Biometrics: Privacy’s Foe or Privacy’s Friend?

JOHN D. WOODWARD

From the INS to ATM’s, both the public and private sectors are making extensive use of biometrics for human recognition. As this technology becomes more economically viable and technically perfected, and thus more commonplace, the field of biometrics will spark legal and policy concerns.

Critics inevitably compare biometrics to Big Brother and the loss of individual privacy. The probiometric lobby generally stresses the greater security and improved service that the technology provides. Is biometrics privacy’s friend or privacy’s foe? This paper explores the various arguments for and against biometrics and contends that while biometrics may pose legitimate privacy concerns, these issues can be adequately addressed. In the final analysis, biometrics emerges as privacy’s friend.

Keywords—Biometrics, biometrics law, constitutional law, identification, information privacy, privacy, regulation of biometrics, security, verification.

I. INTRODUCTION

On May 18, 1997, in his commencement address at Morgan State University, President Clinton stated:

The right to privacy is one of our most cherished freedoms. As society has grown more complex and people have become more interconnected in every way, we have had to work even harder to respect privacy, the dignity, the autonomy of each individual. . . . We must develop new protections for privacy in the face of new technological reality. [1]

While it is doubtful that President Clinton had biometrics in mind during that Sunday speech, biometrics is one such “new technological reality.” From the Immigration and Naturalization Service (INS) to automated teller machines (ATM’s), both the public and private sectors are making extensive use of biometrics for human recognition purposes to provide better security, increased efficiency, and improved service [2]–[4]. As the technology becomes more economically viable and technically perfected, biometrics could refocus the way that Americans look at the brave new world of personal information.

Understanding biometrics thus is essential for elected officials and policymakers charged with determining how this new technology will be used. An understanding of biometrics is also important for the legal, business, and policy advocacy communities so that they can meaningfully participate in the public debate related to biometrics.1

Similarly, an understanding of the law and policy concerns related to biometrics is necessary for the engineers and scientists who are responsible for this new technological reality. History teaches us that new technologies, created by engineers and scientists, spark new law and cause old legal doctrines to be rethought, rekindled, and reapplied by the makers of the nation’s law and policy.

For example, new technology has caused a creative reshaping of existing legal doctrine when the judiciary has embraced a technology more quickly than has the legislature, the executive branch, or even the actual marketplace for the technology. Consider a well-known example from the legal casebooks. In 1928, there was no law requiring coast-wise carriers to equip their tugboats with radio receiver sets. Moreover, no such established custom existed in the maritime industry, despite the fact that such sets could be used by tugs at sea to receive storm-weather warnings. In T. J. Hooper, a landmark legal case, Federal Circuit Judge L. Hand (1872–1961), one of the greatest American jurists of this century, deemed tugboats without radio receiver sets unseaworthy because “a whole calling may have unduly lagged in the adoption of new and available devices” [5]. No longer would strict adherence to local custom and industry practice be a valid defense against negligence.

Today’s new technological reality of biometrics should force us to explore from the law and policy perspectives what is required to safeguard the public interest and to ensure optimal results for society. Engineers and scientists should not be excluded from this law and policy examination. Indeed, the law and policy concerns raised by biometrics are far too important to be left solely to politicians and lawyers.

In examining these law and policy concerns, this paper focuses on privacy. After briefly discussing biometric technologies and biometric applications in Sections II and III, this paper attempts in Section IV to define privacy in the context of biometrics and to examine which specific privacy concerns are implicated by biometrics. This paper then

analyses the various arguments often made that biometrics poses a threat to privacy. This paper concludes that, to the contrary, biometrics is privacy’s friend because it can be used to help protect information integrity. Section V examines the biometric future and contends that “biometric balkanization,” or the use of multiple biometric technologies deployed for multiple applications, provides greater privacy protection than does biometric centralization, or the use of one dominant biometric technology for multiple applications.

II. WHAT IS BIOMETRICS?

A. Definition of Biometrics and Biometric Scanning

While the word “biometrics” sounds very new and “high tech,” it stands for a very old and simple concept—human recognition (Fig. 1). In technical terms, biometrics is the automated technique of measuring a physical characteristic or personal trait of an individual and comparing that characteristic or trait to a database for purposes of recognizing that individual [6].

Biometrics uses physical characteristics, defined as the things we are, and personal traits, defined as the things we do, including the following.

1) Physical characteristics:
   - chemical composition of body odor;
   - facial features and thermal emissions;
   - features of the eye—retina and iris;
   - fingerprints;
   - hand geometry;
   - skin pores;
   - wrist/hand veins.

2) Personal traits:
   - handwritten signature;
   - keystrokes or typing;
   - voiceprint [2]–[4], [6], [7].

Of these, only three of the physical characteristics and personal traits currently used for biometrics are considered truly unique: the retina, the iris, and fingerprints [8].
As such, these three physical characteristics provide the greatest precision for biometrics.

Biometric scanning is the process whereby biometric measurements are collected and integrated into a computer system. Biometric scanning is used for two major purposes: identification and verification. Identification is defined as the ability to identify a person from among all those enrolled, i.e., all those whose biometric measurements have been collected in the database. It seeks to answer the question, “Do I know who you are?” and involves a one-compared-to-many match (or what is referred to as a “cold search”). Verification involves the authentication of a person’s claimed identity from his previously enrolled pattern. It seeks to answer the question, “Are you who you claim to be?” and involves a one-to-one match.

B. Advantages of a Biometric Scanning System

Biometric scanning can be used for almost any situation calling for a quick, correct answer to the question, “Who are you?” The unique advantage of biometric scanning is that it bases recognition on an intrinsic aspect of a human being. Recognition systems that are based on something other than an intrinsic aspect of a human being are not always secure. For example, keys, badges, tokens, and access cards (or things that you physically possess) can be lost, duplicated, stolen, or forgotten at home. Passwords, secret codes, and personal identification numbers (PIN’s) (or things that you must know) can easily be forgotten, compromised, shared, or observed.

