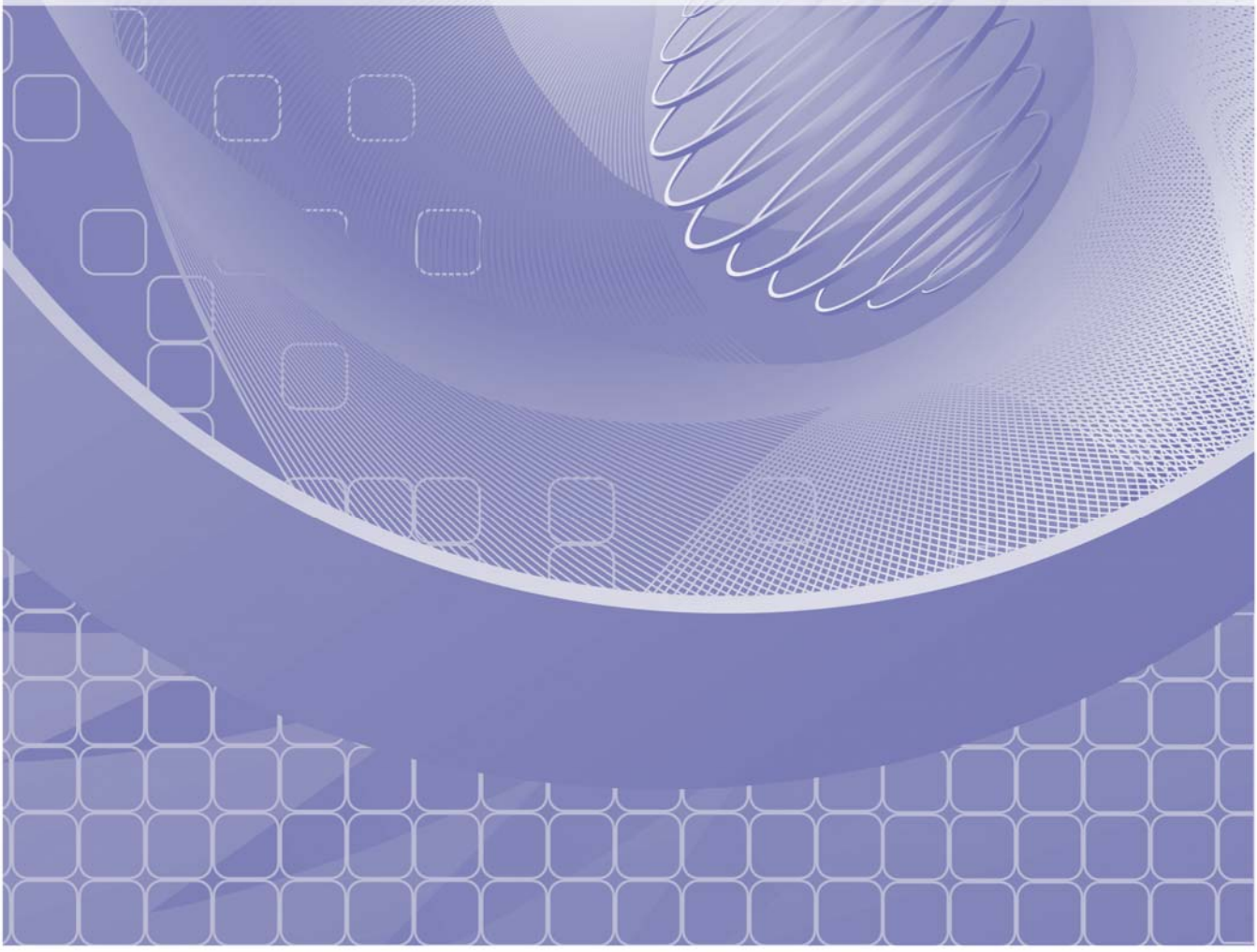
NBSP Publication 0105

March 2006

Report on

United States Federal Laws Regarding Privacy and Personal Data and Applications to Biometrics



www.nationalbiometric.org

National Biometric Security Project

Table of Contents

Section Page

I. Introduction 4
II. Privacy Law Applicable to the Public Sector 13
A. Constitutional Privacy Law 14
1. Specific Constitutional Provisions 15
a. First Amendment 15
b. Third Amendment 16
c. Fourth Amendment 16
d. Fifth Amendment 17
e. Ninth Amendment 17
f. Fourteenth Amendment 18
2. Case Law Examination of the Right to Privacy 19
a. Informational Privacy 20
b. Physical Privacy: Privacy in One's Personal Space 27
c. Physical Privacy: Privacy in One's Body 32
B. Statutory Privacy Laws 41
1. The Privacy Act of 1974 & FOIA 41
a. What is a Record? 42
b. What is a System of Records? 48
c. Privacy Act Requirements and Penalties for Noncompliance 49
d. The Computer Matching and Privacy Act of 1988 50
2. Executive Order 12333 52
III. Privacy and National Security 57
A. National Security Laws 58
B. Immigration Laws 63
C. International Considerations 65
IV. Privacy Law Applicable to the Private Sector 68
A. HIPAA 69
B. Statutes Governing Banks 72
1. The Gramm-Leach-Bliley Act 72
2. The Right to Financial Privacy Act 73
3. The Bank Secrecy Act 74
4. The Electronic Funds Transfer Act 74
5. The Fair Credit Reporting Act 74
C. Statutes Governing Computers 75
1. The Computer Security Act of 1987 75
2. The Computer Fraud and Abuse Act 75
V. Common Law Tort Privacy Rights 77
VI. Conclusion: Impact of United States Privacy Law on the Use of Biometrics 79
Glossary of Terms 91
Bibliography 92

Appendix A: Pending Legislation ……..98
Acceptance Form…… 113

BIOMETRICS FOR NATIONAL SECURITY

"We would like to live as we once lived, but history will not permit it."

John F. Kennedy

I. INTRODUCTION

On January 28, 2001, football fans walked through the turnstiles at Raymond James Stadium in Tampa Bay, Florida to watch the Super Bowl. As they entered the stadium their faces were scanned, converted to digital images, processed by a computer algorithm, and compared to a law enforcement database. All of this was done unbeknownst to the fans as it occurred. The outrage amongst those who protested was unambiguous: this was "Big Brother."[1]

Seven months later, that outrage was temporarily silenced when nineteen terrorists boarded four domestic flights and carried out an attack against America on an unprecedented scale. More than half of those nineteen terrorists were "flagged" as potential risks by the Federal Aviation Administration's profiling system. As many as fifteen of the nineteen terrorists were potentially vulnerable to interception by border authorities. Yet all nineteen were able to board the four planes and carry out their horrific plan.[2]

---

[1] Big Brother refers to the government leader in the novel *1984*. *1984* is about a totalitarian society in which the government spies on the upper classes in their homes and improper thoughts are crimes. Big Brother has become synonymous with invasive government. GEORGE ORWELL, 1984 (1949).

[2] NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 1-4, 384, n. 2 to Chapter 1 (2004) [hereinafter The 9/11 COMMISSION REPORT].

The attacks of September 11, 2001 changed the country. For many, priorities shifted. The need for increased security was brought to the top of national consciousness. According to proponents of biometrics, biometric technology provides an answer to a challenge of utmost importance: how to balance the need for privacy and civil liberties with the need to protect against threats to life and security. However, while such technology may provide an answer, it also creates an opportunity for mischief. It is this potential for misuse that frightens people.

Knowledge is power.[3] Biometric recognition technology works by collecting identifiable physiological or behavioral information about people. The power of biometric recognition technology is simultaneously reassuring and frightening to some of those concerned about its use. Biometric technology's tremendous potential as a key component of a program for defending the United States against terrorist attacks, fighting domestic crime, controlling access to secure places and information, and a myriad of other applications, is surrounded by uncertainty of laws, ambiguous guidelines, and public concern over potential abuse.

Clearly, the security system in place in the summer of 2001 failed. The 9/11 Commission, an independent bi-partisan panel appointed to examine the attacks, found that a more effective use of available information and an analysis of the flagged passengers' travel documents and travel patterns could have identified and intercepted several of the hijackers.[4] At least two and possibly as many of thirteen of the hijackers presented falsified passports.[5] Among its recommendations on how to safeguard against future terrorist attacks, the 9/11 Commission has recommended the implementation of a comprehensive screening system that includes the use of biometric identifiers.[6]

The purpose of this report is to provide an analysis of how the applicable United States laws impact the use of biometrics in general in the United States, particularly with respect to national security. This report will demonstrate that the use of biometrics as part of the nation's efforts to increase security and protect against future terrorist attacks are not at odds with the protection of privacy and civil liberties. This report will further demonstrate how, under the current legal system and state of the law, biometrics can legally be used as a system to verify identity in virtually any situation and, under certain circumstances, to positively identify individuals through the use of databases.

A common misconception is that because biometrics are genetically personal to the individual, biometrics are somehow more private than other forms of identification, such as Social Security numbers, which are assigned by the government. However, there

---

[3] FRANCIS BACON, MEDITATIONES SACRAE, DE HAERESIBUS (1597).

[4] The 9/11 COMMISSION REPORT at 384. The 9/11 Commission is formerly the National Commission on Terrorist Attacks Upon the United States. It was established by President George W. Bush and the United States Congress in November 2002. It was directed to examine the facts and circumstances surrounding the September 11th attacks, identify lessons learned, and provide recommendations against future acts of terrorism. The 9/11 Commission Report was released on July 22, 2004.

[5] *Id*. at n. 32 to Chapter 12.

[6] *Id*. at 387-389.

is arguably nothing inherently private about a biometric. For the most part, a person's biometrics commonly used for instantaneous identification are held out to the public and are readily accessible to others. However, as expected, the concept of privacy seems to be more compelling to the average person as the particular physiological biometric feature used in identification becomes less apparent to the naked eye, such as your unique facial features, or, even less apparent, your hand dimensions, or even more difficult to discern, your fingerprints or your iris patterns. Most everyone understands that any hard surface can readily capture a person's fingerprints. Technology has now developed such that a mere video camera can capture the unique features of your face or even the unique patterns of the iris of your eye.

Notwithstanding the initial perceived privacy concerns of the average person, in the law privacy concerns generally arise when biometrics are used to provide access to other information about an individual or are used in a way that infringes upon a person's rights. For example, what was disturbing about the 2001 Super Bowl event was not necessarily the video cameras that captured the faces of the football fans, but rather the fact that those images were then compared to images in a law enforcement database.

An important concept in applying privacy law to biometrics is the distinction between the two forms of biometric recognition: identification and verification.[7] Identification biometric systems are used to figure out who a person is and can occur without the person's knowledge or consent. The use of facial-recognition technology at the 2001 Super Bowl is an example of such a covert identification system. The facial images covertly captured at that event were converted to a template and searched against a database of previously obtained biometric templates of suspected terrorists and known criminals.[8] Because identification systems require a databank that may contain personal information, and because they can be used without the subject's knowledge or consent, such as in surveillance, the privacy concerns are intensified.

Verification biometric systems work like PIN's or passwords. Unlike identification systems, verification systems are used on a purely voluntary basis (i.e. not secretly). Verification systems make sure you are who you claim to be. They only require two pieces of information: something representing your identity (such as a user name to retrieve your biometric template or a smart card with your template embedded in it) and your biometric information (such as your hand to create your hand geometry template).[9] It should be noted that verification systems can be connected to databanks,

[7] See the *Glossary of Terms* herein for the special definitions of the verbs *identify*, *recognize*, and *verify*, as they have been adopted by the biometric industry and as they are used in this report.

[8] JOHN D. WOODWARD, JR. ET AL., BIOMETRICS: IDENTITY ASSURANCE IN THE INFORMATION AGE 247 (2003).

[9] For example, iris recognition technology can be used as a verification system to limit access to a bank account by embedding the account owner's biometric information into his ATM card. To gain access to the account, the account owner would insert his card into the ATM as usual, and then, instead of entering a PIN to gain access, he would look into the camera. The system would then be able to verify, by matching the biometric information of his iris with the biometric information encoded in the card, that he is, in fact, the account owner and cardholder.

but unlike recognition systems it is not a necessary component.[10] The need for the subject's consent and the lack of a databank greatly reduces the privacy concerns.

Recognition
Identification vs. Verification

Identification	Verification
Who is this person?	Is this person who she says she is?
1:N	1:1
Databank with linked personal information	No Databank[11]
Overt or Covert	Overt

There are currently no legal issues with respect to verification systems, other than the issue of whether an individual is *required* to identify himself in a given situation. However, this issue is present regardless of the form of identification used or presented by the individual and is not specific to biometric identification. The Supreme Court recently decided a seminal case regarding whether and under what conditions a person is required to identify himself to a police officer.[12] This case could have far-reaching implications on privacy rights.

Biometric verification systems are currently used for many purposes, such as controlling access to certain secured locations, and could be legally used in the United States for virtually any purpose where verification of identification is required. Verification of identity is legally required for many purposes, such as driving, border crossing, and obtaining government assistance. The mere act of verification to confirm truthfulness (i.e. to confirm a person is who he purports to be) by using information the

[10] Most authors on this subject do not classify a system where you retrieve your biometric through a PIN a databank. In this report, unless otherwise stated, a reference to a databank is a reference to a databank used in connection with a "one to many" identification system, and does not refer to a "one to one" databank.

