

# 19 BIOMETRICS: IDENTIFYING LAW & POLICY CONCERNS

John D. Woodward, Jr.

**Abstract** Today's "new technological realities" force us to examine, from the law and policy perspectives, what is required to safeguard the public interest and to ensure optimal results for society. Biometrics is one such new technology reality. While not enjoying the media stature and public controversy associated with high tech issues like genetic cloning and cyberspace, biometrics -- which seeks a fast, foolproof answer to the questions, "Who are you?" or "Are you the person whom you claim to be?" -- will cause the law to take notice as it becomes more extensively used in the public and private sectors. Businesses, numerous government agencies, law enforcement and other private and public concerns are making increasing use of biometric scanning systems. As computer technology continues to advance and economies of scale reduce costs, biometrics will become an even more effective and efficient means for identification and verification. After briefly discussing biometric technologies and biometric applications, this chapter defines privacy in the context of biometrics and discusses which specific privacy concerns biometrics implicates. This chapter concludes that biometrics is privacy's friend because it can be used to help protect information integrity. The author also contends that any legitimate privacy concerns posed by biometrics, such as the possibility of a secondary market in individual biometric identification information, can be best handled by the existing law and policy framework. The author next considers the future of biometrics, and contends that "biometric balkanization," or the use of multiple biometric technologies deployed for multiple applications, provides greater privacy protections than does biometric centralization, or the use of one dominant biometric technology for multiple applications.

**Keywords:** Privacy, biometric law, public policy, government, information policy, constitutional law.

## 1. Introduction<sup>1</sup>

On May 18, 1997, in his commencement address at Morgan State University, President William J. 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 . . . [w]e 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 clearly emerging as one such “new technological reality.” From activities as diverse as the Winter Olympics in Nagano, Japan to the prisons of Cook County, Illinois, both the public and private sectors are making extensive use of biometrics. This new technological reality relies on “the body as password” for human recognition purposes to provide better security, increased efficiency and improved service [2,3,53,54]. As the technology becomes more economically viable, technically perfected and widely deployed, biometrics could become the passwords and PINs of the twenty-first century. In the process, biometrics could refocus the way Americans look at the brave new world of personal information [4].

Understanding biometrics is thus essential for elected officials and policymakers charged with determining how this new technology will be used and what role, if any, government should play in its regulation. Familiarity with 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.

Similarly, understanding the law and policy concerns of biometrics is necessary for the engineers and scientists who have brought about 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 nation's law and policy makers.<sup>2</sup>

New technology can cause a creative reshaping of existing legal doctrine when, for example, the judiciary has embraced a technology more quickly than the legislature, the executive branch or even the actual marketplace for the technology. To consider a well-known example from the legal casebooks, in 1928, there was no law or regulation requiring coastwise seagoing carriers to equip their tugboats with radio receiver sets. Moreover, no such custom or practice existed in the maritime industry, despite the fact that such sets could easily be used by tugs at sea to receive storm weather warnings. In a landmark legal case, Federal Circuit Judge Learned Hand, one of the great American jurists of this century, deemed that tugboats without radio receiver sets were unseaworthy because “a whole calling may have unduly lagged in the adoption of new and available devices” [6]. By accepting a new technology -- in this case, wireless communications -- more quickly than the legislative and executive branches or even the affected industry, Judge Hand, in effect, creatively reshaped the law. No longer would strict adherence to local custom and industry practice offer a

---

<sup>1</sup> This chapter is largely based on a previously-published article by the same author: John D. Woodward, “Biometrics: Privacy's Foe or Privacy's Friend?” in *Proceedings of the IEEE*, Sept. 1997.

<sup>2</sup> For an excellent examination of the intersection of science and technology with law and policy, see [5].

guaranteed defense against charges of negligence when a readily-available technology could result in greater utility to society.