Biometrics, on the other hand, is not susceptible to these particular problems. According to Dr. J. Campbell, Jr., a National Security Agency (NSA) researcher and chairman of the Biometric Consortium, no one technology has emerged as the “‘perfect biometric,’ suitable for any application” [9]. While there is no “perfect biometric,” the characteristics of a good biometric scanning system are speed, accuracy, user friendliness, and low cost.

III. HOW ARE BIOMETRICS USED?

A. Biometric Applications

Biometric applications are broad based, expanding, and international. As one industry expert recently stated, “The influence of biometric technology has spread to all continents on the globe” [10]. In concrete terms, this influence translates into about $1 billion worth of computer systems that include biometric devices expected to be installed worldwide during 1997 [2].

While biometric devices are deployed in many computer systems, the overall size of the biometrics industry remains relatively small, though it is rapidly growing. For example, in 1992, revenue from biometric devices was estimated at $8.3 million, with 1998 units sold. By 1999, revenue is projected at $50 million, with 50,000 units sold [6].

While a detailed discussion of biometric applications is beyond the scope of this paper, three major categories highlight how biometric scanning is beginning to touch our lives: high government use, lesser government use, and private-sector use.

1) High Government Use:

a) Law enforcement and prison management: Since March 1990, the Cook County (IL) Sheriff’s Department has been using retinal scanning to process prisoners [4]. Retinal scanning is used to identify and keep track of inmates. Upwards of 300 prisoners are scanned daily, and the Sheriff’s Department’s database includes more than 300,000 retinal patterns [11].

b) Military and national security community: While many of these applications remain classified, it is no secret that one of the principal executive-branch organizations spearheading biometrics research is the highly secretive NSA [3]. Primary uses of biometrics for the national-security community include facilities protection and personnel access [6].

2) Lesser Government Use:

a) Border control and immigration checks: Confronted with a two-fold increase in passenger volume in international air travel during the past decade, along with the urgent need to keep terrorists, criminals, and illegal aliens out of the United States, the INS has been experimenting since 1993 with an automated inspection system using biometric technologies at select ports of entry. The INS’s goal is to remove the law-abiding, frequent traveler from the inspection lines and allow the low-risk person to be inspected and cleared by verifying his identity with a biometrics-based system. This method allows the INS to focus its efforts on potential terrorists and criminals, thus ensuring that INS resources are better utilized.

The INS has four biometrics projects under way at several ports of entry: INSPASS (Airport), the soon-to-be-deployed INSPASS (Land), PORTPASS (Dedicated Commuter Lane), and PORTPASS (Automated Permit Port). INSPASS (Airport) features hand geometry, while PORTPASS (Automated Permit Port) uses voice verification for the driver; PORTPASS (Dedicated Commuter Lane) is not yet automated [12]. The INS also uses voice verification for frequent travelers entering the United States from Canada at a remote border-crossing point in Montana [3].

b) Entitlement programs and licensing: The Los Angeles County Department of Public Social Services reported that finger imaging of welfare recipients in a pilot program alone reduced fraud by more than $14 million and resulted in the termination of more than 3000 previously approved entitlement cases over a three-year period [13], [14]. More than a dozen states are using biometrics to help administer various entitlement programs.

In 1995, the Federal Highway Administration awarded a $400,000 contract to San Jose State University to study and develop standards for biometric identifiers for use with commercial truck drivers’ licenses [3]. Congress mandated this biometric application because of public safety concerns that commercial truck drivers were obtaining concurrent commercial licenses from various individual states in an attempt to evade the regulatory scheme [15], [16]. Congress feared that unscrupulous drivers would use the multiple concurrent licenses in their possession to conceal the true extent of the traffic violations and point totals they had
received by recording their violations over many individual states’ databases as opposed to any one centralized place [18].

c) National identity card and voter registration: National identity card proposals are usually met with concern and consternation in the United States. The Government of the Philippines, however, has decided to embark on an ambitious national identity card project, with plans to enroll up to 63 million people. Likewise, the South African Home Affairs National Identification System will involve an identity card combined with a biometric identifier [10].

With respect to voter registration, Jamaica is experimenting with an eelctoration system to register eligible voters incorporating an identification card with fingerprint minutiae data.

3) Private-Sector Use:

a) Financial services industry: In 1995, Oki Electric Industry Limited, Japan’s leading vendor of ATM’s, teamed up with two U.S. companies, IrisScan and Sensar, to integrate iris-recognition technology into its ATM’s in Japan. Citibank is also evaluating iris recognition for use in the United States [3], [4]. The ATM card holder will first be “enrolled” at his local bank branch. Instead of thinking up a password, the customer will look into a scanner, which will video his iris pattern, instantly convert it to a 256-byte digitized code, and store this code on the magnetic strip of his ATM card. The next time the customer needs fast cash, he simply inserts his card into the machine. A video camera installed in the ATM reads his iris pattern from about three feet away and matches it with the code on his card to grant him access to his account. In October 1996, Oki unveiled IrisIdent, its iris-recognition-based ATM system, in Tokyo, where the system will be tested by a number of Japanese banks.