[11] There is no databank used in the verification process because you are only using your biometric template (i.e., a single biometric template) either embedded in your identification document (e.g., passport, driver's license, smart card) or retrieved from a databank used for storage only. In actuality you are not using the databank (i.e., the other biometric templates) in the process of verification (the one to one comparison), but instead, you are simply employing the single biometric template which was retrieved from storage through the use of a PIN or other user code without any examination or evaluation of the other biometric templates in storage. In contrast, in the identification process, you actually would be searching the contents of the other biometric templates in the databank in order to perform the task of identification. It is the actual search or evaluation of the contents of biometric templates of others that creates a privacy concern by others who have templates in the databank.

[12] The case of *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, No. 03-5554, 542 U.S. __(2004), *aff'd* 59 P.3d 1201 (Nev.2002) is discussed *infra* at II.A.2.a.

person has voluntarily given (such as a photograph or other biometric) does not raise any privacy issues.[13] Accordingly, in examining the legal issues surrounding the use of biometric recognition in this report, such issues are generally only relevant to identification systems.

Despite the growing use of biometric technology, very few laws currently exist that even mention biometrics, let alone the use of biometrics with respect to privacy. However, as the use of biometrics becomes more pervasive, especially in the wake of the September 11th attacks, we can anticipate that in the near future, a significant portion of the public will become increasingly concerned over its implications with respect to privacy. Anticipating that the government's use of biometric recognition technology will eventually lead to an Orwellian "Big Brother" America, some people are already up in arms, warning that such "function creep" is inevitable.[14] Their ultimate concern is that the scope of biometric recognition technology uses will broaden indefinitely and invasively. Others hail the use of biometrics as not only invaluable to our nation's security, but as a formidable protector of privacy. One New York Times Op-Ed columnist recently suggested that a standardized national ID card containing a photograph, a fingerprint, and a bar code could both enhance privacy and provide security by "simultaneously reduc[ing] identity theft and mak[ing] life tougher for terrorists."[15]

Privacy law is not an easy area of law to understand or interpret. Unlike Great Britain, which mentions privacy in its constitution, the United States does not clearly define an individual's privacy rights.[16] Americans do not have an *express* constitutional right to privacy. The idea of a right to privacy is a relatively recent concept first expressed as a person's "right to be let alone" in an 1890 legal journal.[17] Privacy rights in the United States derive from a miscellany of constitutional interpretations, statutes, and common law.[18] Privacy law is dynamic and in a constant state of development.

Adding to the clutter is the fact that statutory privacy laws have developed more as piecemeal reactions to social and political events than as a carefully constructed set of laws codifying a basic human right. For example, video stores are subject to restrictions with respect to releasing information on videos rented by a customer. This statute was enacted in response to the media's release of a list of videos rented by Robert Bork, one

[13] Other means of verification to confirm identity are social security number, mother's maiden name, date of birth, and zip code.
[14] The concept of function creep is discussed *infra* in the Conclusion at Section VI.
[15] Nicolas D. Kristof, *May I See Your ID?*, N.Y. TIMES, March 17, 2004 (Op-Ed).
[16] Britain adopted the Convention for Protection of Human Rights and Fundamental Freedoms (European Convention of Human Rights) through the United Kingdom's Human Rights Act of 1998 in 2000 including Article 8 dealing with privacy: "...everyone has the right for his private and family life, his home and his correspondence..."
[17] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).
[18] Common law is law based on previous court decisions, i.e. precedent, rather than statutes. American common law extends to English common law predating the American Revolution.

of Ronald Reagan's 1987 Supreme Court nominees.[19] Just about every existing privacy statute has a similar story behind it.

Privacy law can be broken down into two main bodies – laws that apply to the government (the public sector) and laws that apply to everyone else (the private sector). Constitutional law and statutory laws govern the public sector. Statutory laws govern the private sector. Both the public sector and private sector are subject to common law tort privacy rights.[20]

Sources of Privacy Law

Public Sector	**Private Sector**
U.S. Constitution	--------
State constitutions	--------
Federal law	Federal law
State law	State law
Common law	Common law

Within these two groups of laws, our legal system recognizes different types of privacy rights, including informational privacy, physical privacy, decisional privacy, and communications privacy. In terms of biometrics, informational privacy and physical privacy are the two most critical areas. Informational privacy allows a person to control his or her own personal data. Although it may be debatable whether a biometric is personal data, biometrics are often linked to other information that is personal data. Accordingly, biometrics falls under the informational privacy category. Physical privacy encompasses the right to control access to one's body and personal space, which would arguably include the right to control access to one's biometric information. The two other types of privacy rights recognized by the courts, decisional privacy and communications privacy, could also impact the use of biometrics, but to a much lesser degree.

[19] RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS 494 (2d ed. 2002).
[20] A tort is a wrongful act by which another is injured. A law has not necessarily been broken, but someone has suffered damages and there are grounds for a private lawsuit.

Recognized Privacy Rights

Privacy Type	Definition
Informational Privacy	The right to control one's own personal data e.g. criminal, financial, and medical records.
Physical Privacy	The right to control access to one's body and personal space, e.g. search and seizures, Peeping Toms, blood tests, DNA swabs.
Decisional Privacy	The right to make autonomous decisions about one's personal life, e.g. abortions, sexual preference.[21]
Communications Privacy	The right to speak to someone else without being heard by others, e.g. intrusive technological hearing devices.[22]

Privacy rights are generally subject to balancing the privacy interests of individuals against the interests of society, such as national security and law enforcement. There is a constant tension between privacy and civil liberties in general, and these societal concerns. During times of relative peace and stability, Americans are generally more concerned about civil liberties. During times of war or instability, Americans are generally more willing to forego some degree of liberty in exchange for increased security.

A recent example of this is the USA PATRIOT Act (the "Patriot Act").[23] Passed in the wake of the September 11th attacks, the Patriot Act strengthened the government's

[21] Requiring a biometric identifier for security purposes could have an indirect effect on a person's right to make a constitutionally protected choice. For example, if abortion clinics, as a security measure, require anyone who enters to provide biometric information, a woman who wants an abortion but wants to retain a certain degree of anonymity may feel a barrier to her decision to have an abortion. In fact, the Supreme Court's premier informational privacy case of *Whalen v. Roe*, 429 U.S. 589 (1977) (discussed *infra* at Section II.A.2.a) also addressed decisional privacy in that the Court reasoned that a person's discomfort with disclosing his personal information to the government with respect to certain prescription drugs could impact the person's decisions about using such drugs.

[22] Communications privacy concerns could arise with respect to voice recognition technology by diminishing one's ability to remain anonymous in speech. (As used in this report, voice recognition technology refers to the technology that can recognize (i.e. identify or verify) a person through their unique voice; it does not refer to the technology that converts the spoken word to type.) Federal and state wiretap laws govern the ability of both the government and private individuals to record private conversations. Recording a conversation, however, is not the same as using technology to identify the speaker through his voice.

ability to secure the nation against future attacks by providing a freer exchange of information among government agencies and broadening the government's surveillance powers. Some complain, however, that the increased security is at the expense of privacy and civil liberties.[24]

The Patriot Act requires the Attorney General to explore the feasibility of using biometrics at ports of entry, such as airports and border crossings. This mandate led to the US-VISIT program, implemented earlier this year.[25] The Patriot Act also permits other uses of biometrics, such as by law enforcement, to identify terrorists and other individuals who may pose a threat to national security.

In the United States, protecting individuals from each other is largely carried out at the state level, with each state having its own set of codified criminal laws that are enforced by its own law enforcement and criminal justice systems. The government's power to enforce its laws and secure its citizens is limited by the Constitution, including the Fourth Amendment, which protects not just citizens, but all persons, against "unreasonable searches and seizures." Because the law with respect to the Fourth Amendment is well developed, a large section of this report will explore some of the seminal Fourth Amendment cases and analyze how the reasoning behind their decisions could be applied to the government's use of biometrics in national security and law enforcement.

This report will examine privacy laws applicable to the biometrics industry in both the public and private sectors. A separate section of this report is devoted to the application of biometric recognition technology in national security. This report concludes by discussing the applicability of the current state of the law to the biometric industry.

This report will demonstrate how courts apply a balancing test to determine whether and in what situations the government's interest in protecting society and enforcing laws outweighs the individual's privacy interest. Factored into this balancing test on the government's side is the importance of the government's interest, whether such interest amounts to a "special need," and the safeguards the government has taken to protect any information collected. On the individual's side, the courts look to whether the person has a reasonable expectation of privacy based on societal norms and the sensitivity of the information. Included in the review of the expectation of privacy is the level of intrusion, the setting and location of the invasion, and the reasonableness (i.e. society's acceptance) of any technology used by the government to obtain information, such as sensory-enhancing technology.

---

[23] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (The USA Patriot Act), Pub. L. No. 107-56, 115 Stat 272 (2001).

[24] On February 4, 2004, New York City became the 247th community in the United States to approve a measure condemning the Patriot Act when the New York City Council passed a resolution criticizing the act's infringement on privacy rights, available at http://www.epic.org/privacy/terrorism/usapatriot/ (Feb. 5, 2004).

[25] The US-VISIT Program is discussed *infra* at Section III.

Based on an in-depth review and analysis of judicial decisions applying this balancing test, this report will hypothesize on how such a balancing test might be applied in the context of the use of biometric recognition technology in both law enforcement and national security.

This report concludes that the use of biometric recognition technology in and of itself is not illegal and does not pose a threat to privacy or civil liberties. Using biometrics for verification purposes holds no privacy implications whatsoever beyond the question of whether and when a person has a right to anonymity. Privacy concerns only arise with respect to identification systems, and then only with respect to the safeguarding and proper handling of information contained in a database.

It is important to note that this report is a living document subject to future court rulings, new legislation, changing policies, and even shifts in social attitudes about privacy and biometric recognition technology. Although technology will not alter inherent truths, new laws and policies could limit or expand the application of biometrics and the extent biometric recognition technology can be used to unlock such truths.

"It is found by experience that admirable laws and right precedents among the good have their origin in the misdeeds of others."

Cornelius Tacitus
First Century Roman Statesman

II. PRIVACY LAW APPLICABLE TO THE PUBLIC SECTOR

The public sector consists of the federal government, as well as state and local governments. However, there are different public sector privacy laws that apply to the various sectors of the government. While the Constitution generally applies to the government at all levels, each state has its own constitution and set of codified laws. Additionally, there are federal statutes governing federal government agencies.

This section of the report examines laws governing the public sector. As this report only addresses federal privacy laws, state and local privacy laws are not discussed.

Part A of this section discusses constitutional privacy law and the privacy rights that have been construed by the courts to exist in the Constitution. A study of both Supreme Court and some lower court cases examines how judicial interpretations of such constitutional rights may be used in determining how the courts might rule on the constitutionality of government uses of biometric recognition technology.

Part B of this section discusses the statutory laws that govern the public sector. A close examination of the Privacy Act of 1974 and how courts have interpreted the term "record" is included to assist in determining whether biometric information would be subject to the Privacy Act.

A. CONSTITUTIONAL PRIVACY LAW

Unlike free speech, the right to a speedy trial, and the right to bear arms, privacy is not expressly mentioned in the United States Constitution. It has been argued that the right to privacy is implicit in the Constitution through various provisions, including the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. The Fourteenth Amendment is the most often cited and well-known Amendment outside of the Bill of Rights. The Supreme Court has held that there is a fundamental right of privacy "implicit in the Fourteenth Amendment's due process clause."[26]

In recognizing a right of privacy, the Supreme Court has held, in various cases that the right of privacy extends to a range of elements of an individual's life, such as marriage, procreation, contraception, and child rearing.[27] The Supreme Court first recognized a fundamental constitutional right to privacy independent of the Fourth Amendment's search and seizure protections in the 1965 landmark case *Griswold v. Connecticut*,[28] which held that a Connecticut state statute criminalizing the sale of birth control to married couples was unconstitutional. The Supreme Court found that this constitutional right to privacy existed within "specific guarantees" of the Bill of Rights, which "create certain zones of privacy,"[29] and that marriage was "a relationship lying within [such] zone of privacy." [30] However, following that broad interpretation, the Supreme Court has been inconsistent, finding that the right of decisional privacy created by the Constitution extends to certain aspects of life (such as abortion and contraception) but not others (such as the right to die).[31] The Supreme Court case of *Roe v. Wade*[32] was based on the recognition of a right to privacy, specifically a woman's right to decide whether or not to terminate her pregnancy, but which right the Court maintained was not absolute. Like *Griswold*, *Roe* addressed decisional privacy.

The Supreme Court's position on privacy under the Constitution has been largely influenced by social values and political beliefs. For example, since the *Roe* Court determined that a woman had a constitutional right to an abortion, abortion rights have been limited by the more conservative composition of the Court and could be lost entirely

---

[26] *Zablocki v. Redhail*, 434 U.S. 374 (1978).
[27] See, e.g., *Griswold v. Connecticut*, 381 U.S. 479 (1965), *Roe v. Wade*, 410 U.S. 113 (1973), *Carey v. Population Services International*, 431 U.S. 678 (1977), *Pierce v. Society of Sisters*, 268 U.S. 510 (1925).
[28] 381 U.S. 479 (1965).
[29] *Id*. at 484.
[30] *Id*. at 485.
[31] See *Washington v. Glucksberg*, 521 U.S. 702 (1997) (no right to commit suicide), *Cruzan v. Director, Missouri Department of Health*, 497 U.S. 261 (1990) (a mentally competent adult has the right to refuse lifesaving medical treatment).
[32] 410 U.S. 113 (1973).

depending on future appointees to the Court, even though the Constitution has obviously not been amended in this regard.