Similarly, 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 chapter focuses on privacy. After briefly discussing biometric technologies in sections 2 and 3, the author, in section 4, defines privacy in the context of biometrics and examines which specific privacy concerns biometrics implicates. The author then analyzes the various arguments often made that biometrics poses a threat to privacy. The author concludes that, to the contrary, biometrics is privacy's friend. Biometrics is privacy's friend because it can be used to help protect information integrity and to deter identity theft. Nonetheless, the author suggests that government can play a positive role in regulating and thereby promoting public acceptance of this new technology. Section 5 examines the biometric future, and contends that "biometric balkanization," or the use of multiple biometric technologies deployed for multiple applications, provides greater privacy protections than does biometric centralization, or the use of one dominant biometric technology for multiple applications.

## 2. What is Biometrics?

### *Definition of Biometrics & Biometric Scanning*

While the word, "biometrics," sounds very new and "high tech," it stands for a very old and simple concept -- human recognition. 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 [7,56].

Biometrics uses physical characteristics, defined as the things we are, and personal traits, defined as the things we do, to include:

#### **Physical Characteristics**

- Chemical composition of body odor
- Facial features & thermal emissions
- Features of the eye: retina & iris
- Fingerprints
- Hand geometry
- Skin pores
- Wrist/hand veins

**Personal Traits**

Handwritten signature

Keystrokes or typing

Voiceprint

Of these, only three of the physical characteristics and personal traits currently used for biometrics are considered truly consistent and unique: the retina, the iris and fingerprints [8,55]. As such, these three physical characteristics provide the greatest reliability and accuracy for biometrics.

Biometric scanning is the process whereby biometric measurements are collected and integrated into a computer system, which can then be used to automatically recognize a person. 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. Identification 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").

Second, biometric scanning is used for verification, which involves the authentication of a person's claimed identity from his previously enrolled pattern. Verification seeks to answer the question: "Are you who you claim to be?" and involves a one-to-one match.

*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 great 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 must physically possess) can be lost, duplicated, stolen or forgotten at home. Passwords, secret codes and personal identification numbers (PINs) (or things that you must know) can be easily forgotten, compromised, shared or observed [9].

Biometric technologies, on the other hand, are not susceptible to these particular problems because biometrics relies on things that you are. For example, one industry representative has summed up the inherent strengths of the biometric his company promotes in the following humorous way: "Your iris: You can't leave home without it."

Depending on the exact use for which the technology is envisioned, an ideal biometric technology would include a system based on: (i) a consistent and unique biometric characteristic, (ii) non-intrusive data collection, (iii) no or minimal contact between the person being scanned and the equipment doing the scanning, (iv) an automated system, i.e., no human decision maker in the decision loop, (v) very high accuracy, and (vi) high speed.

According to Dr. Joseph P. Campbell, Jr., a National Security Agency (NSA) researcher and the former Chairman of the Biometric Consortium (BC), the U.S. Government's focal point for biometric research, no one technology has emerged as the "perfect biometric,' suitable for any application" [10]. While there is no "perfect

biometric,” a good biometric scanning system is fast, accurate, dependable, user-friendly and low-cost.

### **3. How are Biometrics Used?**

Biometric applications are increasingly broad-based, expanding and international; as one industry expert has stated, “The influence of biometric technology has spread to all continents on the globe” [11]. In concrete terms, this influence translates into about \$1 billion worth of computer systems that include biometric devices which were estimated to be installed worldwide during 1997 [12].

While biometric devices are deployed in many computer systems, the overall size of the biometric industry remains relatively small though rapidly growing. For example, in 1992, revenue from biometric devices was estimated at \$8.3 million with 1,998 units being sold. By 1999, revenue is projected at \$50 million with 50,000 units being sold. Accordingly, biometric scanning is likely to have a substantial impact on the way we interact and conduct our affairs in the foreseeable future.

