What Is Privacy in the Context of Biometrics?

The issue of privacy is central to biometrics. Critics complain that the use of biometrics poses a substantial risk to privacy rights. Proponents claim that biometrics protect privacy. Evaluating these arguments requires, in the first instance, an understanding of what privacy means. In this chapter we explore the definition of privacy in general.

Working Definition of Privacy

We all might have strong subjective ideas about what privacy is. Yet, the word "privacy" is hard to define, in part because the meaning depends greatly on the situation, culture, environment, and moment. In the immediate aftermath of September 11, for example, many Americans welcomed more intrusive governmental measures to increase public safety, even though that meant their privacy could suffer. As one New Yorker put it, "I want Big Brother on my shoulder, looking out for me." Pre-September 11, a frequent question asked at "Introduction to Biometrics" seminars was, "What about the privacy concerns?" Post-September 11, the more frequently asked question became, "What about the security aspects?"

Privacy scholar Ruth Gavison sees privacy as consisting of three parts: secrecy, anonymity, and solitude. She offers what is perhaps the extreme privacy model: "Privacy is a limitation of others' access to an individual.... In perfect privacy no one has any information about X, no one pays any attention to X, and no one has physical access to X" (Gavison 1980, 428).

Robert Ellis Smith, the editor of *Privacy Journal*, defines privacy as "the desire by each of us for physical space where we can be free of interruption, intrusion, embarrassment, or accountability and the attempt to control the time and manner of disclosures of personal information about ourselves" (Smith 2000, 6/ Smith 2002, 1–8). This definition hints at three types of privacy recognized by U.S. courts: physical, decisional, and information privacy.

Based on her survey of the extensive privacy literature, however, Professor Lillian R. Bevier concluded that "privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name" (Bevier 1995, 458).

Most important from the standpoint of biometrics, privacy includes an aspect of autonomy—as various scholars have expressed it: our control over information about ourselves, control over who can sense us, or control over the intimacies of personal identity. This control over information about us, or what is termed "information privacy" (or "informational privacy"), lies at the heart of the privacy concerns raised by this new technological reality. Individuals have an interest in determining how, when, why, and to whom information about themselves, in the form of a biometric identifier, would be disclosed.

What Privacy Concerns Does the Use of Biometrics Implicate?

With this working definition of privacy in mind, we next discuss the privacy concerns implicated by the use of biometrics. These concerns relate to identification and invasiveness.

The Individual Gives Up a Biometric Identifier

To determine the specific privacy concerns implicated by biometrics, we must first focus on what exactly is disclosed when biometric data is collected. Regardless of whether an individual voluntarily provides a biometric identifier or is forced to surrender it as part of state action or government-required scheme, he is giving up information about himself. When biometrics, like fingerprinting, iris recognition, or retinal scanning is used, he discloses robust and distinctive information about his identity. When other biometrics, such as hand or finger geometry, are used, at a minimum, he discloses accurate information about who he is. Depending on the biometric, he is giving information about himself that could be used to identify him over large-scale databases.

Invasive Aspects of the Information

Beyond this fundamental disclosure, invasive implications might also be related to privacy concerns that stem from the biometric identification information disclosed. These invasive implications for privacy are essentially three-fold:

- The invasive effects of a secondary market, defined as disclosure of the biometric identification information to third parties
- Any invasive information that might be additionally obtained as part of the biometric identifier
- The invasiveness that might be associated with actual physical harm caused by the technology

Invasive Secondary Market Effects Once a biometric identifier is captured or collected from an individual in the primary market, and even if it is captured only once, the biometric identifier could easily be replicated, copied, and otherwise shared among countless public and private sector databases. This sharing in a secondary market could conceivably take place without the individual's knowledge or consent. Indeed, biometric identifiers could be bought and sold in a secondary market much the way names and addresses on mailing lists are currently bought and sold by data merchants.

An example illustrates the secondary market effect: I give my face and fingerprints to my local sports club so I can access the club and keep better track of my workouts. I do this by presenting my face to a camera whenever I enter and by touching my finger to the computer display on the treadmill and other equipment. I get a detailed monthly fitness report. The sports club conveniently enrolled both of my index fingers so I don't even have to remember which pointer

finger to use. After a while, I start receiving marketing information telling me to show up at the local grocery store, retail outlet, and so on, because I am already preregistered and biometrically enrolled in their systems. That's because, along with my facial photograph, the sports club kept my raw data, or file images, in addition to the fingerprint templates, and sold the information to others.