Alternatively, finger images are also being used to control ATM access. In Indiana, for example, the Purdue Employees Federal Credit Union has been enrolling finger images of customers since February 1997 to give them access to kiosks, or “virtual branches,” that it will install at several Purdue University campus sites later this year.

b) Personnel management: Presently, Woolworth’s supermarkets in Australia operate the world’s largest time and attendance system featuring biometrics. Finger-imaging technology is used to monitor time and attendance for about 100,000 employees [10]. Coca-Cola uses hand-scanning technology for time and attendance [2].

c) Access control: Walt Disney World in Orlando, FL, now uses finger geometry to verify customers who purchase yearly passes [2]. Previously, annual-pass holders were photographed to prevent any illegal or inadvertent pass transfer; the new finger-scanning system has received positive feedback [4].

The computer log-on of the not-so-distant future will be done using a biometric identifier, according to biometrics experts. Under this scenario, a small optical scanner or video camera would be added to the computer workstation. The computer user would then log-on by using, for example, finger imaging or iris recognition.

IV. WHAT IS PRIVACY IN THE CONTEXT OF BIOMETRICS?

A. Working Definition

The issue of privacy is central to biometrics. Critics complain that biometrics poses a substantial risk to privacy rights. Evaluating this argument requires, first, an understanding of what privacy rights entail. The word “privacy” (like the word “biometrics”) is nowhere to be found in the text of the U.S. Constitution. Perhaps the absence of any explicit textual reference to privacy or right of privacy, combined with the word’s apparent flexibility of meaning, makes it all the more difficult to define what privacy is and to explain what the right of privacy should be.

Most important from the standpoint of biometrics, privacy includes an aspect of autonomy—“control we have over information about ourselves [17],” “[c]ontrol over who can sense us [18] . . . control over the intimacies of personal identity” [19], or, as a federal appeals court has phrased it, “control over knowledge about oneself. But it is not simply control over the quantity of information abroad; there are modulations in the quality of knowledge as well” [20].

While the Supreme Court has never explicitly recognized a constitutional right to privacy (and has never dealt with biometrics), America’s highest court has grappled with issues of information privacy. In Whalen v. Roe, an influential case decided in 1977, the court decided the constitutional issue of whether the State of New York could record, in a centralized database, the names and addresses of all individuals who obtained certain drugs, pursuant to a doctor’s prescription [21]. Rejecting the privacy claim, the court ruled that a government database containing massive amounts of sensitive medical information passed constitutional muster because of the security safeguards in place. The court’s opinion concluded with a cautionary note that still echoes loudly today:

We are 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. [21]

In the context of biometrics, this control over information about ourselves, or information privacy, lies at the very heart of the privacy concerns raised by this new technology. 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.

B. What Privacy Concerns Are Implicated?

1) 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 scanning is used. Regardless of whether an individual voluntarily provides a biometric identifier or is forced to surrender it as part of a state action or government-required scheme, he is giving up information about himself. When biometrics like finger imaging, iris recognition, or retinal scanning are used, he discloses truly unique information about his identity. When the other
biometrics are used, he discloses accurate information about who he is.

2) **Invasive Aspects of the Information:** Beyond this fundamental disclosure, there also might be invasive implications related to privacy concerns that stem from the biometric identification information disclosed. These invasive implications for privacy are essentially two-fold: 1) the invasive effects of a secondary market, defined as disclosure of the biometric identification information to third parties, and 2) invasive information that might be additionally obtained as part of the biometric identifier.

   a) **Invasive secondary market effects:** Once a biometric identifier is captured 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 in much the way that names and addresses on mailing lists presently are bought and sold by data merchants.

   Particularly with respect to the private sphere, where the conduct of private actors traditionally has been given a degree of freedom of action from government interference, there presently are few legal limits 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 affirmative action has been taken by a government, the use of biometrics is left to the market. In other similar contexts where an individual has surrendered personal information to private actors, the Supreme Court has not found a constitutionally based privacy right. For example, in *Smith v. Maryland,* the defendant claimed that information in the form of telephone numbers he dialed from his home telephone (what is known as a pen register) could not be turned over to the police absent a search warrant [22]. Rejecting this argument, the court noted that it “consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties” [22].

   In *United States v. Miller,* a case involving a bootlegger’s private financial records, which were turned over to U.S. Treasury agents pursuant to a grand jury subpoena, the bootlegger’s attempt to have the evidence excluded was unsuccessful [23]. The court found that Miller had no expectation of privacy in the records, reasoning that “[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government” [23]. The records therefore could not be considered confidential communications because they had been voluntarily conveyed to the bank in the “ordinary course of business” [23].

   Biometrics is still too new for the Congress or the various state legislatures to have acted from the standpoint of privacy protections aimed at this technology. At present, private actors possessing biometric identification information generally follow a nondisclosure policy—they do not disclose the information to third parties—as part of a strategy of building public acceptance for the technology. Such nondisclosure policies, however, are voluntary.

   Critics contend that biometric identifiers—like other personal information, such as names and addresses for mailing lists—might eventually be “considered to be in the public domain” [24]. The fear is that the individual will lose ultimate control over all aspects of his biometric identifier. 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. Fingerprints have long been used by law enforcement, and finger images—or what in effect is the next generation of fingerprints—are presently being used by various law-enforcement agencies as part of their databases. For example, the Federal Bureau of Investigation (FBI) has embarked on a bold finger-imaging project for its Integrated Automated Fingerprint Identification System (IAFIS). IAFIS would replace the present paper-and-ink-based system with electronic finger images.

   Second, it is possible (and, the 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 suggests that fingerprints and finger imaging might disclose medical information about a person [25], [26]. For example, Dr. H. 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 “[c]ertain chromosomal disorders are known to be associated with characteristic dermatoglyphic abnormalities,” specifically citing Down syndrome, Turner’s syndrome, and Klinefelter’s syndrome as chromosomal disorders that cause unusual fingerprint patterns in a person [25]. Certain nonchromosomal disorders, such as chronic intestinal pseudoobstruction (CIP, described below), leukemia, breast cancer, and Rubella syndrome, have also been implicated by certain unusual fingerprint patterns [25].