1. Specific Constitutional Provisions

The following constitutional provisions, either individually or as a whole, arguably invoke a fundamental right to privacy. The law with respect to biometric privacy is in its infancy. Even the law with respect to privacy in general is far from fully developed and continues to change with societal values and beliefs. Accordingly, it is difficult to say with any certainty which constitutional provisions might be construed to be a source of privacy with respect to biometrics. However, each of the below provisions have been found to confer a right of privacy in other contexts. Thus, any of these provisions could conceivably be central to a debate over the right to privacy with respect to biometric information. Following each constitutional excerpt (presented in numerical order and not in order of importance) is a brief analysis of how it may impact the biometrics industry and the use of biometric recognition technology in the United States.

a. The First Amendment

> "Congress shall make no law … prohibiting the free exercise [of religion]; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble …."

The First Amendment has been construed to confer a fundamental right of privacy, protecting people from having to disclose their political leanings or religious beliefs. It has been described by the Supreme Court as imposing limitations on the government's ability to abridge one's "freedom to associate and privacy in one's associations."[33] It is possible that if the use of biometric recognition technology were to become widespread and were used to identify people, for example, at voting booths or to enter a church or a building where a particular organization assembles, violations of the First Amendment could be asserted. Some people have also raised religious concerns over the use of biometrics.[34] Further, as stated in the Introduction to this report, communication privacy concerns could arise with respect to voice recognition technology by diminishing one's ability to remain anonymous in speech.[35] However, it is debatable whether the right to *free* speech confers a right to *anonymous* speech. Arguably, the inability to remain anonymous could infringe upon a person's right to free speech by intimidating the speaker.

---

[33] *NAACP v. State of Alabama*, 357 U.S. 449, 462 (1958).
[34] For a discussion of religious concerns with respect to biometrics, see, e.g. WOODWARD, JR. ET AL., *supra* note 8, at 231.
[35] See *supra* note 14.

b. The Third Amendment

> "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law."

This prohibition against quartering soldiers in one's home recognizes a right to privacy that exists with respect to one's home. Although this amendment is extremely limited in scope and has no application to biometrics, it demonstrates the heightened expectation of privacy with respect to the home, as opposed to invasions of privacy outside the home, where there is a lesser expectation of privacy (e.g. at an airport). An individual's expectation of privacy is used by the courts in balancing the interests of the public (i.e. the government) and the individual.

c. The Fourth Amendment

> "The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Fourth Amendment protects people from having their homes and their bodies searched and property seized (e.g. by the police) without a proper warrant or, absent a warrant, a special need. The warrant must be based on "probable cause" that a crime has been committed and that evidence of such crime might be found in such locale. Thus, the Fourth Amendment permits searches and seizures only in very limited specific circumstances: i.e. upon reasonable cause of evidence of a crime. Accordingly, it is very likely that the Fourth Amendment would be raised as authority for the right of privacy in connection with biometric identification. Because of the likelihood that the Fourth Amendment would be implemented and because of the fact that the law is well developed in this area, an in depth study of the Fourth Amendment is presented in Section II.A.2 herein. Although the protection from search and seizure is generally related to the use of information in a criminal prosecution, such protection has also been applied to protecting individuals in other contexts. The seizure of a biometric will therefore generally require the consent of the individual unless there is probable cause that a crime was committed or a "special need" demonstrated by the government.

d. The Fifth Amendment

> "No person … shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

The Supreme Court has described the Fifth Amendment as reflecting "the Constitution's concern for" one's right to "a private enclave where [one] may lead a private life."[36] The Fifth Amendment prohibits the government from compelling an individual to disclose incriminating information about himself. The Fifth Amendment has been examined in the context of compulsory blood sampling and fingerprinting, which have been found to not violate the Fifth Amendment's protection against being forced to be a witness against oneself.[37] It is, therefore, likely that the same analysis would be applied to other forms of compulsory biometric identification in criminal cases, and that the conclusion would be that compulsory use of biometric identification in the criminal law context is not a Fifth Amendment violation. However, the use of biometrics outside the area of a criminal investigation will be subject to a separate analysis.

e. The Ninth Amendment

> "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

Although little attention has been paid to this amendment in comparison to, for example, the First Amendment, it is perhaps the broadest of all of the amendments. The Ninth Amendment dictates that the absence of a mention of a right (e.g. the right to privacy) does not mean that such a right does not exist. That being said, however, the failure to state a right to privacy does leave wide open for debate (and judicial interpretation) the extent and scope of such right. Accordingly, this Amendment could be used to argue that people have a fundamental right to privacy with respect to their biometric and other personal information.

---

[36] *Tehan v. United States ex rel. Shott*, 382 U.S. 406, 416 (1966).
[37] See, e.g. *Schmerber v California*, 384 U.S. 757 (1966).

f. The Fourteenth Amendment

> " … No State shall ... deprive any person of life, liberty, or property, without due process of law …."

Outside the Bill of Rights, the Fourteenth Amendment is probably the most cited and well-known constitutional amendment. It is also one of the longest and most varied topically, ranging from provisions regarding equal protection of all citizens under the law, to how persons of each State are counted for purposes of electing representatives, to who can be a Congressman, to the validity of public debt. The above-cited language is from what is known as the "due process clause" of the Fourteenth Amendment. It is the Fourteenth Amendment's due process clause that the Supreme Court in 1973 in *Roe v. Wade*[38] construed as giving a woman a limited right to terminate her pregnancy. Because of its historically broad interpretation, it is likely that the due process clause would be central in any constitutional challenge of the use of biometric identification as a violation of a person's right of privacy.

[38] 410 U.S. 113 (1973).

2. Case Law Examination of the Right to Privacy under the Constitution

The previous section presented the constitutional text on which the right to privacy has been built, and briefly described its status with respect to each relevant constitutional provision. This section will show how the courts have used that text to construct each type of privacy right that currently exists. It will go into much greater detail because by scrutinizing the reasoning behind the courts' decisions one can speculate how the courts may rule upon questions involving biometrics in the future.

Is "taking" someone's biometric information a "seizure?" Or is it no more intrusive than requiring someone's photograph for a passport or driver's license? Is surreptitious facial scanning in a public place no more than visual observation of what is held out to the public? Or is there a reasonable expectation of not being recognized by the government when one walks in a public place? What about stopping someone suspected of committing a crime or being affiliated with an international terrorist group and requiring that person to provide biometric information to be matched against a government database? While these questions have never directly been addressed at the judicial level, an examination of constitutional cases may provide some guidance as to how such issues might be decided if presented to a court.

As stated in the Introduction to this report, the two areas of privacy that will most likely impact biometrics are informational and physical. Accordingly, it is these two areas that are examined in depth in this report. First informational privacy law is examined. Next, physical privacy is examined in two contexts: physical privacy in terms of one's physical space, and physical privacy in terms of one's body.

a. Informational Privacy

Informational privacy relates to the right of an individual to keep his personal information private and out of the reach of the government. A key element of such right is the sensitivity of such information and whether an important government need overrides the individual's interest to keep sensitive information private.

Whalen v. Roe

The 1977 case of *Whalen v. Roe*[39] is the first time the Supreme Court addressed the issue of informational privacy. In particular, the case examined the collection, storage, and dissemination of personal information in government databanks. This case is significant because although the Court determined the information to be highly sensitive, it held in favor of the government. In finding that the government-required databank was constitutional, the Court looked to (1) the importance of the government need and (2) the measures the government was taking to safeguard the personal information.

The case involved a New York state law that required identifying information about people taking certain prescription drugs be included in a database. The Court distinguished between informational privacy and decisional privacy, recognizing that the plaintiffs in the case contended that they were harmed on both levels: one, that the information was highly sensitive and its existence in a database was concerning, and two, that this concern impacted the plaintiffs' decisions about using such prescription drugs. The Court pointed out that the statute "threatens to impair both their interest in the nondisclosure of private information and also their interest in making important decisions."[40]

The Court conducted an analysis of balancing the interests of the state against the privacy concerns of the individual. In this case, the State's interests prevailed. The Court held that the State of New York's requirement that certain personal information of a patient be collected and stored with respect to prescriptions of certain drugs considered by the State to be highly dangerous and vulnerable to abuse, did not amount to an invasion of constitutionally protected privacy rights.[41] The Court reasoned that the "remote possibility" of "unwarranted disclosures" did not provide "sufficient reason for invalidating the entire patient-identification program."[42]

The significance of *Whalen* with respect to the biometric industry is that the Court validated a state's mandated collection and retention of personal information while

[39] 429 U.S. 589 (1977).
[40] *Id*. at 600.
[41] *Id*. at 603-4.
[42] *Id*. at 601-2.

simultaneously recognizing that people have an interest in the privacy of personal information. The Court also recognized that informational privacy protections are not limited to unreasonable searches and seizures in criminal investigations. In rendering its decision, the Court looked not only to the reasons for the law, but also examined the measures the State was taking to safeguard the information it collected and maintained. These measures included restricted access and criminal sanctions for unauthorized disclosure. Such precautionary measures were considered when balancing the interests of the State against the individual's right to privacy. In the final paragraph of the decision, the Court stated:

> A final word about issues we have not decided. 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…. The right to collect and use such data for public purpose is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[43]

This language is significant because it underscores the Court's regard for the importance of adequate administrative procedures safeguarding the personal information against unauthorized disclosure. It is clear that this case was decided in favor of the government in large part because the Court felt that the State's administrative procedures provided adequate safeguards to protect personal information. It is interesting that the Court felt the security systems were so sound that there was no possibility of a privacy invasion.

It is also interesting to note that Justice Brennan, in his concurring opinion, expressed concern over the impact of future technology on the integrity of such databanks and their safeguards, stating:

> What is more troubling about this scheme, however, is the central computer storage of data thus collected…. [T]he Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that

[43] *Id*. at 605-6.

> information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.[44]

As demonstrated above, the Court found the information to be sensitive and that there was a right to privacy in that information. However, the Court was persuaded by the fact that adequate measures were in place to protect and safeguard the individuals' privacy and decrease the potential for unauthorized access.

Discrepancy in the Lower Courts

Although bound by prior Supreme Court holdings, the lower courts have shown inconsistencies in interpreting a person's right to privacy with respect to personal information. For example, in a 1999 case in the Eastern District of Pennsylvania cited *Whalen* as supporting the proposition that there is a constitutional "privacy right to avoid disclosure of personal information."[45] In that case, the plaintiff was seeking records of certain troopers regarding eye disability. The defense countered that this was a violation of the Americans with Disabilities Act. The court found that the release raises issues of privacy and, citing *Whalen*, held that the Constitution protects an individual's privacy right against disclosure of personal information. However, in another 1999 decision, *In re Crawford*,[46] the Ninth Circuit found no invasion of privacy in compelling certain preparers (i.e. the debtor's representative) of bankruptcy petitions to disclose their Social Security number on the petition, even though the petitions are public documents and are accessible by the public. The preparer in this case, a paralegal, refused to disclose his Social Security number, stating that he feared it could make him vulnerable to identity theft. Under the balancing test, the Ninth Circuit, in holding against the preparer, reasoned that the government's interest outweighs the individual's right to keep his Social Security number private, after weighing the following factors:

> The type of record requested, the information it does or might contain, the potential for harm in any subsequent nonconsensual disclosure, the injury from disclosure to the relationship in which the record was generated, the adequacy of safeguards to prevent unauthorized disclosure, the degree of need for access, and whether there is an express statutory mandate, articulated public policy, or other recognizable public interest militating toward access.[47]

The court contrasted Social Security numbers with what it felt was far more sensitive and personal information such as HIV status, sexual orientation, and genetic

---

[44] *Id*. at 606-7.
[45] *Wilson v. Pennsylvania State Police*, CA 94-6547, 1999 U.S. Dist. LEXIS 3165, ___ (E.D. Pa. March 11, 1999) (citing *Whalen v. Roe*, 429 U.S. at 599-600).
[46] 194 F.3d 954 (9th Cir. 1999).
[47] *Id*. at 959.

makeup, positing that the disclosure of a Social Security number would not result in "injury, embarrassment, or stigma."[48] The court concluded:

> The speculative possibility of identity theft is not enough to trump the importance of the governmental interests [i.e. requiring the disclosure of the Social Security number for the Bankruptcy Code's "public access" provision]. In short the balance tips in the government's favor. Accordingly, we cannot say that Congress has transgressed the bounds of the Constitution in enacting the statutes at issue here.[49]

One explanation for the different outcomes of these two lower court cases might be the difference in the way the information was safeguarded (or at least the courts' perceptions of how well safeguarded the information was and the likeliness of the information being compromised). Both cases demonstrate how the courts apply a balancing test, weighing the privacy interests against the government or societal interest. In applying the balancing test, the courts strongly consider the safeguards used to protect the information as well as the sensitivity of the information. One wonders if the *Crawford* case were decided today, whether the growing problem of identity theft might have swayed the court in another direction.

Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, et. al.

On June 21, 2004, the Supreme Court issued its decision in the case of *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, et. al.*[50] The case stemmed from the arrest and conviction of Larry Dudley Hiibel under a Nevada statute for refusing to comply with an officer's request to show identification. The officer got out of his car and approached Hiibel, who was standing next to a truck parked on a country road. A young woman, who turned out to be Hiibel's daughter, was inside the truck. The officer suspected he might be the man who was reported as being seen striking a woman inside a truck. After refusing to comply with the officer's repeated requests to show identification, Hiibel was arrested, charged, and eventually convicted of resisting a public officer in violation of a Nevada statute. The statute in question permits an officer to detain a person to ascertain his identity if the officer has reason to believe that person has committed a crime. Hiibel challenged the constitutionality of the State statute on both Fourth and Fifth Amendment grounds. Hiibel claimed this law violated the Fourth Amendment's prohibition on unreasonable seizure and the Fifth Amendment prohibition on self-incrimination.