While a detailed discussion of biometric applications is beyond the scope of this chapter, the following three major categories of biometric applications -- High Government Use, Lesser Government Use, and Private Sector Use -- highlight how biometric scanning is beginning to touch our lives:

#### **High Government Use**

*Law Enforcement*

*Prison Management*

*Military & National Security Community*

#### **Lesser Government Use**

*Border Control & Immigration Checks*

*Entitlement Programs*

*Licensing*

*National Identity Card & Voter Registration*

#### **Private Sector Use**

*Banking and Financial Services*

*Personnel Management*

*Access Control*

*Information System Management*

### **4. What is Privacy in the Context of Biometrics?**

#### *Working Definition*

The issue of privacy is central to biometrics. Critics complain that the use of biometrics poses a substantial risk to privacy rights. Evaluating this argument requires, in the first instance, an understanding of what privacy rights entail. The

word “privacy” (like the word “biometrics”) is nowhere to be found in the text of the United States Constitution, America's highest law. Perhaps the absence of any explicit textual reference to privacy or right of privacy, combined with the word's apparent flexibility of meaning, make it all the more difficult to define what privacy is and to explain what the right of privacy should be.

Most importantly from the standpoint of biometrics, privacy includes an aspect of autonomy – “control we have over information about ourselves” [12], “[c]ontrol over who can sense us” [13], “...control over the intimacies of personal identity” [14], 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” [15].

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.

In the American legal experience, privacy protections have followed two traditional pathways depending on whether the source of the privacy intrusion is a governmental or private sector activity. While privacy is not explicitly cited in its text, the Constitution, through the Bill of Rights, protects the individual from government's intrusion into the individual's privacy. For example, the Bill of Rights contains privacy protections in the First Amendment rights of freedom of speech, press and association; the Third Amendment prohibition against the quartering of soldier's in one's home; the Fourth Amendment right to be free from unreasonable searches and seizures; the Fifth Amendment right against self-incrimination; and the Ninth Amendment's provision that “[t]he enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people” [16].

With respect to private sector actions, the Constitution traditionally embodies what is essentially a *laissez-faire* spirit. As constitutional law scholar Laurence Tribe has noted, “[T]he Constitution, with the sole exception of the Thirteenth Amendment prohibiting slavery, regulates action by the government rather than the conduct of private individuals and groups [66].” With respect to the conduct of private individuals, the Supreme Court has been reluctant to find a privacy right in personal information given voluntarily by an individual to private parties [17,57].

For private sector intrusions into privacy, the common-law, through its doctrines of contract, tort and property, has, in varying degrees, attempted to provide certain protections for the individual (e.g., [18])<sup>3</sup>. However, the law has not used these doctrines to protect individual information in private sector databases. Generally, as a matter of law, an individual in possession of information has the right to disclose it.

Accordingly, the private sector enjoys great leeway as far as what it can do with an individual's information. “Except in isolated categories of data, an individual has nothing to say about the use of information that he has given about himself or that has

---

<sup>3</sup>As early as 1879, Judge Thomas M. Cooley, in his treatise on torts, included “the right to be let alone” as a class of tort rights, contending that “the right to one's person may be said to be a right of complete immunity.” Echoing and popularizing Cooley's phrase, Warren and Brandeis, in their classic article written over one hundred years ago, articulated their view of privacy as a “right to be let alone” which would enable society to “achieve control of press invasions of privacy” [58,59].

been collected about him. In particular, an organization can acquire information for one purpose and use it for another . . . generally the private sector is not legislatively-constrained” [19].

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 information privacy issues. In *Whalen v. Roe*, an influential case decided twenty-one years ago, 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. Rejecting the information 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, however, 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” [20].

### *What Privacy Concerns Are Implicated?*

#### **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 consistent and unique information about his identity. When the other biometrics are used, at a minimum, he discloses accurate information about who he is.

#### **Invasive Aspects of the Information**

Beyond this fundamental disclosure, there also might be invasive implications related to privacy concerns which 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) any invasive information which might be additionally obtained as part of the biometric identifier.

#### *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 much the way names and addresses on mailing lists are currently bought and sold by data merchants.