   For example, Dr. M. M. Schuster, 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 CIP, which affects 50,000 people nationwide. Based on the results of a seven-year study, Dr. Schuster found that 54% of CIP patients have this rare digital-arch fingerprint pattern. Schuster’s discovery suggests a genetic basis to the disease in that the more digital arches in the fingerprint, the stronger the correlation to CIP [27].

   From examining the retina or iris, an expert can determine that a patient may be suffering from common afflictions like diabetes, arteriosclerosis, and hypertension; furthermore, unique diseases of the iris and the retina can also be
detected by a medical professional [28], [29]. While both the iris and retina contain medical information, it is by no means obvious that biometric scanning of the iris or retina automatically implicates privacy concerns related to the disclosure of medical information. A necessary area of further technical inquiry is whether the computerized byte code taken of the iris or retina actually contains this medical information or if the information captured is sufficient to be used for any type of diagnostic purpose. While much research remains to be done, the availability of such information, with its possible links to medical information, raises important questions about the privacy aspects of the information disclosed.

C. Biometrics as Privacy’s Foe: Criticisms

1) The Loss of Anonymity and Autonomy: A basic criticism of biometrics from the standpoint of privacy is that we, as individuals, lose our anonymity whenever biometric scanning systems are deployed. Controlling information about ourselves includes our ability to keep other parties from knowing who we are. While we all know that at some level, a determined party—whether the state or a private actor—can learn our identity (and much more about us), biometric scanning makes it plain that our identity is now fully established within seconds. As Prof. 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 [sic] with whom they are dealing exercises power over them” [30]. Privacy advocate R. Ellis Smith agrees, noting that “[i]n most cases, biometric technology is impersonal” [2]. At the same time, if the technology meets with widespread success, individuals may find that they are required to provide a biometric identifier in unexpected, unwelcome, or unforeseen future circumstances. Moreover, one cannot make up a biometric as easily as one can an address and phone number. In this sense, perhaps, the loss of anonymity leads to an inevitable loss of individual autonomy.

To the extent that there is less individual anonymity today than in decades or centuries past, biometrics is not to blame. Rather, far larger economic, political, and technological forces are at work. America’s transformation from an agrarian to an industrial to a postindustrial service economy, combined with the massive growth of government since the New Deal of the 1930’s, has 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 keep extensive information on individuals. Summarizing this trend, one scholar has noted that

in the present service economy, information has become an increasingly valuable commodity, . . . The computer has exacerbated this problem through its capacity to disclose a large amount of personal information to a large number of unrelated individuals in a very short amount of time. [31]

While a biometric identifier is a very accurate identifier, it is not the first nor is it the only identifier used to match or locate information about a person. Names and numerical identifiers such as social security numbers (SSN’s), 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 ability to search, for example, the full text of stored documents—make identifiers far less important for locating information about an individual.

Critics of biometrics also overlook the fact that there usually is a good reason why recognition in the form of identification or verification is needed. The benefits of establishing a person’s identity outweigh the costs of losing anonymity. For example, given the massive problem of missing children, there is growing support for the idea of day care providers using biometrics to make certain that children are released at the end of the day to a parent or guardian whose identity has been verified.

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 $400 million a year [32], [33]. Credit card fraud is estimated at $2 billion per year. The financial services industry believes that a significant percentage of these losses could be eliminated by biometric scanning [2].

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 biometric measures 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.

Drawing a parallel to the financial services industry, despite the existence of many comprehensive payment systems—like credit cards, which combine 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 discounted. Moreover, as explained below, the ability of biometrics to serve as privacy-enhancing technologies should not be discounted.

2) The Biometrics-Based Big Brother Scenario: Aside from the alliterative qualities the phrase possesses, critics of biometrics seem inevitably to link the technology to Big Brother [2]–[4], [24]. Its critics argue that biometrics, in combination with impressive advancements in computer and related technologies, would 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 M. 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” [34].
For example, in the traffic stop of the future, the police officer will pull over the vehicle, walk to the driver’s side window, and ask for the driver’s license. This license will have a magnetic strip containing the byte code of the driver’s fingerprint, which will be required by the state’s department of motor vehicles. The officer will then take a portable optical scanner from his pocket and ask the vehicle’s driver to biometrically scan in. The officer will be able to identify the driver, as the data is transmitted for immediate matching to the central database, where any outstanding arrest warrants, traffic citations, delinquent taxes, tardy child-support payments, and the like could be entered. The concern is that a mere traffic stop would tell the police officer a great deal about the motorist in mere seconds; the fear is that armed with this informational power, there would be abuses by law enforcement.

This use of biometrics is superior to the present system of checking a driver’s license because it makes it much more difficult in practical terms for a person to obtain a driver’s license using a false identity. Not only would law enforcement know in a very short time the criminal status of any driver they have stopped but whenever a driver’s license would be presented for other secondary identification purposes, the claimed identity could be confirmed by the use of a biometric scan-in at the point of service. For example, background checks for firearms purchases could be done easily in this manner. While the threat of criminal penalties for using false identification might deter some individuals, the use of biometrics as described above sets the hurdle all the higher for criminals seeking to obtain a driver’s license by using an alias.