Several organizations filed amicus briefs, including the ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Privacy Activism in support of Hiibel, and the Criminal Justice Legal Foundation and the National

[48] *Id*. at 13-14.
[49] *Id*. at 960.
[50] No. 03-5554, 542 U.S. __(2004), *aff'd* 59 P.3d 1201 (Nev.2002).

Association of Police Organizations in support of the State. The United States also filed an amicus brief in support of the State.

In its Amicus Brief, the ACLU cited *Berkemer v. McCarty*, 468 U.S. 420 (1984), in which the Supreme Court held that an individual detained during a *Terry*[51] stop is not obligated to respond to the officers questions, even though the officer has the right to "ask the detainee a moderate number of questions to determine his identity and try to obtain information confirming or dispelling the officer's suspicions."[52] "If the officer does not learn facts arising to the level of probable cause, the individual must be allowed to go on his way."[53] Refusing to answer questions has been held to not be grounds for raising suspicion to a level that would warrant arrest.[54]

The United States, in its Amicus Brief, supported its position by pointing out that the Fourth Amendment only protects against "government practices that intrude on a legitimate expectation of privacy" and that "[b]ecause a person's name, like his voice or handwriting, is revealed in a variety of everyday interactions, there is no legitimate expectation of privacy associated with one's identity."[55] The United States further states that even if a requirement that a person comply with a request for identification "implicates legitimate expectations of privacy" such "intrusion on privacy is substantially outweighed by the substantial government interest in compelling disclosure."[56]

The Supreme Court held 5-4 that the law did not violate the Fourth and Fifth Amendments. The four dissenting justices stated that under the Fifth Amendment prohibition of self-incrimination, Hiibel was not obligated to identify himself.

The Court's opinion regarding the Fourth Amendment held that a police officer in the ordinary course of conducting an investigation is free to ask a person to identify himself without implicating Fourth Amendment concerns. To ensure that the resulting seizure (i.e., the detainee's name) is constitutionally appropriate, the law enforcement officer must have reasonable suspicion that the detainee may be involved in a crime. Turning again to the balancing test, the Court stated: "[t]he reasonableness of a seizure under the Fourth Amendment is determined 'by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests.'"[57]

The Supreme Court noted that although the request that a suspect identify himself is well established, "it has been an open question whether the suspect can be arrested and

---

[51] The case of *Terry v. Ohio* is discussed *infra* at Section II.A.2.c.

[52] *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, Brief for the American Civil Liberties Union as Amicus Curiae in Support of Petitioner at 5, citing *Berkemer v. McCarty*, 468 U.S. 420, 439 (1984), *available at* Http://www.epic.org/privacy/hiibel/

[53] *Id*. at 9, citing *Illinois v. Wardlow*, 528 U.S. 119, 125 (2000).

[54] *Florida v. Royer*, 460 U.S. 491, 498(1983) (citing *United States v. Mendenhall*, 466 U.S. 544, 556 (1980).

[55] *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, Brief for the United States as Amicus Curiae Supporting Respondent at 5, *available at* Http://www.epic.org/privacy/hiibel/

[56] *Id*. at 5-6.

[57] No. 03-5554, 542 U.S. __(2004), slip op. at 9, citing *Delaware v. Prouse*, 440 U.S. 648, 654 (1979).

prosecuted for refusal to answer." The Fifth Amendment states that "[n]o person . . . shall be compelled in a criminal case to be a witness against himself." The Court focused on whether providing one's name could even be "incriminating". The Court held that "petitioner's challenge must fail because in this case disclosure of his name presented no reasonable danger of incrimination."[58] The Court noted that "[t]he narrow scope of the disclosure requirement is also important. One's identity is, by definition, unique; yet it is, in another sense, a universal characteristic. Answering a request to disclose a name is likely to be so insignificant in the scheme of things as to be incriminating only in unusual circumstances."[59]

In his dissent, Justice Stevens points out that the majority's conclusion assumes that the disclosure of Hiibel's name would not be used to incriminate him or provide "a link in the chain of evidence needed to prosecute him."[60] Stevens refutes this assumption stating, "[b]ut why else would an officer ask for it?"[61] Stevens argues that Hiibel's identity could be incriminating. Stevens states, "I think that, on the contrary, the Nevada Legislature intended to provide its police officers with a useful law enforcement tool, and that the very existence of the statute demonstrates the value of the information [i.e. the detainee's name] it demands."[62] Interestingly, Justice Stevens, in arguing that "it is clear that the disclosure of petitioner's identity is protected" by the Fifth Amendment privilege, states, "[i]ndeed, if we accept the predicate for the Court's holding, the [Nevada] statute requires nothing more than a useless invasion of privacy." Because Stevens' statement that asking for a person's identification is an "invasion" of privacy embraces the broadest definition of "privacy," it is conceivable that this statement will be cited by those advocates concerned about privacy violations of biometrics as a method of identification. However, even if it were the case that one's name is, as a general rule, private information, if obtaining a person's identity is lawful under the circumstance, the use of biometrics as a means of verifying identity does not violate a person's privacy.

Justice Breyer wrote a separate dissenting opinion with which Justices Souter and Ginsburg joined. Citing dicta from the Fourth Amendment cases of *Terry v. Ohio*[63] and *Berkemer v. McCarty*,[64] Justice Breyer points out the Court noted that the police officer could ask the detainee to identify himself, but the detainee was not obligated to respond. Breyer concludes that, "[t]here are sound reasons rooted in Fifth Amendment considerations for adhering to this Fourth Amendment legal condition circumscribing police authority to stop an individual against his will."[65]

One of the more interesting observations is that the "stop and identify" ordinances (such as the Nevada statute in question) have their origin in traditional vagrancy laws. If society is comfortable with requiring identification in the context of vagrancy, it would

[58] No. 03-5554, 542 U.S. __(2004), slip op. at 11.
[59] *Id*. at 12.
[60] *Id*. at 5.
[61] *Id*.
[62] *Id*. at 6.
[63] The case of *Terry v. Ohio* is discussed *infra* at Section II.A.2.c.
[64] 468 U.S. 420 (1984).
[65] No. 03-5554, 542 U.S. __(2004), slip op. at 3.

seem that in a situation involving threats to life, such as national security, identification would seem appropriate.

It is also interesting to note that the state law in question did not mandate the procurement of proof of identification, only that the subject state his name to the police officer when asked. Therefore, the law contemplates a certain degree of honesty on the part of the subject. It would seem a person wanting to hide his identity would be apt to lie and give a false name, and the statute offers no means of verifying his statement as to his identity. In fact, the Court leaves open the question of whether requiring documented proof of identity would be constitutional, stating that "the statute does not require a suspect to give the officer a driver's license or any other document. Provided that the suspect either states his name or communicates it to the officer by other means . . . the statute is satisfied and no violation occurs."[66] Accordingly, this decision leaves open for argument that implicit in the Court's holding is that requiring proof of identification under such circumstances would be unconstitutional.[67] Therefore, if proof of identification is not permissible, the use of biometrics to identify an individual or verify an individual's identity would be equally unlawful, as would any proof of identity required from the individual.

It is important to keep in mind that the Court's analysis is in the context of a criminal investigation that could result in the loss of liberty (i.e., imprisonment). The process of identification in other contexts such as border control (via passports or other means of identification) is not in question in *Hiibel*. Additionally, the use of biometrics is not brought into question by this decision. The use of biometrics (i.e. with a passport) should not add a second layer of analysis or basis for questioning the constitutionality of the identification of the individual. Moreover, Hiibel was merely standing on the street. If he were exercising a privilege under government control, such as driving an automobile, the issue of the requirement of providing or the right to demand identification would never have arisen. Accordingly, if an individual is exercising a privilege, such as entering the United States, identification should not be an issue. In this manner, the individual has presented himself to a government official knowing that he shall be asked to identify himself. Hiibel was simply on a public road and was approached by a police officer. Hiibel did not voluntarily offer himself for purposes of identification.

The outcome of *Hiibel* could have far-reaching consequences, including setting the stage for the constitutionality of a national ID card. While it is unlikely that the decision will once and for all settle the issue of whether a national identification card is constitutional, whatever the outcome, the case will certainly be significant.

---

[66] *Id*. at 6.

[67] It is also interesting that in the video of Hiibel's arrest, the officer specifically asks Hiibel for "identification," which, presumably, is beyond the scope of what the statute permits. None of the justices commented on this; the justices focused solely on the legality of the statute and not on the actions of the officers.

b. Physical Privacy: Privacy in One's Personal Space

Physical privacy has been addressed by the Supreme Court primarily in the context of the Fourth Amendment's search and seizure protections in criminal law. The Supreme Court and the lower courts have decided many cases involving individuals being compelled to provide fingerprints, blood or DNA samples, and other physiological information.

Katz v. United States

The seminal Fourth Amendment search and seizure case is *Katz v. United States*,[68] in which a two-prong test emerged to determine whether a search is constitutional: (1) does the individual have a reasonable expectation of privacy and (2) is that expectation objectively reasonable. The case centered around the FBI's use of an electronic listening and recording device on a public telephone to gather evidence against the petitioner. The Court held that the government's eavesdropping activities violated the petitioner's justifiable expectation of privacy while using the telephone booth and thus constituted a "search and seizure" within the meaning of the Fourth Amendment. This case essentially put an end to 40 years of cases that held that privacy only existed while you were in your home, allowing the right to privacy for the first time to extend beyond the boundaries of one's own home. However, the *Katz* Court purposely declined to review the issue of whether "physical penetration of a constitutionally protected area is necessary before a search and seizure can be said to be violative of the Fourth Amendment."[69] The Court stated that the Fourth Amendment does not create a "general constitutional 'right to privacy,'" but rather offers specific protections against "certain kinds of governmental intrusion" as other Amendments protect against other kinds of government intrusions.[70] The Court further stated that the general right of privacy, which the Court (quoting the famous Warren & Brandeis article) described as the "right to be let alone by other people" is, in the Court's opinion, a right "left largely to the … States."[71] The result of this important decision is that what is open to public view is not considered subject to a reasonable expectation of privacy. This is known as the "public view doctrine" and was examined in subsequent Supreme Court cases, including *California v. Ciraolo*, discussed below.[72]

Justice Harlan, in his concurring opinion, warned, perhaps prophetically, that "reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[73]

In an interesting footnote to the *Katz* decision, the Court stated:

---

[68] 389 U.S. 347 (1967).
[69] *Id*. at 350.
[70] *Id*.
[71] *Id*. at 350-1.
[72] 476 U.S. 207 (1986); *See also Smith v. Maryland*, 442 U.S. 735 (1979) where the Court held that an individual did not have a reasonable expectation of privacy in the phone numbers he dialed.
[73] 389 U.S. at 362.

> Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.[74]

In his concurring opinion, noting that the Court acknowledged that there are situations that call for a warrantless search, Justice White essentially declared that the President should have carte blanche authority with respect to electronic surveillance when it comes to national security, stating:

> We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.[75]

In a separate concurring opinion, the more liberal Justices Douglas and Brennan disagreed with Justice White's view, pointing out that the President and the Attorney General do not have the required detached neutrality of a magistrate, and stating:

> There is, so far as I understand constitutional history, no distinction under the Fourth Amendment between types of crimes.[76]

California v. Ciraolo

In *California v. Ciraolo*, the Court held that an individual does not have a reasonable expectation of privacy in whatever can be viewed from high above his fenced-in backyard. In this case, the police received an anonymous tip that marijuana was being grown in someone's backyard. Unable to observe the backyard due to a six-foot outer fence and ten-foot inner fence encasing the yard, the police hired a private plane and flew over the backyard to take photographs of the marijuana.[77]

The lower court found that the use of the high fences manifested a reasonable expectation of privacy in what the court determined was part of the "cartilage" of the home.[78] The lower court focused particularly on the fact that the surveillance "was undertaken for the specific purpose of observing this particular enclosure within [the] curtilage."[79]

The Supreme Court, reversing the lower court's decision, looked to the fact that the observations took place in public airspace and were observable with the naked eye.

---

[74] *Id*. at 358.
[75] *Id*. at 364. National Security is discussed *infra* at Section III.
[76] *Id*. at 360.
[77] 476 U.S. at 209.
[78] *Id*. at 212. The curtilage doctrine stands for the proposition that the sanctity of a person's home extends to all areas that are intimately linked to the home, both physically and psychologically. *Id*. at 213.
[79] *Id*. at 210, citing the lower court's opinion, 161 Cal.App.3d. 1081, 1089 (1984).

The Court concluded that the individual's expectation of privacy was not reasonable.[80] The Court further stated that an airplane was not "within the category of future 'electronic' developments that could stealthily intrude upon an individual's privacy" that Justice Harlan warned about in *Katz*.[81]

Kyllo v. United States

Another important Supreme Court case that examined the extent of a person's right to physical privacy is the 2001 case of *Kyllo v. United States* in which the Court held that a thermal scan of a person's home is an unreasonable search.[82] First, the Court noted that "the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares,"[83] and that "visual observation" does not even amount to a search at all.[84] Nevertheless, the Court felt that obtaining information about the interior of one's house using "sense-enhancing technology" that is "not in general public use" constituted a search of a "constitutionally protected area."[85]

It is possible that a court, if faced with the issue of whether non-consensual facial scanning is unconstitutional, might invoke this reasoning and extend it to find that facial scanning amounts to no more than visual observation of what is held out to the public. On the other hand, one might argue that there is a difference between being seen and being recognized, and that an ordinary person has a reasonable expectation of not being recognized by the government when he merely walks in a public place. The outcome may depend on the circumstances and the location. For example, a person walking through Times Square in New York City may have a greater and more reasonable expectation of anonymity than a resident walking through his rural town with a population of a few hundred people. However, perhaps if the person in Times Square were watching the ball drop on New Year's Eve, any right he may have to anonymity might be outweighed by the public's interest in security.