Particularly with respect to the private sphere, where the conduct of private actors has traditionally been given a degree of freedom of action from government interference, there are few current 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 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 right to privacy in the information surrendered. 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 [21]. 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: “The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.” Moreover, these records could not therefore be considered confidential communications because they had been voluntarily conveyed to the bank in the “ordinary course of business” [24].

Technology is fast and the law is slow [25]. Thus, biometrics is still relatively too new for the Congress or the various state legislatures to have acted from the standpoint of adopting privacy protections aimed specifically at this technology. In an impressive first step toward understanding private sector applications of biometrics, on May 20, 1998, Congress held hearings on the topic of “Biometrics and the Future of Money.” These hearings, before the Subcommittee on Domestic and International Monetary Policy of the Committee on Banking and Financial Services of the U.S. House of Representatives, chaired by Michael N. Castle, featured panels of leading technologists as well as policy experts. In terms of activities in the state legislatures, California has been the most pro-active. There, the legislature has been considering biometric privacy legislation as part of its identity theft reforms.

Currently, private actors possessing biometric identification information generally follow a nondisclosure policy -- they do not disclose this information to third parties - - as part of a strategy of building public acceptance for the technology. However, such nondisclosure policies are completely 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” [26]. The fear is that the individual will lose ultimate control over all aspects of her biometric identifier.

#### *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. Fingerprints have long been used by law enforcement and 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. 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.

Secondly, 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 [27,28]. 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 “[c]ertain chromosomal disorders are known to be associated with characteristic dermatoglyphic abnormalities,” specifically citing Down syndrome, Turner syndrome and Klinefelter syndrome as chromosomal disorders which cause unusual fingerprint patterns in a person [28]. Certain non-chromosomal disorders, such as chronic, intestinal pseudo-obstruction (CIP) (described below), leukemia, breast cancer and Rubella syndrome, have also been implicated by certain unusual fingerprint patterns.

For example, Dr. Marvin 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 a medical disorder called CIP which 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. 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 [29].

While still controversial within the scientific communities, several researchers report a link between fingerprints and homosexuality [30,60,61,62]. 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. While this research is far from conclusive, the availability of such information with its possible links to medical information and lifestyle preferences again raises concern about the need to protect the privacy of the information.

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 [31,63]. 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 as well as public perception concerns.

*Biometrics as Privacy's Foe: Criticisms of Biometrics***The Loss of Anonymity; the Loss of 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. Part of 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 Professor 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 organisation [sic.] with whom they are dealing exercises power over them" [32]. Privacy advocate Robert Ellis Smith agrees, noting that, "In most cases, biometric technology is impersonal." 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, you cannot make up a biometric as easily as you 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 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 were at work. America's transformation from an agrarian to industrial to post-industrial, service 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 keep extensive information on individuals. Summarizing this trend, one scholar has noted, "[I]n 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 [18]."

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, 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.

Moreover, there is usually a good reason why recognition in the form of identification or verification is needed. Balancing the equities involved and depending on the case, the benefits of establishing a person's identity generally outweigh the costs of losing anonymity. For example, given the massive problem of missing and abused children, we 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.

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 [33,64]. 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.

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.

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 dismissed. Moreover, as explained below, 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" [34].

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 which 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" [35]. Professor Clarke has perhaps 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 non-conformism and dissent would be muted to the point envisaged by the anti-utopian novelists.

There is at least one example from United States history where supposedly confidential records were 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 [36]. By the Spring of 1942, the United States Government forced persons of Japanese descent, including United States citizens, to relocate from their homes on the West Coast and report to “Relocation Centers” [37].

### *Function Creep*

The biometric-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, to improve airport security, to protect our 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 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 recordkeeping 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.” By 1961, the Internal Revenue Service (IRS) began using the SSN for tax identification purposes. By 1997, “[e]verything from credit to employment to insurance to many states' drivers licenses requires a Social Security Number.” 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, a Russian proverb aptly identifies the danger of biometrics for freedom-loving Americans, “If you are a mushroom, into the basket you must go.”