This Big Brother concern, however, goes beyond normal police work. Every time an individual uses his biometric identifier to conduct a transaction, a record would be made in a database, which the government, using computer technology, could then match and use against the citizen—even in ways that are not authorized or that 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” [35]. Prof. Clarke perhaps has offered the best worst-case 1984-like scenario:

Any high-integrity identifier [such as biometric scanning] 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 anti-utopian novelists. [30]

There is at least one example from U.S. history where supposedly confidential records were used in ways likely never intended. In November 1941, almost two weeks before the Japanese attack on Pearl Harbor, President F.D. Roosevelt ordered that a comprehensive list be made of the names and addresses of all foreign- 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 [36]. By the spring of 1942, the U.S. government forced persons of Japanese descent, including U.S. citizens, to leave their homes on the West Coast and report to “relocation centers” [37].

a) Function creep: The biometrics-based Big Brother scenario would not happen instantly. Rather, when first deployed, biometrics would be used for very limited, clearly specified, sensible purposes—to combat fraud, improve airport security, protect children, etc. But as Justice Brandeis warned in his famous Olmstead dissent:

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. [38]

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

The classic example of function creep is the use of the 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 [39]. In fact, the original Social Security cards containing the SSN bore the legend, “Not for Identification” [30]. By 1961, the Internal Revenue Service (IRS) began using the SSN for tax identification purposes [30], [39]. By 1997, “[e]verything from credit to employment to insurance to many states’ drivers licenses requires a Social Security Number” [40]. From its origins as “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 have 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, a Russian proverb aptly identifies the danger of biometrics for freedom-loving Americans: “If you are a mushroom, into the basket you must go.”

b) By using biometrics, government reduces 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 fora, 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 its privacy.

Analyses can be drawn from previous cases where the government has used cutting-edge technology to intrude in
Biometrics is one kind of technological advance that the Dow dissenters warned about. Citizens no longer would have a reasonable expectation of privacy any time they use a biometric identifier because the government’s use of biometrics and computer matching would be merely utilizing commercially available technologies.

While biometrics is an important technological achievement, its use should be kept in a law and policy perspective: Big Brother concerns implicate far more than biometrics. The underlying issue is not controlling biometrics but rather the challenge of how law and policy should control contemporary information systems. Computers and the matching they perform permit various fragments of information about an individual to be combined and compiled to form a much more complete profile. These profiles can be collected, maintained, and disclosed to organizations with which the individual has no direct contact or to which the individual would prefer to prevent disclosure. [31]

Biometrics should be viewed as an appendage to this enormous challenge.

Critics also overlook the many legitimate reasons why the government needs to use biometric applications. Biometric applications related to national security and prison management are easy to grasp; all of us want solid guarantees that only the correct military personnel can access nuclear missile silos and that ax murderers cannot slip out of prison by masquerading as someone else. These same concerns related to the use of false identity apply across the board; for example, the government has a legitimate purpose in preventing fraud in the programs it administers.

Fraud is a significant issue in public-sector programs. A persistent problem of state welfare entitlement programs is fraud perpetrated by double dippers—individuals who illegally register more than once for benefits by using an alias or other false information about themselves. Many experts believe that fraud in entitlement programs like welfare can be as high as 10%, which translates in dollar terms to over $40 billion a year in potential savings [14] if the fraud is prevented.

Biometrics can be used to help stop this fraud. B. Rasor, a senior U.S. Secret Service official, commented that “[b]iometrics would put a sudden and complete stop to as much as 80% of all fraud activity” [14]. In Connecticut, which has embarked on a robust biometric identification program for welfare recipients known as the Digital Imaging System, the state’s Department of Social Services “conservatively estimates that in the first year of operation [1996], savings in the range of $5 512 994 to $9 406 396 have been achieved” [42].

In these tight budgetary times when welfare programs are being curtailed and resources are overextended, anyone who is illegally receiving an entitlement payment is, at the bottom line, depriving an honest, needy person of his entitlement because there is simply less money to go around.

To the extent that critics have concerns about function creep, two points need to be made. First, as explained above, the critical and key function-creep issue is controlling information systems, not controlling a nine-digit number or an 8-byte numerical template used as a biometric identifier. Second, issues specifically related to biometrics can be best addressed within our present legal and policy framework. We do not need a new “Law of Biometrics” paradigm; the old bottles will hold the new wine of biometrics quite well. In this regard, legislative proposals, particularly at the federal level, should be considered and studied, particularly if the threat of function creep is real. These proposals could include:

1) a Code of Fair Information Practices (CFIP) specifically adapted to the use of biometrics. A CFIP could emphasize that organizations holding biometric identification information have responsibilities to protect such data and that individuals who provide such biometric identification information have certain rights, including the right to prevent their biometric identification information from being traded in a secondary market;

2) an outright legal prohibition on any kind of transactions in the secondary biometrics market.

3) Cultural, Religious, and Philosophical Objections:
   a) Cultural objections—Stigma and dignity: S. Davies of Privacy International notes that it is no accident that biometric systems are being tried out most aggressively with welfare recipients; he contends that they are in no position to resist the state-mandated intrusion [43]. Interestingly, in the General Accounting Office (GAO) report on the use of biometrics to deter fraud in the nationwide Electronic Benefits Transfer program, the U.S. Department of Treasury expressed concern over how finger imaging “would impact on the dignity of the recipients” and called for more “testing and study” [13].

While stigma and dignity arguments tied to the less fortunate elements of society have a strong emotional appeal,
the available empirical data suggest that the majority of entitlement recipients actually support the use of biometrics. For example, a recent survey of 2378 food stamp and Aid to Families with Dependent Children recipients in San Antonio, TX, who will be participating in a biometrics pilot program, found that “90% think finger imaging is a good idea and 88% think finger imaging will help make people more honest when applying for benefits” [44]. Survey data in Connecticut suggest similar results [45].

b) Religious objections: Several religious groups criticize biometrics on the grounds that individuals are forced to sacrifice a part of themselves to a godless monolith in the form of the state. For example, observing 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 P. Robertson expresses doubts about biometrics and notes how the technology is proceeding according to Scripture [46]. 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 [14].