Even more challenging from a constitutional analysis standpoint is "identification enhancing" technology, such as an iris scanning device. Such technology allows what would ordinarily be a relatively indistinguishable iris to be used to positively identify a person by converting the unique patters of the iris into an algorithm. Although iris-scanning devices cannot presently be used without the consent and cooperation of the subject, it is conceivable that advances in the technology could achieve such capability.

Arguably, an iris-scanning device could be analogized to a thermal scanning device. The *Kyllo* Court found that use of a thermal scanning device that allowed the government (e.g. law enforcement) to view contents of the home that would normally not

[80] *Id*. at 214.
[81] *Id*. at 215.
[82] 533 U.S. 27 (2001).
[83] *Id*. at 32, citing *California v. Ciraolo*, 476 U.S. at 213.
[84] *Id*.
[85] *Id*. at 34.

be discernible without such "sense-enhancing technology" is a search subject to Fourth Amendment protection. A court might likewise find that use of an iris scanning device that allows the government to view the iris in a way the human eye and brain are not capable of is a search subject to Fourth Amendment protection.

However, the *Kyllo* decision concerned a person's home, which the Court considered to be a place where a person could "retreat" and "be free from unreasonable government intrusion,"[86] and where "privacy expectations are most heightened."[87] Use of an iris-scanning device or other biometric identifier in a public place would likely not be subject to the same level of scrutiny. Or would the "place" of invasion be the body, rather than the physical public place? If so, would it thus be necessary to extend this privacy consideration to a person's body? Presumably, privacy expectations in one's body are even more heightened than in one's home. The issue of privacy in one's body will be addressed in the next section.

It is noteworthy that the Court in *Kyllo* stated: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[88] The Court cited the *Ciraolo* case as an example of how technology can alter what is a reasonable expectation of privacy.[89] There was a time when a person had a reasonable expectation of privacy in his own backyard if he built a high enough fence around his property. That expectation of privacy has been eroded by the advent of airplanes.

It is interesting that the Court was comfortable with the notion of an airplane being used to view the contents of someone's backyard, but not with a thermal scanning device being used to view the contents of one's home. Is the difference between the two the fact that society has accepted airplanes, which were not invented to spy on people, even though they have that capacity? Maybe the difference is that airplanes flying above private property are commonplace, whereas thermal scanning devices are not a part of every day life. Perhaps if there were no passenger airplanes and if the government were using flying machines solely to survey people's backyards, the Court's decision in *Ciraolo* would have been different.

Is a facial scanning device, such as the one used at the 2001 Super Bowl, within Justice Harlan's category of "electronic developments that could stealthily intrude upon an individual's privacy"? Or would the fact that it was used in a public place, rather than in one's home or backyard, help tip the scales in favor of its use? No arrests were made as a result of the use of such technology at the 2001 Super Bowl. Accordingly, one can merely speculate how the Supreme Court might rule on that issue. At the very least, these cases demonstrate how what is a reasonable expectation of privacy today may change as society accepts new technologies.

---

[86] *Id*. at 31.
[87] 533 U.S. at 33.
[88] *Id*. at 33-34.
[89] *Id*. at 34.

Posed another way, the question may be whether law enforcement is limited in the extent to which technology can be used to enhance human capability. An officer with excellent eye sight, a sharp memory, and who has been working a particular beat for many years may be better able to recognize and positively identify people than another less experienced and less skillful officer. Would it be unconstitutional for the newer officer with only average eyesight and poor memory skills to use technology to upgrade him to the level of the seasoned officer? How far can that technology be taken to enhance the officer's ability to recognize and identify people on his beat? At what point do such enhanced capabilities cross the threshold? The Court's rulings, while seeking to draw some guidelines, have been largely fact-sensitive. The factual sensitivity of the rulings demonstrates the difficulty in drawing bright lines to divide what is a reasonable expectation of privacy from what is a justifiable means of law enforcement.

The cases in this section looked at the Fourth Amendment's protections with respect to one's physical space, such as a home or backyard. The cases in the next section examine the protections under the Fourth Amendment afforded to an individual's body.

c. Physical Privacy: Privacy in One's Body

The Fourth Amendment provides for "the right of the people to be secure in their *persons*" (*emphasis added*). The extent to which a person's body is protected from government intrusion has been the subject of extensive and ongoing analysis by the Supreme Court. Although the subjects in each case range from convicts to suspects to railroad employees to schoolchildren, the common denominator is the Court's use of a balancing test to weigh the individual's privacy interest against the government's (i.e. society's) interest.

Collection With Suspicion

The Supreme Court's seminal case that analyzed an intrusion into the body for Fourth Amendment purposes was *Schmerber v. California*.[90] The case involved the drawing of blood from a criminal suspect without his consent to collect evidence of intoxication. In *Schmerber*, the defendant was suspected of drunk driving and was arrested while being treated for his injuries at a hospital.[91] While admitted, and over his objections, the police had a physician draw a blood sample, which was subsequently used against him.[92] In deciding whether this action implicated the Fourth Amendment, the Supreme Court first determined that the compulsory administration of a blood test invokes the Fourth Amendment because it clearly constitutes a search of a person.[93] Therefore, the Court needed to determine whether the intrusion was justified under the circumstances.[94]

The *Schmerber* Court formulated a balancing test to use in determining whether intrusions into the body would stand up under Fourth Amendment scrutiny. The Court reasoned that because the expectation of privacy in one's body is so personal, the Court would require a determination that the intrusion was justified based on the specific facts.[95] The Court stated: "the questions we must decide in this case are whether the police were justified in requiring petitioner to submit to the blood test, and whether the means and procedures employed in taking his blood respected relevant Fourth Amendment standards of reasonableness."[96] If the intrusion is justified and meets the standard of reasonableness, then, under the balancing test, it will pass muster under the Fourth Amendment.

---

[90] 384 U.S. 757 (1966).
[91] *Id*. at 758.
[92] *Id*.
[93] *Id*. at 767.
[94] *Id*. at 768.
[95] 384 U.S. at 768.
[96] *Id*.

In determining what would be justifiable, the Court looked to the law generally, which recognizes the idea that once a person is legally arrested, the police may search that person, based upon a need for safety or the collection of evidence. [97] However, the Court believed that such considerations were not implicated in this case because the search was an intrusion "beyond the body's surface."[98] The Court further stated that there is "an interest in human dignity and privacy which the Fourth Amendment protects" and that such fundamental interests require clear justification.[99] To meet the Fourth Amendment requirements, absent emergency circumstances, a search warrant would be required.[100] The Court felt that in this case, the officer had probable cause, it was an emergency situation, and the act was reasonable.[101] In determining whether the act itself was reasonable the Court looked at the blood test, saw that is was a highly effective measure to determine one's alcohol level, acknowledged that these types of tests are very common, that the amount of blood necessary to extract is minimal, and that "for most people the procedure involves virtually no risk, trauma, or pain."[102] The Court also held that the evidence produced from the blood was admissible at trial and did not violate the Fifth Amendment's privilege against self-incrimination. The Court specifically stated that its holding was reached on the facts of the case, and that the "integrity of an individual's person is a cherished value of our society" and that its holding in "no way permits more substantial intrusions, or intrusions under other conditions."[103]

It is important to note that in analyzing the reasonableness of the intrusion, the Court looked to not only the nature of the blood tests, but also to society's familiarity and acceptance of the procedure, noting that blood tests have "become routine in our everyday life."[104] It leaves open the inquiry that, similar to the technology inquiry of *Kyllo*, the Court might have subjected intrusions that are not so commonplace (e.g. a facial scan) to a much stricter review. Just as noteworthy is that fact that the Court considered the extent of the physical risk involved. The standard procedures used to capture one's biometric information involve "virtually no risk, trauma, or pain" and, arguably at least, less intrusion upon a person's dignity than drawing blood.

The Supreme Court continued this line of reasoning in *Winston v. Lee*,[105] holding that the surgical intrusion into a criminal suspect to remove a bullet was unreasonable under the Fourth Amendment because there was no compelling need. The case arose because the State wanted to compel a criminal suspect to undergo surgery to remove a bullet from his chest to prove his guilt or innocence in a robbery.[106] The Supreme Court reasoned that extracting a bullet from a suspect is the "'more substantial intrusion'

[97] *Id*. at 769.
[98] *Id*.
[99] *Id*. at 769-770.
[100] 384 U.S at 770.
[101] *Id*. at 770-771.
[102] *Id*. at 771.
[103] *Id*. at 772.
[104] *Id*. at 771 n.13.
[105] 470 U.S. 753 (1985).
[106] *Id*. at 755.

cautioned against in *Schmerber* ... and to permit the procedure would violate [the suspect's] right to be secure in his person guaranteed by the Fourth Amendment."[107]

The Court analyzed the privacy implications that the act would invoke, namely that "a compelled surgical intrusion into an individual's body for evidence … implicates expectations of privacy and security of such magnitude that the intrusion may be 'unreasonable' even if likely to produce evidence."[108] The Court stated that a person's being embodies the "most personal and deep-rooted expectations of privacy."[109]

The Court looked to *Schmerber* for its line of reasoning and invoked the same balancing test, weighing society's interests against the privacy interests of the individual. The Court reasoned that "the ordinary [probable cause and search warrant] requirements of the Fourth Amendment would be the threshold requirements" and that the analysis would focus on the extent of how reasonable or what the magnitude of the intrusion would be.[110] The Court stated that "a crucial factor in analyzing the magnitude of the intrusion in *Schmerber* is the extent to which the procedure may threaten the safety or health of the individual. ... [F]or most people [a blood test] involves virtually no risk, trauma, or pain."[111] The Court noted that another significant factor is the extent of "the intrusion upon the individual's dignitary interests in personal privacy and bodily integrity."[112]

In a case that involved a much greater intrusion on dignity, the Court had to decide, among other constitutional issues involving pre-trial detainees, whether visual body cavity searches violated the Fourth Amendment. In *Bell v. Wolfish*,[113] detainees were required to strip and expose their body cavities so they could be visually inspected to check for smuggled contraband.[114] The Court again applied the *Schmerber* balancing test to determine if these inspections were reasonable under the Fourth Amendment, stating that "each case requires a balancing of the need of the particular search against the invasion of personal rights that search entails."[115] While the Court noted that they did not "underestimate the degree to which [the] searches…invade[d] the personal privacy of inmates," the Court reasoned that a detention facility is a unique place and that this type of intrusion is not unreasonable.[116]

Another important Fourth Amendment case is the case of *Terry v. Ohio*[117] in which Chief Justice Warren decided the fundamentals of what has become known as the "stop and frisk." This case is important to understand because its implications could shed

---

[107] *Id.*
[108] *Id.* at 759.
[109] *Id.* at 760.
[110] 470 U.S. at 760.
[111] *Id.* at 761.
[112] *Id.* at 762.
[113] 441 U.S. 520 (1979).
[114] *Id.* at 558.
[115] *Id.* at 559.
[116] *Id.* at 560.
[117] 392 U.S. 1 (1968).

some light on how the Supreme Court might view a mandatory submission to biometric identification.

The *Terry* Court was faced with balancing the distinctions between the safety of the public and the police against the rights under the Fourth Amendment to control one's own person and be "free from all restraint or interference of others,"[118] including the right to walk down the street.[119] The government was urging for a distinction to be made between a "stop" and an "arrest" (in other words, a "seizure" of a person), and between a "frisk" and a "search," rationalizing that police should be allowed to briefly detain someone for questioning and, if suspicion arises, frisk that person for weapons.[120] The Court first had to determine if the Fourth Amendment was applicable. They found that "it must be recognized that whenever a police officer accosts an individual and restrains his freedom to walk away, he has 'seized' that person."[121] The Court found the same to be true for a pat down, stating:

> It is simply fantastic to urge that such a procedure performed in public by a policeman while the citizen stands helpless, perhaps facing a wall with his hands raised, is a 'petty indignity.' It is a serious intrusion upon the sanctity of the person, which may inflict great indignity and arouse strong resentment and it is not to be undertaken lightly.[122]

To determine the extent of the intrusion upon the person, the Court engaged in its balancing test, weighing the government's interest (the need to stop and frisk) against the individual's privacy interest and the invasion that the stop and frisk entails.[123] The Court ultimately found that there must be "articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[124]

As a result of *Terry v. Ohio*, police officers are now permitted to stop an individual for questioning if the officer finds the person's behavior suspiciously indicative of a crime, and may conduct a limited pat down for weapons if the officer has reason to believe the person may be armed and dangerous.[125]

According to the line of reasoning of the foregoing cases involving collection with suspicion, stopping a person and requiring him to submit to a biometric identification test based on reasonable suspicion may be found to be reasonable. By way

---

[118] *Id*. at 9 (quoting *Union Pac. R. Co. v. Botsford*, 141 U.S. 250, 251 (1891)).
[119] *Id*. at 9 (citing *Beck v. State of Ohio*, 379 U.S. 89 (1964)).
[120] *Id.* at 10.
[121] *Id*. at 16.
[122] 392 U.S. at 16-17.
[123] *Id*. at 21.
[124] *Id.*
[125] *Id*. at 27. The Supreme Court continued this line of cases with *California v. Hodari*, 499 U.S. 621 (1991), where the Court further articulated the extent of what constituted the seizure of a person. In *Hodari*, the Court was required to determine what constitutes a seizure (as opposed to a mere stop). The Court found that to be seized requires more than a showing of force; it requires that there be a submission to the assertion of authority or the yielding to this authority, or to the physical force of the officers.

of illustration, imagine a situation where the police in Los Angeles were looking for an individual believed to have committed a crime, and such person had left fingerprints at the crime scene. Then suppose that all the police officers in Los Angeles carried a hand held device that had the capability of capturing a fingerprint image by a person merely touching the device with his hand and determining whether there is a match with the fingerprints found at the crime scene. If a stop and questioning would be justified, then perhaps requiring a person to place his finger on such a device would also be reasonable if the officer had reason to believe such person might be the person they are looking for (e.g. because he matched the physical description).