Later, while shopping in the mall, sales associates insist on selling me athletic gear, protein supplements, and diet aids because their facial recognition system identified me as a failed jock from the sports club. Later, the police are confronted with the grisly homicide of the sports club manager in his office, where the only evidence is a single latent print left on the murder weapon. After no matches are made against the FBI's criminal master file, the new sports club management readily agrees to turn over the file images of fingerprints of all its members, including mine, so the latent print can be searched against them.

Particularly with respect to the private sphere, where the conduct of private actors has traditionally been given a large degree of freedom of action from government interference, few current legal limits exist in the United States on the use of biometric information held by private actors. This observation is not meant to suggest that the federal or state governments would not be able to regulate the use of biometric information held by private actors; rather, it emphasizes what the present regulatory baseline is with respect to the regulation of biometric information: Until regulatory action has been taken by government, the use of biometrics is left to the market. The legal situation is very different in the European Union, where a comprehensive privacy protection framework exists.

Invasive Information Is Obtained In addition to the identification information associated with the biometric, invasive information threatening privacy could conceivably include three other types of concerns. First, biometric identifiers could be used extensively for law enforcement purposes, as raised in the sports club example. Fingerprints have long been used by law enforcement, and electronic finger images—or what are in effect the next generation of fingerprints—are presently being used by various law enforcement agencies as part of their databases, such as the FBI's Integrated Automated Fingerprint Identification System (IAFIS).

Second, it is possible (and this point needs to be stressed: *only* possible) that some biometrics might capture more than just mere identification information. Information about a person's health and medical history might also be incidentally obtained. Recent scientific research, while the subject of controversy, suggests that fingerprints might disclose such information about a person. For example, Dr. Howard Chen, in his work on dermatoglyphics, or the study of the patterns of the ridges of the skin on parts of the hands and feet, notes that "certain chromosomal disorders are known to be associated with characteristic dermatoglyphic abnormalities," specifically citing Down syndrome, Turner syndrome, and Klinefelter syndrome as chromosomal disorders that cause unusual fingerprint patterns in a person. Certain nonchromosomal disorders, such as chronic, intestinal pseudo-obstruction (CIP) (described in the next paragraph),

leukemia, breast cancer, and Rubella syndrome, have also been implicated by certain unusual fingerprint patterns.

Dr. Marvin M. Schuster, the recently retired director of the division of digestive diseases at Johns Hopkins Bayview Medical Center, has discovered a "mysterious relationship" between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called CIP that affects 50,000 people nationwide. Based on the results of a seven-year study, Dr. Schuster found that 54 percent of CIP patients have this rare digital arch fingerprint pattern. In comparison, arch fingerprints appear in only seven percent of the general population. Schuster's discovery suggests a genetic basis to the disease. Schuster explained that in the case of CIP, "the more digital arches there are in the fingerprint, the stronger the correlation [to the condition]. The majority of CIP patients possess at least one digital arch. This discovery offers an important clue in diagnosing CIP, and it suggests that the disorder is congenital. It could potentially save people with CIP from multiple needless operations" (Hancock and Hendricks 1996).

While still extremely controversial within the scientific communities, several researchers report a link between fingerprints and homosexuality. For example, psychologists at the University of Western Ontario report that homosexual males are more likely than their heterosexual counterparts to show asymmetry in their fingerprints. "What we found is a statistically significant difference between groups of heterosexual and homosexual men," researcher Doreen Kimura said (Associated Press 1994). While this research is far from conclusive, the availability of such information with its possible links to medical and related information again raises concern about privacy and can create misperceptions.

From examining the retina or iris, an expert can determine that a patient may be suffering from common afflictions such as diabetes, arteriosclerosis, and hypertension; furthermore, a medical professional can also detect unique diseases of the iris and the retina. Moreover, the onset of certain diseases (such as diabetes) and conditions (such as pregnancy) may cause the retinal pattern to change; are the changes enough to cause a previously enrolled user to be rejected by a system because the user's biometric is no longer recognized by the system? Although both the iris and retina contain medical information, it is by no means obvious that the biometric data taken of the iris or retina implicates privacy concerns related to the disclosure of medical information. A necessary area of further technical inquiry is whether the computerized code taken of the iris or retina actually contains any medical information or if the information captured is sufficient to be used for any type of diagnostic purpose.