Similar objections have also been made in the context of the government’s mandated provision of SSN’s. In Bowen v. Ray, a leading Supreme Court case dealing with this issue, a Native American objected to the provision of an SSN for his minor daughter’s application for welfare assistance as a violation of the family’s religious beliefs. The court refused to sustain this challenge [47].

As Bowen v. Ray demonstrates, the courts are experienced in dealing with objections involving the state’s mandatory provision of identifiers. The judiciary has an adequate framework to deal with biometrics-related religious concerns if they should arise in this context.

c) Philosophical objections—Biometrics-based branding: Biometrics merits criticism on the grounds that a biometric identifier is nothing more than biometrics-based branding or high-tech tattooing. There is an understandably odious stigma associated with the forced branding and tattooing of human beings, particularly since branding was used as a recognition system to denote property rights in human slaves in the eighteenth and nineteenth centuries and tattooing was used by the Nazis to identify concentration camp victims in this century. More than just the physical pain of the brand or tattoo accounts for society’s revulsion. Analogizing from these experiences, biometric identifiers are merely a physically painless equivalent of a brand or tattoo that the state will impose on its citizens. While biometrics may lack the performance of a microchip monitor that could be implanted in humans [48], the biometric identifier will similarly serve the interests of the state. Biometrics is another example of the state’s using technology to reduce individuality.

Comparisons of biometrics to brands and tattoos again appeal to the emotions. Essentially, these arguments are the ultimate form of the Big Brother concerns outlined above. Slave owners and Nazis forced branding and tattooing on victims who had absolutely no choice. In the private-sector realm, citizens are making voluntary choices to use or not use biometrics. When biometrics is used in the public sector, the use will be for legitimate purposes and will be overseen by democratic institutions.

4) Actual Physical Harm, Physical Invasiveness: To this author’s knowledge, there are no documented cases of biometrics’ causing physical harm to a user. Anecdotally, some users of biometrics have complained that hand geometry systems dry their hands, while military aviators participating in an experimental program voiced concern that retinal scanning would damage their 20/20 vision with extended use over time.

In terms of the physical invasiveness associated with biometrics, retinal scanning requires close contact with the biometric apparatus in the sense that the retina pattern is captured from about three inches away from the eye. Finger imaging requires physical touching of the scanner, as does hand geometry. Iris recognition stands out as perhaps the most “hygienic” of the biometrics in that no part of the user’s body has to touch anything to operate the system. Any liability resulting from actual physical harm caused by biometric systems would be addressed by the individual states’ tort liability regimes. Eventually, the judiciary will have the opportunity to decide the admissibility of biometric identification as scientific evidence using prevailing legal standards [49].

C. Biometrics as Privacy’s Friend: Support for Biometrics

1) Biometrics Protects Privacy by Safeguarding Identity and Integrity: While critics of biometrics contend that this new technology is privacy’s foe, the opposite, in fact, is true. Biometrics is a friend of privacy whether used in the private or public sectors. Biometrics proves itself as privacy’s friend when it is deployed as a security safeguard to prevent fraud.

To consider a specific example drawn from the financial services industry but applicable to almost any fraud-prevention scenario, criminals eagerly exploit weaknesses within the present access systems, which tend to be based on passwords and PIN’s, by clandestinely obtaining these codes. They then surreptitiously access a legitimate customer’s account. The honest client effectively loses control over his personal account information. His financial integrity is compromised and his finances are gone because a criminal has gained unauthorized access to the information. In effect, he has suffered an invasion of his privacy related to his financial integrity. With biometrics-based systems, fraud, while never completely defeated, becomes more difficult for the criminal element to perpetuate. Biometrics means less consumer fraud, which means greater protection of consumers’ financial integrity.

Numerous examples exist of impostors’ masquerading under a false identity to convince state actors that they are someone other than who they really are. For example, James E. Young (Young 1) suffered financial losses as well as loss to his reputation when a person with the same first and last name (Young 2) was able to get Young 1’s undergraduate transcript from his state university. This transcript contained extensive personal information, including Young 1’s SSN.
Young 2 then used this information to establish charge accounts, with which he purchased items billable to Young 1 [50]. In such a case, biometric applications would almost certainly help protect a citizen’s information integrity by making it more difficult for the criminal to obtain the information; Young 2’s biometric would not match Young 1’s.

2) Biometrics Used to Limit Access to Information: Biometrics becomes a staunch friend of privacy when the technology is used for access-control purposes, thereby restricting unauthorized personnel from gaining access to sensitive personal information. For example, biometrics can be effectively used to limit access to a patient’s medical information stored on a computer database. Instead of relying on easily compromised passwords and PIN’s, a biometric identifier would be scanned in at the computer workstation to determine database access. The same biometric systems can be used for almost any information database (including databases containing biometric identifiers) to restrict or compartmentalize information based on the “need to know” principle.

Biometrics also protects information privacy to the extent that it can be used, through the use of a biometric log-on explained above, to keep a precise record of who accesses what personal information within a computer network. For example, individual tax records would be much better protected if an IRS official had to use his biometric identifier to access them, knowing that an audit trail was kept detailing who accessed which records. Far less snooping by curious bureaucrats would result.

3) Biometrics as Privacy-Enhancing Technology: Beyond protecting privacy, biometrics can be seen as enhancing privacy. There are several newly developed biometric technologies that use the individual’s physical characteristic to construct a digital code for the individual without storing the actual physical characteristics in a database [51]–[53]. For example, using finger-image-based technology, a person’s fingerprint is used during enrollment to create a PIN for the individual. This encoded PIN can only be decoded by a match with the appropriate finger pattern. During verification, a computer search is done to ensure that the same PIN has not previously been entered into the system, thereby eliminating the fraud risk. At the same time, only the PIN, and not the actual fingerprint, is stored in the database [53]. In this regard, the maker claims to have created the first anonymous verification system using fingerprint patterns and light waves to protect privacy [53].