### *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 their privacy.

Analogies can be drawn from previous cases where the Government has used cutting-edge technology to intrude in an area where 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 [40,65]. Fearful that industrial competitors might try to steal its trade secrets, Dow took elaborate precautions at its facility. Despite the elaborate precautions the company took to ensure its privacy, the Supreme Court, in a 5-4 vote, found that Dow had no reasonable, legitimate and objective expectation of privacy in the area 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” [41].

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

#### *The Case for Biometrics*

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 broader 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[18].” 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 materials and that serial killers do not slip out of prison by masquerading as someone else. These same concerns related to the use of false identity really 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 one time for benefits using an alias or otherwise false information about themselves. Many experts believe that fraud in entitlement programs, like welfare, can be as high as ten percent, which translates in dollar terms to over \$40 billion a year in potential savings.

Biometrics is being used to help stop this fraud. Bob Rasor, a senior U.S. Secret Service official, commented that, “Biometrics would put a sudden and complete stop to as much as 80% of all fraud activity.” In Connecticut, which has embarked on a robust biometric identification program for welfare recipients known as the Digital Imaging System (DIS), the state's Department of Social Services (DSS) “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 her entitlement because there is simply less money to go around.

To the extent 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 x-byte numerical template used as a biometric identifier. Secondly, 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 of the law 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 or the emergence of an undisciplined secondary market is real. With respect to private sector use of biometrics, viable options exist for our nation's policymakers. For a more detailed analysis of this biometric blueprint proposal, refer to [41,43].

### **Cultural, Religious, Philosophical Objections**

#### *Cultural: Stigma & Dignity*

Simon 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 [44]. 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 [67].”

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 survey of 2,378 entitlements recipients in San Antonio, Texas, who participated in a biometric 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” [45]. Survey data in Connecticut and other states suggests similar results [46].

#### *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, 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 Pat Robertson expresses doubts about biometrics and notes how the technology is proceeding according to Scripture [47]. 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.

Recently, in one of the first legal challenges to government use of biometrics, New York courts upheld a decision of the New York State Department of Social Services

to discontinue public assistance payments where a recipient refused to provide her biometric on religious grounds [68]. Similar objections have also been made in the context of the Government's mandated provision of social security numbers. In *Bowen v. Ray*, a leading Supreme Court case dealing with this issue, a Native American objected to the provision of a SSN for his minor daughter's application for welfare assistance as a violation of the family's Native American religious beliefs. The Court refused to sustain this challenge [48].

As these cases demonstrate, the courts are experienced in dealing with similar 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.

#### *Philosophical: Biometric-Based Branding*

Biometrics merits criticism on the grounds that a biometric identifier is nothing more than biometric-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 which could be implanted in humans, the biometric identifier will similarly serve the interests of the State [49]. Biometrics are another example of the State taking 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 to use biometrics. When biometrics is used in the public sector, the use will be for legitimate purposes and will be overseen by democratic institutions.

#### *Actual Physical Harm; Physical Invasiveness*

To the author's knowledge, there are no actual 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.

Any liability resulting from any proven 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 [50].

### **Biometrics as Privacy's Friend: Support for Biometrics**

#### *Biometrics Protects Privacy by Safeguarding Identity and Integrity*

While critics of biometrics contend that this new technology is privacy's foe, the opposite is, in fact, 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 with the present access systems which tend to be based on passwords and PINs by clandestinely obtaining these codes. They then surreptitiously access a legitimate customer's account or ATM. The honest citizen effectively loses control over her personal account information. Her financial integrity is compromised and her finances are gone because a criminal has gained unauthorized access to the information. In effect, she has suffered an invasion of her privacy related to her financial integrity. With biometric-based systems, identity theft, 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.

#### *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 PINs, a biometric identifier is required 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 compartment 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 Internal Revenue Service official had to use her 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.

#### *Biometrics as Privacy Enhancing Technology*

Beyond protecting privacy, biometrics can be seen as enhancing privacy. There are several newly-developed biometric technologies which use the individual's physical characteristic to construct a digital code for the individual without storing the actual physical characteristics in a database [51,22,24].