Much research remains to be done; however, a biometric identifier with any possible links to medical information will raise lingering questions about the privacy aspects of the information disclosed. More important, the mere perception that such sensitive information may be disclosed could dissuade people from using potentially beneficial biometric systems.

Actual Physical Harm; Physical Invasiveness Part of the "urban legend" surrounding biometrics holds that retinal scanning "shoots a laser beam into the eye." This is not the case, but urban legends die hard. Anecdotally, certain aviators, who are extremely proud of their 20/20 vision, supposedly had a hard time accepting retinal scanning devices in an experimental program because at least some of them feared the devices would adversely affect their perfect vision. Other users feared that diseases, such as conjunctivitis, may result from having to come into close proximity with a binocular-like device that strangers had touched. Some users of biometrics have complained that hand geometry systems dry their hands. Such fears, even when unfounded, can negatively affect the system because dissatisfied users will go out of their way not to cooperate with the system; some may even actively engage in acts of sabotage to prevent its use.

Documented cases of biometrics causing actual harm to a person are difficult, if not impossible, to find, but many of the technologies are fairly new. And to date, no enterprising plaintiff's attorney has brought a class-action lawsuit for personal injury on this biometrics-induced harm basis. The bottom line is that any liability resulting from any proven actual physical harm caused by biometric systems would be addressed by the individual state's tort liability regimes. On a related note, eventually, the judiciary will also have the opportunity to decide the admissibility of biometric identification as scientific evidence using the prevailing standards articulated by the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals* in 1993.

Biometrics as Privacy's Foe: Criticisms of Biometrics

This section discusses the "foe" side of the coin: the criticisms of biometrics leading to loss of anonymity and autonomy and the "Big Brother" scenario, including the danger of function creep and degradation of the individual's reasonable expectation of privacy.

The Loss of Anonymity; the Loss of Autonomy

A basic criticism of biometrics is that we, as individuals, risk losing our anonymity and autonomy whenever biometric systems are deployed. Part of controlling information about ourselves includes our ability to keep other parties from knowing things about us, like who we are. While we all know that a determined party—whether the government or a private party—can learn our identity (and much more about us), the use of biometrics makes it clear that our identity is now fully established within seconds. As Roger Clarke explains, "The need to identify oneself may be intrinsically distasteful to some people.... They may regard it as demeaning, or implicit recognition that the organization with whom they are dealing exercises power over them" (Clarke 1994).

Robert Ellis Smith agrees, noting that, "In most cases, biometric technology is impersonal" (Smith 1996). At the same time, as the technology improves, its use may become more ubiquitous, and individuals may find that they are required to provide a biometric identifier in unexpected, unwelcome, or unforeseen circumstances. Moreover, you cannot simply "make up" a biometric as you can a name, an address, or a phone number. In this sense, perhaps, the loss of anonymity leads to an inevitable loss of individual autonomy.

Biometrics should not really be blamed for the fact that there is less individual anonymity in society today than in decades or centuries past, however. Rather, far larger economic, political, and technological forces have been at work. America's transformation from an agrarian to industrial to post-industrial service (or "information age") economy, combined with the massive growth of government since the New Deal of the 1930s, have put a greater premium on the need for information about individuals and organizations. At the same time, technical advances have made it much easier and more convenient to collect, compile, and keep extensive information on individuals. This information-centric trend takes place because in the Information Age information has great value as a commodity. The computer, the enabler of "info-centrism," has helped make information a valuable commodity because it can process large amounts of personal information from large numbers of people in little time and at low cost.

While a biometric identifier is an accurate identifier, it is not the first nor the only identifier used to match or locate information about a person. Names and numerical identifiers such as social security numbers, account numbers, and military service numbers have long been used to access files with personal information. Moreover, the impressive search capabilities of computer systems with their abilities to search, for example, the full text of stored documents, make identifiers far less important for locating information about an individual.

We also should not lose sight of the fact that there is usually a good reason why individual recognition in the form of identification or verification is needed. Balancing the equities involved and depending on the case, the benefits—to the individual as well as to society—of establishing a person's identity generally outweigh the costs of losing anonymity. For example, given the massive problem of missing and abused children, many citizens would eagerly support the idea of day care providers using biometrics to make certain that our children get released at the end of the day to a parent or guardian whose identity has been verified. However, reasonable people can disagree as to the cost-benefit analysis.