Collection Without Suspicion: If Special Need Exists

In *Skinner v. Railway Labor Executives' Assn.*,[126] the Court held that while the Fourth Amendment applied to drug and alcohol testing, under the circumstances such testing was reasonable without a need for a warrant or reasonable suspicion due to a compelling government interest. *Skinner* arose from a federal safety statute, which was used by the Federal Railroad Administration to promulgate rules mandating blood and urine tests for railroad employees involved in certain train accidents to test for alcohol and drug use, and authorized breath and urine tests for employees who violated certain rules.[127]

The Court began its analysis by determining the extent of the government's participation in the activity, finding that it was sufficient to implicate the Fourth Amendment.[128] The Court again applied the balancing test and found that this type of circumstance qualified as a special need justifying a departure from the normally required warrant and probable cause requirements.[129] The Court stated that the warrant would add little certainty and would instead hinder the government's objective.[130] The Court further reasoned that "in limited circumstances, where the privacy interests implicated by the search are minimal, and where an important government interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such [reasonable] suspicion."[131] It is noteworthy that the Court based its decision at least in part on the fact that the employees had a diminished expectation of privacy working in a highly regulated industry.[132]

In *Vernonia School Dist., 47J v. Acton*,[133] the Court held a public school district did not violate a student's constitutional right to be free from unreasonable searches by requiring athletes to submit to random urine tests. The Court started its analysis with the Fourth Amendment, stating, "state-compelled collection and testing of urine …

[126] 489 U.S. 602 (1989).
[127] *Id*. at 606.
[128] *Id*. at 614-616.
[129] *Id*. at 620.
[130] 489 U.S. at 624.
[131] *Id*. at 624.
[132] *Id.* at 627-628.
[133] 515 U.S. 646 (1995).

constitutes a 'search.'"[134] The Court analyzed the requirements of the Fourth Amendment and noted that some searches do not need to be based on probable cause and do not require a warrant. The Court stated that "a search unsupported by probable cause can be constitutional … when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable."[135]

The Court felt that maintaining "swift and informal disciplinary procedures" in a public school constituted a special need.[136] The Court discussed how a school and the children who attend it are in a special situation since they have special goals, rights, and responsibilities. The Court pointed out that all 50 states require public school students to receive certain vaccinations and many impose other requirements that are meant to protect both the individual child and all the children in the school. The Court noted that the Fourth Amendment is "different in public schools than elsewhere; the 'reasonableness' inquiry cannot disregard the schools' custodial and tutelary responsibility."[137] The Court further reasoned that the student athletes have an even lesser expectation of privacy; by joining a school's athletic team, they voluntarily subject themselves to a higher level of scrutiny and regulation, including physical exams.[138]

The Court then applied its balancing test, finding that the character of the intrusion and the privacy interests compromised were not significant, even negligible,[139] and that the school's interest in deterring drug use was both important and compelling.[140] Based on all the factors, the Court found the random urine test policy was "reasonable and hence constitutional."[141]

The line of reasoning used in *Skinner* and *Vernonia* might be extended to the mandatory use of biometric recognition technology at airports, where the government has an interest in passenger safety and there is a lesser expectation of privacy. After all, passengers are already faced with having their purses and bags rummaged through, having their shoes inspected, and having their bodies scanned for metal objects. In a different context (i.e. if no special need existed), such acts would be seen as highly invasive of people's privacy. But in airports across the country, these procedures are tolerated by thousands of Americans every day, presumably because they understand the very real threat inherent in air travel. Using biometric recognition technology as part of airport security is merely an extra layer of protection in ensuring air travel safety.

Perhaps, then, even outside of air travel, in the face of a special need, such as strong evidence that a terrorist is hiding out in a particular home building a weapon or that a man is beating his wife in the privacy of their home, using a thermal scanning

---

[134] *Id*. at 652 (citing its holding in *Skinner v. Railway Labor Executives' Assn*., 489 U.S. 602, 617 (1989)).
[135] *Id*. at 653 (citing *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987)).
[136] *Id*.
[137] *Id*. at 656.
[138] 515 U.S. at 657.
[139] *Id*. at 658-660.
[140] *Id*. at 661.
[141] *Id*. at 665.

device to ascertain the truthfulness of such evidence and potentially prevent harm to others would be justifiable.

DNA Databanks

In the *United States v. Kincade*,[142] the Ninth Circuit Court of Appeals addressed the issue of whether forcing a parolee to give a blood sample for inclusion in a DNA databank violates the Fourth Amendment. Generally, the Fourth Amendment requires a warrant based on probable cause unless the search or seizure satisfies a "special need." The court concluded that the government's desire to create a comprehensive databank was "normal law enforcement," which the court found is not a special need, and does not outweigh the parolee's reasonable expectation of privacy. The court felt that the government's desire for a databank did not justify departure from the usual warrant and probable cause requirements or the lesser standard of reasonable suspicion that Kincade was involved in a crime. That is, Kincade had to be suspected of another crime in which his DNA was needed to ascertain guilt.

On January 5, 2004, by a majority vote, the Court of Appeals decided that *Kincade* would be reheard by the en banc court, and that the prior opinion not be cited as precedent by any court in the Ninth Circuit except to the extent adopted by the Ninth Circuit Court of Appeals.[143] This decision is significant because rehearings en banc usually only involve cases of extraordinary public importance. The Ninth Circuit Court of Appeals held the en banc hearing on March 23, 2004.

The Ninth Circuit Court of Appeals' holding in *Kincade* (which, as noted above, is now under reconsideration) can be summed up as follows: (1) a DNA databank is not a special need and (2) the parolee's reasonable expectation of privacy is outweighed by the government interest.

Other courts have disagreed with the Ninth Circuit Court of Appeals' determination. The Seventh Circuit upheld a Wisconsin DNA collection statute because its purpose, which was to obtain reliable proof of a felon's identity (not to search for evidence of wrong doing), was, in the court's opinion, a special need.[144] The Tenth Circuit upheld a federal statute requiring DNA samples from convicted sex offenders because the seizure met the special needs exception.[145] The Ohio Court of Appeals upheld an Ohio statute requiring convicted felons to give a DNA sample for inclusion in a DNA database because it met a special need of law enforcement.[146] In evaluating whether the special need outweighed the privacy interest of the defendant, the Ohio court noted that prisoners and probationers have diminished expectations of privacy, and that

[142] 345 F.3d 1095 (9th Cir. 2003).
[143] 354 F.3d 1000.
[144] *Green v. Berge*, 2004 U.S. App. LEXIS 236 (U.S. App., 2004).
[145] *United States v. Plotts*, 347 F.3d 873, 877 (10th Cir. 2003).
[146] *State v. Steele*, 802 N.E.2d 1127, 155 Ohio App. 3d 659, 672 (Ohio App., 2003).

the blood sample was a minimal intrusion into the privacy interest.[147] The indication is that the special need of a DNA databank would not outweigh the privacy interests of a person who is not under arrest or a criminal suspect.

Similarly, the Fourth, Fifth, and Eleventh Circuits have also upheld DNA sample statutes. The Fourth Circuit allowed a DNA sample to be collected from a suspect who had been arrested on probable cause because the court reasoned that convicted felons, probationers, and arrested persons lose some, if not all, of their privacy interests.[148] The same court also upheld a federal statute requiring probationers to submit to a DNA test.[149] In reviewing the same federal statute, the Fifth Circuit also upheld the statute because the court found that correct identification is a special need and inmates do not have a reasonable expectation of privacy.[150] A federal court in Georgia upheld a Georgia law requiring all convicted felons to submit a DNA sample because the State's compelling interest in obtaining reliable and accurate identifying characteristics of individuals convicted of felonies outweighed the convicted felon's reduced privacy interest.[151]

Although the decisions discussed above addressing the mandated drawing of blood have limited applicability because they involve criminal suspects, convicts, and parolees, they are nevertheless important. With the exception of the *Kincade* decision, which is being reheard and could ultimately be reversed, all of the courts found proof of identification and correct identification (and in the Supreme Court case of *Schmerber*, collection of evidence) to outweigh the requirement of a warrant and probable cause. Drawing blood is far more invasive than any method of obtaining biometric information and certainly more likely to cause "risk, harm, or pain." Thus, it is likely that any other method of collecting biometric information from convicts, parolees, and possibly even people who have been arrested or are mere suspects will be sanctioned. It is also conceivable that such less invasive methods of obtaining biometric information might be justified in other situations (i.e. in a non-criminal context) without the consent of the individual if the government's interest is found to reach the level of a "special need," such as part of airport security screening for public safety reasons.

[147] *Id.*
[148] *Jones v. Murray*, 962 F.2d 302, 306 (4th Cir. 1992).
[149] *United States v. Stegman*, 295 F. Supp. 2d 542, 550 (U.S. Dist., 2003).
[150] *Groceman v. United States Department of Justice*, 354 F.3d 411 (2004).
[151] *In re D.L.C.*, 2003 Tex. App. LEXIS 10619 (Tex. App., 2003).

Section Highlights: *Summary of Case Law and Application to Biometrics*

The common denominator in all of the privacy cases discussed in this section is the balancing test that the courts use to weigh the individual's privacy interest against a particular public (i.e. government) interest. The factors the courts consider in the public's favor are the importance of the public interest and the precautions taken to safeguard the information. On the individual's side, the courts look to whether there is a reasonable expectation of privacy and the level of the intrusion on the person. *See chart of Factors Used in the Balancing Test on the next page.*

This balancing test would almost certainly be applied to the use of biometric identification by the government for national security purposes. Although the nation's concern about national security, particularly in air travel, have been tipping the scales in favor of biometric technology since September 11th, there is still an intense concern about privacy and civil liberties and a perception that biometrics is somehow privacy invasive. Accordingly, in applying biometric recognition technology for national security, even if the technology will only be used for verification purposes without a databank, the government should be prepared to demonstrate that national security (e.g. protection of lives, or even property, such as buildings, bridges, railways, parks, and monuments) is a "special need" and that the interest of national security is furthered by the use of biometric identification. The government should endeavor to utilize the least intrusive, least offensive method possible without compromising the security goals. It should also implement measures to safeguard any information collected to protect against unauthorized uses and disclosures.

Factors Used in the Balancing Test:

Public Interest **Vs.** **Individual Privacy Interest**

Public Interest:
Courts look to whether the public interest is important enough to justify the action.

(1) What is the purpose of the action? E.g. criminal investigation, crime prevention, health and safety, national security.
(2) Is the public interest furthered by the action?
(3) Does the situation rise to the level of a special need permitting the action without a warrant based on probable cause?

Reasonable Expectation of Privacy:
Courts look to society's views on what is reasonable.

(1) Where is the intrusion? There is a diminished expectation of privacy in certain places and situations, such as prisons, schools, and airports.
(2) What is the level of intrusion? E.g. what is the extent of the risk, trauma, pain, an indignity of the intrusion?
(3) What technology (e.g. sensory-enhancing) is being used? How commonplace is the technology? (e.g. metal detectors)

Safeguard Measures:
What are the measures used to safeguard the information?

The more sensitive the information, the stronger the safeguards need to be. Strong safeguards can tip the scale in favor of the public interest even if the information is highly sensitive

Sensitivity of Information:
How sensitive is the information?

Courts have found certain information to be more sensitive, such as health information, while other information, such as Social Security numbers, less so.

B. STATUTORY PRIVACY LAW (PUBLIC SECTOR)

The previous section examined privacy as a constitutional right and the judicial decisions analyzing the scope of such right. This section examines statutory privacy laws governing the public sector and cases interpreting such laws. There are numerous statutes that impact the government's ability to collect information on people, including many on wiretapping and surveillance. However, the one that will likely be the most significant to NBSP, its subcontractors, and biometrics is the Privacy Act of 1974. It is impossible to adequately discuss the Privacy Act of 1974 without also addressing the Freedom of Information Act. Accordingly, the two statutes are discussed together in this section of the report. Also included is a brief discussion of the Computer Matching and Privacy Act of 1988, which amended the Privacy Act of 1974. Finally, although not a statute, Executive Order 12333 is discussed as part of this section as it directly impacts the government's ability to collect, maintain, use, and disseminate personal data. Other public sector federal privacy statutes are not discussed in this report because they have little, if any, foreseeable impact on biometrics. Federal privacy statutes impacting the private sector are discussed in Section IV of this report.