The applications of this type of anonymous verification system are extensive. Most notably, such a biometrics-based system would seem to provide a ready commercial encryption capability. Moreover, rather than technological advances eroding privacy expectations—as we saw, for example, with the EPA’s use of a special aerial camera over Dow—biometrics, as used to create an anonymous encryption system, would provide for privacy enhancement.

Many of the criticisms of biometrics discussed above are either off the mark—in that they really should be aimed at contemporary information systems, which are the result of economic, political and technological change—or fail to acknowledge why knowing an individual’s identity is necessary. As Section V explains, the use of biometrics might provide for even further individual privacy protections through a phenomenon known as biometric balkanization.

V. BIOMETRIC CENTRALIZATION VERSUS BIOMETRIC BALKANIZATION: WHICH PROTECTS PRIVACY BETTER?

It is important to address whether a specific biometric technology will come to dominate biometric scanning systems. In other words, will the biometric future feature biometric centralization, whereby one biometric will dominate multiple applications, or will we see biometric balkanization, where multiple biometrics are used for multiple applications? At present, finger imaging has an early lead in terms of industry presence and received an important seal of governmental approval when it was endorsed by the GAO [13]. The popularity of finger imaging is explained primarily by its accuracy, the fingerprint’s long acceptance as the biometric of choice.

For example, with regard to public acceptance of finger imaging, a recent survey of 1000 adults revealed that 75% of those polled would be comfortable having a finger image of themselves made available to the government or the private sector for identification purposes. This high acceptance is arguably underscored by the fact that over half of those surveyed said that they had been fingerprinted at some point in their lives. Only 20% thought that fingerprinting stigmatizes a person as a criminal [54]. Despite this early lead, however, it is not clear that finger imaging will emerge as the biometric of choice.

It is tempting to predict that finger imaging will dominate or that another biometrics will come to monopolize the market because of its perceived advantages. This view, however, overlooks one of the great strengths of the present biometrics market: it offers many robust technologies, which allows maximum choice for users. A more likely outcome is that “biometric balkanization” will result: multiple biometrics will be deployed not only by various public- and private-sector actors but by the same actor depending on the specific mission.

Arguably, biometric balkanization, like its Eastern European namesake, can take on a sinister spin. Individuals will be forced to give up various identifying “pieces” of themselves to countless governmental and corporate bureaucracies. In an Orwellian twist, the retina, the iris, the fingerprints, the voice, the signature, the hand, the vein, the tongue, and presumably even body odor will all be extracted by the state and stored in databases.

Yet, biometric balkanization offers at least two key advantages for the protection of privacy. First, it offers maximum flexibility to the private or public actor that will use the technology. The actor can tailor a specific biometric program to meets its own unique mission within its resource constraints. Depending on the situation and the degree of accuracy in identification required, the optimal biometric for that use can be selected. For example, the best biometric
Table 1  Selected Listing of Biometrics Applications Used by U.S. and State Government Agencies

<table>
<thead>
<tr>
<th>U.S. Department of Justice</th>
<th>Border Patrol evaluating facial imaging, voice verification, hand geometry, and finger imaging technologies. The INSPASS system uses hand geometry for automation of frequent flyers at a number of U.S. airports. The IDENT system uses finger technology to secure the southwest border of the United States.</th>
</tr>
</thead>
<tbody>
<tr>
<td>U.S. Immigration and Naturalization Service</td>
<td>Hand geometry for access control.</td>
</tr>
<tr>
<td>Drug Enforcement Administration</td>
<td>Finger imaging for IAFIS. IAFIS would replace the present paper-and-ink-based system with electronic finger images. National Crime Information Center 2000 will use various biometric technologies.</td>
</tr>
<tr>
<td>Federal Bureau of Investigation</td>
<td>Evaluating finger imaging and voice verification for smart gun technology. A smart gun incorporates, for example, biometric technology into the operating system of a firearm to restrict the firing of the weapon to authorized users.</td>
</tr>
<tr>
<td>National Institute of Justice</td>
<td>Evaluating finger imaging and voice verification for smart gun technology. A smart gun incorporates, for example, biometric technology into the operating system of a firearm to restrict the firing of the weapon to authorized users.</td>
</tr>
<tr>
<td>California Department of Justice, SINS (Statewide Integrated Narcotics System)</td>
<td>Finger imaging to secure access to sensitive information about narcotics.</td>
</tr>
<tr>
<td>U.S. Department of Commerce</td>
<td>Hand geometry to secure access to the department’s Office of Computer Services.</td>
</tr>
<tr>
<td>U.S. Department of Defense—Various Components</td>
<td>Voice verification, hand geometry, and finger imaging for access control. Much of the department’s biometric work is classified; numerous technologies are being evaluated.</td>
</tr>
<tr>
<td>U.S. Department of Energy</td>
<td>Hand geometry in conjunction with smart cards for access control. Finger imaging for access control. Much of the department’s biometric work is classified; numerous technologies are being evaluated.</td>
</tr>
<tr>
<td>Department of Motor Vehicles at the state level</td>
<td>Various states, including California, Colorado, Florida, New Jersey, and Texas, are considering finger imaging for drivers licenses.</td>
</tr>
<tr>
<td>Entitlement programs</td>
<td>A number of states, such as California, Connecticut, Illinois, Massachusetts, New Jersey, New York, Pennsylvania, and Texas, are using finger imaging to prevent welfare fraud. Hand geometry, retinal scanning, and signature dynamics are being evaluated by other states.</td>
</tr>
<tr>
<td>Federal Aviation Administration</td>
<td>Evaluating various biometric technologies for airport security applications.</td>
</tr>
<tr>
<td>Federal Bureau of Prisons</td>
<td>Various biometric technologies, including hand geometry and finger imaging, are securing access and verifying identity of prisoners, staff, and visitors across the United States.</td>
</tr>
<tr>
<td>Other prisons</td>
<td>Retinal scanning, iris recognition, finger imaging and hand geometry for securing access and verifying identity of prisoners, staff, and visitors across the United States.</td>
</tr>
<tr>
<td>U.S. Department of State</td>
<td>Evaluating various biometric technologies to aid in visa and passport processing.</td>
</tr>
<tr>
<td>U.S. Department of Treasury</td>
<td>Evaluating signature dynamics for the electronic signing-off of income tax returns.</td>
</tr>
<tr>
<td>Internal Revenue Service</td>
<td>Evaluating hand geometry.</td>
</tr>
<tr>
<td>U.S. Secret Service</td>
<td>Evaluating various biometric technologies to aid in currency control.</td>
</tr>
</tbody>
</table>