The applications of this type of anonymous verification system are extensive. Most notably, such a biometric-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 in *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 should really be aimed at contemporary information systems which are the result of economic, political and technological change or the criticisms fail to acknowledge why knowing an individual's identity is necessary. As the next section explains, the use of biometrics might provide for even further individual privacy protections through a phenomenon known as biometric balkanization.

### **5. Biometric Centralization vs. 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 would 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. The popularity of finger imaging is explained primarily by its consistency and uniqueness, the fingerprint's long acceptance by the public, and extensive competition in the finger imaging market leading to rapidly decreasing user costs, among other factors.

For example, with regard to public acceptance of finger imaging, a survey of 1,000 adults revealed that 75 percent 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 over half of those surveyed saying they had been fingerprinted at some point in their lives. Only twenty percent thought that fingerprinting stigmatizes a person as a criminal [52].

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. However, this view overlooks one of the great strengths of the current biometric market: It offers many robust technologies which allow 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 multiple biometrics will be deployed 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 the 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, biometric balkanization offers maximum flexibility to the private or public actor that will use the technology. The actor can tailor a specific biometric

program to meet 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 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 the tax authorities monitoring returns.

Secondly, biometric balkanization might actually mean a synergy of the actors' 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 biometric technologies, the individual gains greater protection for private information.

Biometric balkanization could also lead to the safeguard of biometric compartmentation 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 finger geometry pattern captured at Disney World would be of little value to tax authorities investigating phony signatures on fraudulent tax returns from the Sunshine State.

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

On balance, however, the greater threat to privacy will likely not arise from the use of advanced technology to monitor 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 biometric blueprint, or plan to safeguard biometric identification information for which they are responsible. Accordingly, limited government regulation should be viewed as biometric technology-promoting and not biometric technology-opposing.

## **6. Conclusions**

Biometrics is a new technology which 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 Learned 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

biometrics present. The situation is compounded in that the American approach to privacy matters has tended to be ad hoc and piecemeal. 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 aim. To the extent 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 compartmentation viable.

We are eyeball to eyeball with a new technology reality that promises greater security and efficiency for both its public and private sector users. Biometrics can be used in worthwhile ways and, at the same time, safeguard legitimate privacy concerns. Now is not the time to blink.

## Acknowledgments

The author gratefully acknowledges the invaluable assistance he has received from Arthur S. DiDio, M.D., J.D., Ivan Fong, Esq., Professor Steve Goldberg, Jonathan Massey, Esq., Professor Julie R. O'Sullivan, and Shirley Cassin Woodward, Esq. who contributed comments to earlier versions of this chapter.

## References

- [1] President William J. Clinton, Commencement Address at Morgan State University, May 18, 1997.
- [2] R. Chandrasekaran, "Brave New Whorl: ID Systems Using the Human Body Are Here, But Privacy Issues Persist," *Washington Post*, March 30, 1997.
- [3] A. Davis, "The Body as Password," *Wired*, July 1997.
- [4] J. D. Woodward, "Biometric Scanning, Law & Policy: Identifying the Concerns; Drafting the Biometric Blueprint," *University of Pittsburgh Law Review*, Fall 1997.
- [5] S. Goldberg, *Culture Clash: Law & Science in America*, New York University Press, NY, 1994.
- [6] *The T. J. Hooper*, 60 F.2d 737 (2d Cir.) cert. denied, 287 U.S. 662 (1932)(Hand, J.).
- [7] B. Miller, "Everything You Need to Know About Automated Biometric Identification," *Security Technology & Design*, April 1997.
- [8] P. T. Higgins, biometric consultant, in Washington, D.C. (Jan. 13, 1998).
- [9] C. Tilton, "Put a Finger on Your Security," *Security Advisor*, Premiere, 1998.
- [10] K. McManus, "At Banks of Future, An Eye for an ID," *Washington Post*, May 6, 1996.

