiry Into the Terrorist Attacks of September 11, 2001*, House Permanent Select Committee on Intelligence and Senate Select Committee on Intelligence, 107th Cong., 2nd Sess., S. Rept. No. 107–351 and H. Rept. No. 107–792, Dec. 2002, p. xvi (available at *http://www.fas.org/irp/congress/2002_rpt/911rept.pdf*) (emphasis supplied).

for biometric systems to provide security, it is necessary that people not have a false sense of security about them. The weaknesses and flaws of the technologies must be acknowledged and countermeasures need to be considered. The systems cannot be seen as the ultimate security tool, and thus the perfect solution. Rather biometrics (in one layer, or many) are simply another tool in a layered approach to security. They are not a panacea—but they can play an important role in protecting America and should not be demonized as unacceptable technology.

—Paul Rosenzweig is Senior Legal Research Fellow in the Center for Legal and Judicial Studies at The Heritage Foundation and Adjunct Professor of Law at George Mason University School of Law. Alane Kochems is an independent researcher affiliated with The Heritage Foundation. Ari Schwartz is Associate Director of the Center for Democracy and Technology.