used to verify access to a government entitlements program might differ from the best biometric used by a university to ferret out undergraduate examination fraud, which in turn might differ from the best biometric needed in a prison environment, where hostile users will go to extreme lengths to foil identification efforts. Similarly, voice verification might be ideal for determining account access over the telephone, while signature dynamics might be better suited for monitoring tax returns.

Second, biometric balkanization might actually mean a synergy of the actor’s interest and the individual’s concerns. Consider, for example, the public-sector use of biometrics. Government agencies basically want dependable, workable biometrics to achieve their primary purpose—verifying or identifying an individual. The individual essentially wants the same thing, plus protection of private information. If different technologies are used for different situations, citizens will not face the necessity of reporting to the government’s “biometric central” for enrollment. By allowing the agencies maximum choice of biometrics technologies, the individual gains greater protection for private information.

Biometric balkanization could also lead to the safeguard of biometric compartmentalization, which would be
achieved through the use of different biometric identifiers. For example, an iris pattern used for ATM access would be of little use to the Connecticut Department of Social Services, which uses finger imaging, just as a hand geometry pattern captured at Disney World would be of little value to Orlando police investigating a crime scene unless hand geometry systems played a role in crime-scene access.

From the privacy-enhancement perspective, biometric balkanization is the equivalent of being issued multiple identification numbers or PIN’s or passwords, with the important difference that biometrics-based systems provide better security and greater convenience.

On balance, however, the greater threat likely will arise not from the use of advanced monitoring technology but rather from sloppiness in database management. The potential for a breach in database security increases greatly as shortcuts are taken, budgets are slashed, trained personnel are few, and leaders do not draft and implement a biometrics blueprint or plan to safeguard biometric identification information for which they are responsible. For these reasons, the Supreme Court’s warning in Whalen v. Roe (discussed above) rings true for biometrics.

VI. CONCLUSION

Biometrics is a new technology that is being deployed in a variety of creative public- and private-sector applications. As biometrics gains in popularity and grows in uses, the law, or at least a modern-day equivalent of Judge Hand, will likely take notice. As this paper has suggested, while biometrics is a new technology, it does not require a striking new legal vision to regulate it. Rather, the situation is more akin to new wine in old bottles in that existing legal doctrines can deal with the challenges that biometrics present. The situation is compounded in that the American approach to privacy matters has tended to be ad hoc and piecemeal; for example, federal law forbids the disclosure of video records by a private actor, but the state can sell motor vehicle information from drivers to data merchants. While the question of whether America needs a comprehensive approach to privacy concerns is beyond the scope of this paper, the legal and policy challenges posed by biometrics are not so novel and extraordinary that they cannot be dealt with under existing processes.

Before succumbing to the criticisms of biometrics as privacy’s foe, the countercase needs to be made: biometrics is privacy’s friend. Critics of biometrics are too quick to kill the biometric identifier when it is really the “information society” and the technical underpinning of computer matching that should be the focus of their concern. To the extent that biometrics raises important legal and policy issues, the existing institutional framework can address these concerns.

Biometrics protects information integrity in both the private- and public-sector context. By restricting access to personal information, biometrics provides effective privacy protection. Biometric balkanization further safeguards privacy by allowing maximum choice for the organization using biometrics, which also makes biometric compartmentalization viable.

We are eyeball to eyeball with a new technological reality that promises greater security and efficiency for both its public- and private-sector users. Now is not the time to blink.

APPENDIX I

See Table 1.

APPENDIX II

See Table 2.
ACKNOWLEDGMENT

The author wishes to acknowledge the assistance of I. S. Nathenson, editor-in-chief of University of Pittsburgh Law Review, and Dr. W. Shen, guest editor of this special issue.

He wishes to thank Dr. A. S. DiDio, M.D., Adjunct Prof. I. K. Fong, Prof. S. Goldberg, Adjunct Prof. J. Massey, Prof. J. R. O’Sullivan, and S. Cassin Woodward for their helpful comments on earlier versions of this paper. He also thanks Dr. J. Campbell, Jr. and L. Alyea, chair and vice chair of the Biometric Consortium, respectively, D. Harper of the National Computer Security Association, B. Miller, chairman of CardTech/SecurTech, and W. Rogers, editor of Biometric Digest, for inviting him to speak at conferences hosted by their organizations; he benefited greatly from the participants’ many insightful comments.

REFERENCES


[22] Smith v. Maryland, 442 U.S. 735 (1979) [citations omitted].


[38] Olness v. United States, 277 U.S. 439, 479 (1927).