- [11] G. Roethenbaugh, "Biometrics: A Global Perspective," in *BiometriCon '97 Conference Proceedings*, March 12-14, Arlington, VA, 1997.
- [12] C. Fried, *An Anatomy of Values*, Harvard University Press, Cambridge, MA, 1970.
- [13] R. B. Parker, "A Definition of Privacy," *Rutgers University Law Review*, Vol. 27, pp. 275, 1974.
- [14] T. Gerety, "Redefining Privacy," *Harvard Civil Rights-Civil Liberties Law Review*, Vol. 27, pp. 233, 1977.
- [15] *United States v. Westinghouse Elec. Corp.*, 638 F. 2d 570 (3rd Cir. 1980) (holding that medical records of a private sector employee, while within the ambit of constitutional privacy protection, could nonetheless be disclosed to a government agency upon a proper showing of governmental interest).
- [16] *Griswold v. Connecticut*, 381 U.S.479, 1965.
- [17] *Smith v. Maryland*, 442 U.S. 735, 1979.
- [18] P. Mell, "Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness," *Berkeley Technology Law Journal*, (footnote omitted), 1997.
- [19] M. Rotenberg and E. Cividanes, *The Law of Information Privacy: Cases & Commentary*, 1997.
- [20] *Whalen v. Roe*, 429 U.S. 589, 1977.
- [21] *Smith v. Maryland*, 442 U.S. 735, 1979.
- [22] A. Cavoukian, Assistant Privacy Commissioner of Ontario, "Go Beyond Security -- Build in Privacy: One Does Not Equal the Other," (May 1996) available at [http://www.microstar-usa.com/tech\\_support/faq/privacy.html](http://www.microstar-usa.com/tech_support/faq/privacy.html).
- [23] *United States v. Miller*, 425 U.S. 435, 1976.
- [24] "Privacy and Data Security Targets of Mytec's Commercialization Strategy," *PR Newswire*, June 20, 1997.
- [25] E. Alderman and C. Kennedy, *The Right to Privacy*, (1995).
- [26] S. G. Davies, "Touching Big Brother: How Biometric Technology Will Fuse Flesh and Machine," *Information Technology & People*, 1994.
- [27] M. Skoler, "Finger and Palm Prints: A Window on Your Health," *Glamour*, Apr. 1984.
- [28] H. Chen, *Medical Genetics Handbook*, W. H. Green, St. Louis, MO, pp. 221-226, 1988.
- [29] "Gastroenterology: Fingerprinting GI Disease," *Johns Hopkins Physician Update*, pp. 5, April 1996.
- [30] S. LeVay, *Queer Science: The Use and Abuse of Research into Homosexuality*, MIT Press, Cambridge, MA, 1996.
- [31] B. Bates, *A Guide to Physical Examination and History Taking*, 5th edition, 1991.
- [32] R. Clarke, "Human Identification in Information Systems: Management Challenges and Public Policy Issues," *Information Technology & People*, December 1994.
- [33] J. Hall, "For New ATM, the Eyes Have It," *Trenton Times*, September 19, 1995.
- [34] "FutureBanking," *American Banker*, October 21, 1996.
- [35] U.S. Department of Health, Education and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, MIT Press, Cambridge, 1973.
- [36] J. Toland, *Infamy: Pearl Harbor and Its Aftermath*, Anchor, NY, 1992.
- [37] *Korematsu v. United States*, 323 U.S. 214 (1944).
- [38] *Olmstead v. United States*, 277 U.S. 439, 479 (1927) (Brandeis, J. dissenting).
- [39] *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir. 1993).
- [40] *Dow Chemical Co. v. United States*, 476 U.S. 227 (1985).
- [41] J. D. Woodward, Testimony on "Biometrics and the Future of Money" before the Subcommittee on Domestic and International Monetary Policy, Committee on Banking and Financial Services, U.S. House of Representatives, May 20, 1998.
- [42] D. Mintie, "Report from Connecticut," *Biometrics in Human Services User Group Newsletter*, Vol 3, No. 1, March 1997. <http://www.dss.state.ct.us/faq/bhsug031.htm>.