1. The Privacy Act of 1974 and the Freedom of Information Act

The Privacy Act of 1974[152] (the "Privacy Act" or the "Act") is the first and most comprehensive statutory law enacted to address privacy concerns in the United States. Nevertheless, and despite its name, it is extremely limited in scope. The Privacy Act regulates the collection, maintenance, use, and dissemination of personal information of United States citizens and legal resident aliens by the federal government (it does not apply to state and local governments and it does not apply to private individuals or private entities). The Act requires all federal agencies to adopt and publish minimum standards with respect to the collection, maintenance, use, and dissemination of personal information, and it restricts such agencies from disclosing personally identifiable records. There are several exceptions to the nondisclosure rules. One of the exceptions requires disclosures mandated under the Freedom of Information Act ("FOIA").[153] Importantly, the Act only applies to "records" maintained within a "system of records." Accordingly, what constitutes a "record" and what constitutes a "system of records" is critical to understanding whether a person's biometric information would be subject to the Privacy Act.

---

[152] 5 U.S.C. §552a et seq.

[153] 5 U.S.C. §552 et seq. It should be noted that pursuant to the revisions made to Circular A-110, (the publication that sets the rules and procedures governing federal grants to nonprofit institutions, hospitals, and universities) following the Omnibus Consolidated and Emergency Supplemental Appropriations Act for Fiscal Year 1999, all research data generated through federal grants is now subject to FOIA. Circular A-110 currently requires agencies to respond to FOIA requests for certain grantee research findings by obtaining the requested data from the grantee and processing it for release to the requester. This is important because NBSP and its subcontractors, although not federal agencies, do receive federal funding. Whether data derived from a research study conducted by any of these organizations would be subject to FOIA would depend on a case-by-case analysis. However, it is important to note that this potential for required disclosure exists. *Office of Mgmt. & Budget, Circular A-110*, ''Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations', 64 Fed. Reg. 54,926 (Oct. 8, 1999).

a. What is a "Record"?

The Privacy Act defines "record" as:

> " …any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or photograph;"

The use of the terms "finger or voice print or photograph" leaves little doubt that biometrics presumably fall within the parameters of the Privacy Act. However, to what extent biometrics are records is not entirely clear. Under a narrow interpretation of the definition, a biometric must be linked to something else about that person, such as his "education, financial transactions, medical history, and criminal or employment history" to be considered a record. Under a broader interpretation of the definition, as long as that biometric is linked to *anything* about that person, including his name or Social Security number or anything else that can be traced back to that person, it is a record. Under the broadest reading of the definition, a biometric in and of itself is a record even if it is not linked to any other information about the individual.

Interpretations of the Term "Record"

Narrow	Broad	Very Broad
Biometric must be linked to information "about" the person, such as medical history	Biometric can be linked to any other piece of information, such as name or SSN	Biometric need not be linked to anything else because it is a record in and of itself

There is vast disagreement among the courts as to how broadly to interpret the Privacy Act's definition of "record." The United States Supreme Court has only minimally addressed this issue. Such differing interpretations are critical to how broadly biometrics will be construed as a record. For example, is a biometric that is linked to a person's name and/or Social Security number a record? Or is more (or less) required, such as information about the person's education, financial transactions, medical history, and criminal or employment history? Or perhaps a biometric itself is a record. A study of the differing opinions of the term "record" is important in analyzing how biometrics might be viewed in relation to the Privacy Act.

The Office of Management and Budget ("OMB") Guidelines instruct that a record can be "any item of information about an individual that includes an individual identifier" and "can include as little as one descriptive item about an individual."[154]

Supreme Court Examination of "Record"

In the 1994 case *U.S. Dept. of Defense v. Federal Labor Relations Authority*,[155] the Supreme Court applied a broad view of the term "record" in holding that home addresses qualified for protection under the Privacy Act. The Supreme Court ultimately held that the disclosure of the home addresses was a "clearly unwarranted invasion of the employees' personal privacy within the meaning of the Freedom of Information Act."[156] However, the Court did not provide an analysis of the term, but rather, assumed that the home addresses were records. Nevertheless, the case is worth studying because it required an in-depth examination of both the Privacy Act and of FOIA and is the only time the Supreme Court dealt with the term "record" under the Privacy Act.

The case arose out of two local labor unions requesting certain federal agencies (the petitioner in this case) to provide them with the names and home addresses of the agency employees in the bargaining units represented by the unions.[157] The agencies, while agreeing to provide the names along with workstations, refused to release home addresses.[158] When the unions were denied this information, they filed unfair labor practice charges with the Federal Labor Relations Authority ("FLRA") (the respondent in this case) contending that disclosure of this information was required under the Federal Service Labor-Management Relations Statute (the "Labor Statute").[159]

The Labor Statute "provides that agencies must, 'to the extent not prohibited by law,' furnish unions with data that are necessary for collective-bargaining purposes."[160] The agencies argued that the Privacy Act prohibited this type of disclosure.[161] The FLRA rejected this argument and ordered disclosure of the home addresses.[162]

The United States Court of Appeals for the Fifth Circuit sided with the FLRA, holding that disclosure of the addresses fell within the FOIA exception to the Privacy Act, which requires disclosure unless disclosure "would constitute a clearly unwarranted invasion of privacy."[163] To determine if this exception to a FOIA disclosure applied, the Court of Appeals used a balancing test, weighing "the public interest in effective

[154] OMB Guidelines, 52 Fed. Reg. 12990 (1987).
[155] 510 U.S. 487 (1994).
[156] *Id*. at 489.
[157] *Id*. at 490.
[158] *Id*.
[159] *Id*.
[160] 510 U.S. at 490.
[161] *Id*.
[162] *Id*.
[163] *Id*. at 491.

collective bargaining" against "the interest of employees in keeping their home addresses private."[164]

The Supreme Court, in reversing the Fifth Circuit's decision, began its analysis with the Labor Statute in order to understand the nature of the "public interest" at hand.[165] The Court stated that the Labor Statute requires the union representative and the agency to negotiate in good faith by mandating that the agency give the representative all necessary data "to the extent not prohibited by law" so that they can arrive at a collective bargaining agreement.[166]

The Court next turned to the Privacy Act, which states that "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record would be … required under [FOIA]."[167] The Court stated that the addresses are "records" covered by the broad terms of the Privacy Act, and unless FOIA would require their release, "their disclosure is prohibited by law."[168]

After determining that the addresses were subject to the Privacy Act, the Court then looked to whether the FOIA exception would apply to determine whether it would require the release of the information.[169] The Court stated that the purpose of FOIA is to allow the public to understand the operations and activities of the government, and provide for a general philosophy of full agency disclosure unless certain information is specifically exempt.[170] The Court determined that the only FOIA exception that would apply to an employee's home address would be the exemption for "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[171]

To determine whether the disclosure of home addresses is a clearly unwarranted invasion of privacy under FOIA, the Court looked to *Department of Justice v. Reporters Committee For Freedom of Press*,[172] which interpreted the exemptions of FOIA. In *Reporters Committee*, the Court had reasoned that in order to determine if the exemption applies the Court must balance the public interest in disclosure against the interest Congress intended to protect through the exemption.[173]

The Court, applying the *Reporters Committee* balancing test, weighed the privacy interests of the employees in not having their addresses disclosed against the extent to

---

[164] *Id*. at 492.
[165] 510 U.S. at 492.
[166] *Id*. at 493.
[167] *Id*. at 494 (citing The Privacy Act, 5 U.S.C. §552a(b)(2)).
[168] *Id*.
[169] 510 U.S. at 494.
[170] *Id*. at 495.
[171] *Id*.
[172] 489 U.S. 749 (1989).
[173] 510 U.S. at 495.

which disclosure would shed light on the agency's performance of its duties. This balancing test is notably similar to the one the Court applied in the Fourth Amendment cases discussed in Section II.A.2 of this report. The Court ultimately found that the balance favors the employees because disclosure does not further the purpose of FOIA.[174] Finding that the employees' interest in nondisclosure substantially outweighed what the Court deemed to be a negligible public interest in disclosure, the Court held that the disclosure would be clearly unwarranted and that therefore, "FOIA does not require the agencies to divulge the addresses and the Privacy Act, therefore, prohibits their release to the unions."[175]

As stated above, it is important to note that the Supreme Court did not analyze the definition of the term "record" or discuss what information should be considered a record under the Privacy Act, but rather the Court assumed that a home address is a record. This assumption arguably implies that the Court took a broad view of the definition of "record." In fact, the Court states that "the addresses sought ... are 'records' covered by the broad terms of the Privacy Act,"[176] suggesting that the Court believes the term "record" should be subject to a broad interpretation. However, because the Supreme Court has never directly analyzed what information would be considered a "record," it is necessary to examine the lower court decisions to determine how the term is defined.

Lower Court Decisions Applying Broad Interpretations of "Record"

The Second and Third Circuits have both applied a broad interpretation of the term "record." In the 1992 case *Quinn v. Stone*,[177] the Third Circuit Court of Appeals, in finding that an out-of-date home address on a roster and time card is a record covered by Privacy Act, affirmed the OMB's definition, holding that the term "record" encompasses "any information about an individual that is linked to that individual through an identifying particular" and is not "limited to information which taken alone directly reflects a characteristic or quality."[178]

In *Bechhoefer v. United States Department of Justice Drug Enforcement Administration*,[179] the Second Circuit analyzed the tests established by the other courts of appeals and essentially adopted the Third Circuit's test.[180] The Second Circuit explained its decision to adopt this test as follows: first, it found the Third Circuit's test to be "most consistent with the 'broad terms' ... of the statutory definition;"[181] second, it found the Third Circuit's test to be the only one consistent with the Supreme Court's decision in *U.S. Dept. of Defense v. Federal Labor Relations Authority* (discussed above); and, finally, it found the Third Circuit's test to be supported by the legislative history of the

[174] *See id.* at 497-499.
[175] *Id*. at 502.
[176] 510 U.S. at 494.
[177] 978 F.2d 126 (3d Cir. 1992).
[178] *Id*. at 133.
[179] 209 F.3d 57 (2d Cir. 2000).
[180] *Id*. at 60.
[181] *Id*.

Privacy Act and by the guidelines issued by OMB.[182] Finding that Congress intended the term "personal information" to have a broad meaning, the Second Circuit held that the term "record" is to be interpreted broadly to include, at the very least, any personal information "about an individual that is linked to that individual through an identifying particular."[183] Although the court was proposing a broad interpretation, the information in question was a letter containing the individual's name along with, among other pieces of information, his employment and his membership in an association. Even a court utilizing the narrowest interpretation of the term "record" would have likely found the information in this case to fit the definition of record. Yet the Second Circuit's reasoning is still important in terms of its analysis of the other circuit courts' decisions, the legislative history, the OMB Guidelines, and its ultimate agreement in theory with the Third Circuit's broad construction.[184]

Lower Court Decisions Applying Narrower Interpretations of "Record"

Other courts have taken a more narrow reading of the definition of "record." The Court of Appeals for the District of Columbia rejected the Third Circuit's view that something is a record if it is either linked to an identifying particular or is itself an identifying particular. The court instead held that to constitute a "record" the information must not only include his name or another identifying particular but must also actually describe the individual in some way (i.e. be "about" the individual).[185]

The Courts of Appeals for the Ninth and Eleventh Circuits have also adopted very narrow constructions of the term "record," thereby limiting Privacy Act coverage of personal information maintained by the government. Under those courts' narrow interpretations, in order for information to qualify as a "record" under the Privacy Act, the information "must reflect some quality or characteristic of the individual involved."[186] The D.C. Circuit rejected the Ninth and Eleventh Circuits' definitions of "record" (discussed below) as too narrow. Ultimately, the D.C. Circuit held that an NLRB computer system for tracking and monitoring cases did not constitute a system of records because its files contained no information "about" individuals, even though the

[182] *Id*. at 61-62.
[183] *Id*. at 62.
[184] Several other lower courts have also applied a broad interpretation of the term "record," including the Fourth Circuit Court of Appeals [*See, e.g., Williams v. VA*, 104 F.3d 670, 673-74 (4th Cir. 1997)], the Western District of New York [*Sullivan v. United States Postal Serv.*, 944 F. Supp. 191(1996)], and the Western District of Virginia, where the court found social security numbers to constitute records as defined by the Privacy Act. *Doe v. Herman*, 1999 U.S. Dist. LEXIS 17302 (U.S. Dist., 1999)(an appeal filed on other issues was aff'd in part, rev'd in part, 306 F.3d 170 (4th Cir. 2002), cert. granted, 123 S. Ct. 2640 (2003), and aff'd, 2004 U.S. LEXIS 1622 (2004)).
[185] *Tobey v. N.L.R.B.*, 40 F. 3d 469, 471-473 (D.C. Cir. 1994).
[186] *Boyd v. Sec'y of the Navy*, 709 F.2d 684, 686 (11th Cir. 1983) (per curiam) (although utilizing a narrow view, by finding that memorandum reflecting plaintiff's failure to follow orders and his relationship with management qualified as a record); *accord Unt v. Aerospace Corp.*, 765 F.2d 1440, 1448-49 (9th Cir. 1985) (letter written by employee containing allegations of mismanagement against corporation that led to his dismissal held not a record because it was "about" the corporation and only indirectly reflected on any quality or characteristic of the employee).

information included the initials or identifying number of the field examiner assigned to the case.[187] Although the court recognized that the case information could be, and apparently was, used in conjunction with other information to draw inferences about a field examiner's job performance, it stated that such use "does not transform the … files into records about field examiners."[188]

Several other lower courts have also limited Privacy Act coverage by applying narrower constructions of the term "record," including the District Court of New Jersey in the case of *Ingerman v. IRS*,[189] where the court found that a person's Social Security number standing alone is not a "record" under the Privacy Act because it does not contain the person's name, identifying number, or other identifying particular. The court noted that the Social Security number itself is the identifying particular, which the court felt did not constitute a record in and of itself. The same narrow construction would likely find that a biometric, in and of itself and not connected to any other identifying particular, would likewise not be a record.