Similarly, to consider a "pocketbook" example, the world's financial community has long been concerned about growing problems of ATM fraud and unauthorized account access, estimated to cost $500 million a year, check fraud at least $2 billion, and credit card fraud about $1.5 billion per year. The financial services industry believes that a significant percentage of these losses could be eliminated by the use of biometrics, by ensuring that only the authorized account

holder could access the account. MasterCard, for example, has been evaluating various biometrics since 1995 and believes fingerprint technology is the best technology to reduce credit card fraud. According to Joel Lisker, the company's senior vice president of security and risk management, "We estimate that a fingerprint system, fully implemented, could save the financial services industry billions of dollars" (Haapaniemi 1998).

Critics give too much credit to biometrics' alleged ability to erode anonymity without giving enough attention to the market's ability to protect privacy in response. It is not obvious that more anonymity will be lost when biometrics are used. Public and private sector organizations already have the ability to gather substantial amounts of information about individuals by tracking, for example, credit card use, consumer spending, and demographic factors.

A parallel to the financial services industry might be helpful. Despite the existence of many comprehensive payment systems such as credit cards, which combine extreme ease of service with extensive record-keeping, many Americans still prefer to use cash for transactions—a form of payment that leaves virtually no record. An individual who wants anonymity might have to go to greater lengths to get it in the biometric world, but the ability of the marketplace to accommodate a person's desire for anonymity should not be so readily dismissed. Moreover, as explained next, the ability of biometrics to serve as privacy enhancing technologies should not be discounted.

The Biometric-Based "Big Brother" Scenario

Aside from the alliterative qualities the phrase possesses, critics of biometrics seem to inevitably link the technology to "Big Brother." Biometrics, in combination with impressive advancements in computer and related technologies, would, its critics argue, enable the State to monitor the actions and behavior of its citizenry. In this vein, concern has been expressed that biometric identifiers will be used routinely against citizens by law enforcement agencies. As Marc Rotenberg of the Electronic Privacy Information Center has succinctly explained, "Take someone's fingerprint and you have the ability to determine if you have a match for forensic purposes" (American Banker 1996).

This "Big Brother" concern, however, goes beyond normal police work. Every time an individual used her biometric identifier to conduct a transaction, a record would be made in a database that the government, using computer technology, could then match and use against the citizen—even in ways that are not authorized or meet with our disapproval. To borrow the reasoning of a 1973 report on national identity card proposals, the biometric identifier, in ways far more effective than a numerical identifier, "could serve as the skeleton for a national dossier system to maintain information on every citizen from cradle to grave" (U.S. Department of Health, Education and Welfare 1973).

Roger Clarke has perhaps offered the best worst-case *1984*-like scenario:

> Any high-integrity identifier [such as biometrics] represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the State, and the scope for nonconformism and dissent would be muted to the point envisaged by the antiutopian novelists (Clarke 1994).

At least one example exists from U.S. history of supposedly confidential records being used in ways never likely intended. In November 1941, almost two weeks before the Japanese attack on Pearl Harbor, President Franklin D. Roosevelt ordered a comprehensive list made to include the names and addresses of all foreign-born and American-born Japanese living in the United States. To compile the list, staffers used 1930 and 1940 census data. Working without the benefit of computers, staffers compiled the list in one week. Following the attack, President Roosevelt issued Executive Order 9066, authorizing military personnel to detain and relocate persons of Japanese ancestry. By the spring of 1942, the U.S. government forced persons of Japanese descent, including U.S. citizens, to relocate from their homes on the West Coast and report to relocation centers. An estimated 120,000 people, many of whom were U.S. citizens, were held without judicial review. John Miller and Stephen Moore, two libertarian scholars, contend, "The history of government programs indicates that privacy rights are violated routinely whenever expediency dictates" (Miller and Moore 1995).

Function Creep

The biometric-based "Big Brother" scenario would not happen instantly. Rather, when first deployed, biometrics would be used for limited, clearly specified, sensible purposes—to combat fraud, to improve airport security, to protect our children, and so on. But consider what Justice Louis Brandeis (of "right to privacy" fame) warned in his famous *Olmstead v. United States* dissent of 1927:

> Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well meaning but without understanding.

What would inevitably happen over time, according to civil libertarians, is a phenomenon known as "function creep" or "mission creep": identification systems incorporating biometrics would gradually spread to additional purposes not announced or not even intended when the identification systems were originally implemented.