- [43] J. D. Woodward, "Private Sector Use of Biometrics: The Need to Safeguard Privacy Concerns -- The Need for a Biometric Blueprint," in *CTST '98 Proceedings*, Washington DC, 1998.
- [44] "Foolproof Identification Methods Create Privacy Worries," (*National Public Radio Broadcast*, Segment number 2360, October 8, 1996.
- [45] C. Edwards, "Reports from the States: The Texas Lone Star Imaging System," *Biometrics in Human Services User Group*, May 1997. <http://www.dss.state.ct.us/faq/bhsug04.htm>.
- [46] D. Mintie, "The Connecticut DSS Biometric Project and EBT Card: Implementation Issues," in *CTST '96 Government Conference Proceedings*, Arlington, VA, 1996.
- [47] "Biometrics: Chipping Away Your Rights?," *The 700 Club Fact Sheet*, VA, October 9 1995.
- [48] *Bowen v. Ray*, 476 U.S. 693 (1986) (holding that the Free Exercise Clause of the First Amendment does not compel the Government to accommodate a religiously-based objection to the provision of a Social Security Number for Little Bird in the Snow, a minor welfare recipient).
- [49] R. E. Smith, "The True Terror is in the Card," *New York Times Magazine*, September 8, 1996.
- [50] *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1993).
- [51] "Test Center Comparison," *Infoworld*, June 16, 1997.
- [52] "People Patterns: Fingerprints? No Problem," *Wall Street Journal*, January 31, 1997.
- [53] R. Nanavati, Presentation on "Top Ten Trends in Biometrics" at CardTech/SecurTech Conference, in Washington, D.C, April 27, 1998.
- [54] F. James, "Body Scans Could Make ID Process Truly Personal," *Chicago Tribune*, June 4, 1997.
- [55] D. R. Richards, "Rules of Thumb for Biometric Systems," *Security Management*, October 1, 1995.
- [56] G. Roethenbaugh, Biometrics Explained, 1998. Available at: <http://www.ncsa.com/services/consortia/cbdc/explained.html>.
- [57] *United States v. Miller*, 425 U.S. 435 (1976).
- [58] S. D. Warren & L. D. Brandeis, "The Right to Privacy," *Harvard Law Review*, 1890.
- [59] A. F. Westin, *Privacy and Freedom*, 1967.
- [60] R. E. Cytowic, "All in the Genes," *Washington Post*, September 1, 1996, (book review).
- [61] N. Hawkes, "Fingerprint Clue to Health," *Times of London*, February 26, 1996.
- [62] "Briefs," *Biometric Technology Today*, April 1998.
- [63] Dr. F.P. Nasrallah, Assistant Professor of Ophthalmology at George Washington University, and Dr. Arthur S. DiDio, M.D. in Washington, D.C., personal communication, Apr. 4, 1996.
- [64] M. Barthel, "Banks Eyeball Sci-Fi Style Identification for ATMs," *American Banker*, Sept. 22, 1995.
- [65] *United States v. Knotts*, 460 U.S. 276 (1983) (holding that governmental surveillance by beeper placed in a container with the consent of the owner of the container did not violate the reasonable expectations of privacy of the defendant who placed the container in his car and drove over public highways).
- [66] L. Tribe, "The constitution in cyberspace: Law and Liberty beyond the electronic frontier," Keynote address at The first conference on Computers, Freedom, & Privacy, 1991. Available at [http://www.eff.org/pub/Legal/cyber\\_constitution.paper](http://www.eff.org/pub/Legal/cyber_constitution.paper) (viewed Nov 28, 1997).
- [67] United States General Accounting Office, *Electronic benefits Transfer: Use of biometrics to deter fraud in the nationwide EBT program*, GAO/OSI-95-20, pp. 6-7, Sept. 1995.
- [68] *Buchanan v. Wing*, \_\_\_N.Y.S.2d\_\_\_ (N. Y. App. Div. 1997).