The classic example of function creep is the use of the Social Security Number (SSN) in the United States. Originated in 1936, the SSN's sole purpose was to

facilitate record-keeping for determining the amount of Social Security taxes to credit to each contributor's account. In fact, the original Social Security cards containing the SSN bore the legend, "Not for Identification." By 1961, the Internal Revenue Service (IRS) began using the SSN for tax identification purposes. By 2002, countless transactions from credit to employment to insurance to many states' drivers licenses require a Social Security Number and countless private organizations ask for it even when it is not needed specifically for the transaction at hand. From "Not for Identification," the SSN has become virtual mandatory identification.

Moreover, given the consequences of function creep, the size, power, and scope of government will expand as all citizens get their biometric identifiers thrown into massive government databases by the "men [and women] of zeal, well-meaning but without understanding" about whom Justice Brandeis warned. In effect, an old Russian proverb aptly identifies the danger of biometrics for freedom-loving Americans: "If you are a mushroom, into the basket you must go."

Reduction of the Individual's Reasonable Expectation of Privacy

Just as function creep implies that biometrics will gradually (and innocently) grow to be used by zealous, well-meaning bureaucrats in numerous, creative ways in multiple forums, function creep will also enable the government to use the new technology of biometrics to reduce further over time the citizenry's reasonable expectations of privacy.

Analogies can be drawn from previous cases in which the government has used cutting-edge technology to intrude in an area in which the private actor had manifested a subjective expectation of privacy. For example, the Environmental Protection Agency (EPA), in an effort to investigate industrial pollution, used "the finest precision aerial camera available" mounted in an airplane flying in lawful airspace to take photographs of Dow Chemical Company's 2,000-acre Midland, Michigan, facilities. Fearful that industrial competitors might try to steal its trade secrets, Dow took elaborate precautions at its facility. Despite the precautions the company took to ensure its privacy, the Supreme Court, in a 5–4 vote handed down in 1985, found that Dow had no reasonable, legitimate, and objective expectation of privacy in the area the EPA had photographed. The dissent noted that, by basing its decision on the method of surveillance used by the government, as opposed to the company's reasonable expectation of privacy, the Court ensured that "privacy rights would be seriously at risk as technological advances become generally disseminated and available to society" (*Dow Chemical Co. v. United States*, 476 U.S. 227 (1986)).

Some contend that biometrics is precisely the kind of technological advance the *Dow* dissenters warned about. Citizens no longer would have a reasonable expectation of privacy any time they use a biometric identifier because the gov-

ernment's use of biometrics and computer matching would be merely utilizing commercially available technologies.

Cultural, Religious, and Philosophical Objections

Other criticisms of the use of biometrics originate on cultural, religious, and philosophical grounds. These objections might not be shared by large numbers of people, but to the extent those who advocate them have sincerely held beliefs, they merit discussion.

Cultural: Stigma and Dignity

Simon Davies of Privacy International notes that it is no accident that biometric systems are being tried out most aggressively with welfare recipients. The British scholar contends that they are in no position to resist the State-mandated intrusion. Interestingly, in the 1995 GAO Report on the use of biometrics to deter fraud in the nationwide Electronics Benefit Transfer (EBT) program, the U.S. Department of the Treasury expressed concern over how finger imaging would impact on the dignity of the recipients and called for more testing and study.

While stigma and dignity arguments tied to the less fortunate elements of society have a strong emotional appeal, the available empirical data from Connecticut suggests that the majority of entitlement recipients actually support the use of biometrics. Some have criticized such surveys as flawed because the recipients could be reluctant to provide their true opinions because of retaliation fears.

Religious Objections

Several religious groups criticize biometrics on the ground that individuals are forced to sacrifice a part of themselves to a godless monolith in the form of the State. For example, certain Christians interpret biometrics to be a "mark of the beast," an objection based on language in the New Testament's "Revelation":

> [The Beast] causeth all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: And that no man might buy or sell, save that he had the mark, or the name of the beast, or the number of his name.... And his number is six hundred, threescore, and six (Revelation, 13:16–18).

Certain Christians consider biometrics to be the brand discussed in Revelation and biometric readers as the only means of viewing these brands. For example, stressing that "the Bible says the time is going to come when you cannot buy or sell except when a mark is placed on your head or forehead," fundamentalist Christian Pat Robertson has expressed doubts about biometrics and has noted how the technology is proceeding according to scripture. And at least one religious group has complained that the hand geometry devices used by California were making "the mark of the beast" on enrollees' hands.