According to the OMB's guidelines, even publicly available information, such as newspaper clippings or press releases, can constitute a "record."[190] Several courts have agreed with this interpretation.[191] Under such an interpretation, a biometric would constitute a record subject to the Privacy Act even if it were construed as publicly available information, since biometrics are certainly no more public than published information.

It should be noted that many biometric "records" are often one-way encrypted digitized representations that reveal nothing about the person. As such, they may be less likely to be deemed to be "records" under the Privacy Act. In iris identification, for example, there is no need to have any personal information maintained in the database. All that is needed is the encrypted template for the access control system to function. Thus, to fall under the Privacy Act, such encrypted template (separate from the biometric) would itself have to be deemed a record. Because the encrypted template cannot be traced to the person from whom it was taken, it is highly questionable whether an encrypted template is a record if there is no other personally identifying information attached to it.

---

[187] *Id*. at 471-473.
[188] *Id*. at 472-73.
[189] No. 89-5396, slip op. at 6 (D.N.J. Apr. 3, 1991); *aff'd*, 953 F.2d 1380 (3d Cir. 1992) (unpublished table decision).
[190] *See* OMB Guidelines, 40 Fed. Reg. 56,741, 56,742 (1975) ("[c]ollections of newspaper clippings or other published matter about an individual maintained other than in a conventional reference library would normally be a system of records").
[191] *See Clarkson v. IRS*, 678 F.2d 1368, 1372 (11th Cir. 1982) (permitting challenge to agency's maintenance of newsletters and press releases); *Murphy v. NSA*, 2 Gov't Disclosure Serv. (P-H) ¶ 81,389, at 82,036-37 (D.D.C. Sept. 29, 1981) (permitting challenge to agency's maintenance of newspaper clippings).

b. What is a System of Records?

Additionally, to be covered by the Privacy Act, the record must be contained in a system of records. The OMB Guidelines require two criteria for a system of records to exist, namely: (1) there must be an "indexing or retrieval capability using identifying particulars [that is] built into the system;" and (2) the agency must "in fact, retrieve records about individuals by reference to some personal identifier."[192]

According to the Department of Justice, "the highly technical 'system of records' definition is perhaps the single most important Privacy Act concept, because (with some exceptions …) it makes coverage under the Act dependent upon the method of retrieval of a record rather than its substantive content."[193] The Department of Justice points out that "a major criticism of the Privacy Act is that it can easily be circumvented by not filing records in name-retrieved formats."[194] The Department of Justice surmises that some courts, in recognizing this potential for abuse, have relaxed the "actual retrieval" standard in certain cases and that some subsections of the Privacy Act have been construed to apply even to records not incorporated into a "system of records."[195]

Therefore, if biometric information is not in a central database, then it would probably not be covered by the Privacy Act. Further, even if it is contained in a database, biometric information may not come within the parameters of the Privacy Act if it is not retrieved by the agency "by reference to some personal identifier."

However, a federal appeals panel in Washington DC recently determined that photographs were records under the Privacy Act, rejecting the argument that the photographs at issue were not records because they were not retrieved by name or other identifier. The court reasoned that "a 'system of records' may be a group of any records retrieved by an identifying particular such as a photograph. In other words, the personal identifier may be the photograph itself."[196]

A case by case analysis, including an examination of how biometrics are used, stored, and retrieved, is necessary to determine if a particular application of biometrics constitutes records maintained in a system of records.

---

[192] OMB Guidelines, 40 Fed. Reg. 28,948, 28,952 (1975).

[193] United States Department of Justice, Overview of the Privacy Act of 1974 (May 2002), citing to *Baker v. Dep't of the Navy*, 814 F.2d 1381, 1384 (9th Cir. 1987), http://www.usdoj.gov/04foia/04_7_1.html; *Shannon v. Gen. Elec. Co.*, 812 F. Supp. 308, 321 (N.D.N.Y. 1993); *see also Crumpton v. United States*, 843 F. Supp. 751, 755-56 (D.D.C. 1994) (although records disclosed to press under FOIA contained information about plaintiff, they were not retrieved by her name and therefore Privacy Act did not apply), *aff'd on other grounds sub nom. Crumpton v. Stone*, 59 F.3d 1400 (D.C. Cir. 1995).

[194] United States Department of Justice, Overview of the Privacy Act of 1974 (May 2002), citing to Privacy Commission Report at 503-04 & n.7, http://www.usdoj.gov/04foia/04_7_1.html.

[195] United States Department of Justice, Overview of the Privacy Act of 1974 (May 2002).

[196] "Prisoners' Privacy Act Suit Challenges BOP Photo Program", PRIVACY TIMES, vol. 24 no. 9, 5 (May 4, 2004) (quoting *Maydak v. U.S*, 363 F.3d 512 (D.C. Cir. 2004).

c. Privacy Act Requirements and Penalties for Noncompliance

If an agency's use of biometrics implicates the Privacy Act, e.g. if the biometric information maintained constitutes a system of records, certain procedures must be undertaken.

The Privacy Act prohibits disclosure of any record without consent, subject to a host of exceptions, including disclosures required under the Freedom of Information Act and "routine use" disclosures (disclosures and uses of such record "for a purpose which is compatible with the purpose for which it was collected").

The Privacy Act requires every federal agency maintaining a record on an individual within a system of records to: (1) permit the individual to control the use and dissemination of information contained in the record; (2) permit the individual to review, correct, or amend information contained in the record; (3) safeguard the data by "establishing appropriate administrative, technical, and physical safeguards to insure security and confidentiality of records" and "protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is maintained;" and (4) publish in the *Federal Register* a notice of the existence and the character of the system of records (known as a "Privacy Act Systems of Records Notice").

Such agencies are subject to civil suit for specified violations of the Privacy Act. There had been a split in the circuits as to whether the plaintiff must prove actual damages in the event of an intentional or willful violation. The Supreme Court recently settled this issue when it ruled for the first time that an individual must prove actual damages that resulted from an intentional or willful violation of the Privacy Act, and not merely that he suffered an "adverse effect."[197] The Court distinguished between a plaintiff having standing to sue because of a violation of the Act and suffering actual damages as a result of such violation. In other words, the Court held that a violation does not amount to per se damages. The Court focused on Section (g)(4) of the Act, which provides that if the agency acted in an intentional or willful manner, the United States is liable to an individual in an amount equal to "actual damages sustained by the individual … but in no event shall a person entitled to recovery receive less than … $1,000 …." The Court reasoned that a person was only "entitled to recovery" if he sustained actual damages. The Court declined, in this decision, to resolve the split among the federal appeals courts over whether pecuniary loss is necessary to qualify for actual damages or whether adequately demonstrated mental anxiety, without actual monetary loss, is sufficient.

[197] *Doe v. Chao*, 72 USLW 4178, 124 S.Ct. 1204 (2004).

d. The Computer Matching and Privacy Act of 1988

The Computer Matching and Privacy Act of 1988 amended the Privacy Act by adding several new provisions and definitions. These provisions added procedural requirements for agencies to follow when engaging in computer-matching activities, which involves the sharing of data among federal government agencies. The practice is often used to detect and prevent fraud because it allows agencies to essentially compare the information on their respective databases by matching a person's identifying information, such as a name or social security number.

Pursuant to the amendments of the Computer Matching and Privacy Protection Act, the Privacy Act now requires federal agencies involved in computer matching programs to (1) enter into written agreements with the other agency or agencies participating in the matching programs, (2) notify applicants and beneficiaries that their records are subject to matching, (3) verify the accuracy of the information before taking any negative action against an individual based on such information, (4) obtain the Data Integrity Board's approval of the match agreements, and (5) furnish detailed reports about matching programs to Congress and OMB.

Clearly, a biometric identifier could be used in a computer-matching program. Accordingly, any government agency using a biometric as part of a computer-matching program will need to comply with such provisions.

Section Highlights: *Summary of Privacy Act*

The Privacy Act requires that certain safeguards and procedures be implemented with respect to any records maintained in a system of records. There is some question as to whether a biometric is a "record" as such term is defined by the Privacy Act, especially if the biometric is not attached to any other information to link the biometric to the individual and no personal information about the person is maintained. Further, biometrics, arguably, are not necessarily maintained in a system that meets the Act's definition of "system of records". Accordingly, some might argue that biometrics collected for a given purpose are not subject to the Privacy Act.

However, because of the potentially steep penalties for violators, it is recommended that any government agency that collects biometric information maintain such information in strict compliance with the Privacy Act. Additionally, from a public relations standpoint, it is important that that the government comply with the Privacy Act to help allay public fears that the system will be compromised and that their privacy will be in jeopardy.

2. Executive Order 12333

Although not a statute, Executive Order 12333 (sometimes referred to herein as the "Order") is critical to a full understanding of laws that could impact the biometric industry and, in particular, government agencies and their subcontractors engaging in applied research studies of biometric technology. Unlike the Privacy Act, Executive Order 12333 does not apply to all government agencies, but applies only to certain agencies involved in intelligence activities.

The stated purpose of Executive Order 12333, which was issued by President Reagan on December 4, 1981, is "to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers."

Part 1.1 of the Order states that the goal of the United States intelligence effort is to "provide the President and the National Security Council with the necessary information on which to base decisions concerning the conduct and development of foreign, defense and economic policy, and the protection of United States national interests from foreign security threats." Part 1 also requires the Intelligence Community[198] to conduct various intelligence activities, including collection, production and dissemination of intelligence, protection of intelligence and intelligence sources and methods from unauthorized disclosure, creation of contracts for the research, development, and procurement of technical systems and devices relating to authorized functions, and cooperation within the various agencies regarding the sharing of intelligence.

Part 2.2 of the Order sets forth "certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and protection of individual interests." Accordingly, the acquisition of such information must comply with the Order and must not violate the Constitution or any other applicable law.

Part 2.3 permits the agencies listed in Part 1 (i.e. the Intelligence Community) "to collect, retain or disseminate information concerning [United States] persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." There are 10 listed categories of "types of

[198] Under Executive Order 12333 (Exec. Order No. 12333, 46 Fed. Reg. 59,941, 87 Stat. 555 (1981)) the Intelligence Community includes the CIA, the National Security Agency (NSA), the Defense Intelligence Agency, the offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs, the Bureau of Intelligence and Research of the Department of State, the intelligence elements of the Army, Navy, Air Force, and Marine Corps, the FBI, the Department of the Treasury and the Department of Energy, and the staff elements of the Director of Central Intelligence.

information" that may be collected, retained, and disseminated by the Intelligence Community. The first and most obvious type of permitted information is information that is either *publicly available* or is obtained with the *consent* of the human subject.

The following is a list of the 10 types of information that may be collected by the Intelligence Community pursuant to the Order:

1. information that is publicly available or collected with the consent of the person concerned;
2. information constituting foreign intelligence or counterintelligence;
3. information obtained in the course of a lawful foreign intelligence, counterintelligence, international narcotics, or international terrorism investigation;
4. information needed to protect the safety of any person or organization;
5. information needed to protect foreign intelligence or counterintelligence sources or methods from unauthorized disclosure;
6. information concerning persons who are reasonably believed to be potential sources or contacts for the purpose of determining their suitability or credibility;
7. information arising out of a lawful personnel, physical, or communications security investigation;
8. information acquired by overhead reconnaissance not directed at specific US persons;
9. incidentally obtained information that may indicate involvement in activities that may violate federal, state, local, or foreign laws; and
10. information necessary for administrative purposes.

The Order does not define the term "information concerning." Presumably biometric data is *information concerning* a person, which would therefore mean that collection of biometric data is subject to the limitations of the Order. However, Booz Allen Hamilton asserts that matching a person with his biometric data is not possible when the information, e.g., the fingerprint or facial image, is irreversibly converted to a data file, and that in such instance, since the data cannot be traced back to the subject person, such biometric data may not be subject to the Order.[199]

Part 2.4 of the Order provides that "agencies within the Intelligence Community shall use the least intrusive collection techniques feasible" against United States persons." Specifically, electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, and monitoring devices are not permitted "unless they are in accordance with procedures established by the head of the agency concerned and approved by the attorney general." Electronic surveillance, as defined in Part 3.4, means "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party" to the communication.

[199] Booz Allen Hamilton, *Application of Executive Order 12333 to Human Subject Research and Testing: A "Quick Look"* (October 2003).

The collection techniques prohibited by Part 2.4 that may be applicable to biometric data collection include physical search, physical surveillance, and perhaps monitoring devices.

Part 2.7 authorizes agencies within the Intelligence Community "to enter into contracts or arrangements for the provision of goods or services with private companies" in the United States.

Part 2.10 prohibits human experimentation except in accordance with guidelines issued by the Department of Health and Human Services and states that "no agency within the Intelligence Community shall sponsor, contract for or conduct research on human subjects except in accordance with guidelines issued by the Department of Health and Human Services. The subject's informed consent shall be documented as required by those guidelines."

Accordingly, any research study conducted by any agency within the Intelligence Community, including any research study involving the collection of biometric information, is subject to the specific rules of Part 2.10 and the collection restrictions in Part 2.3. If the collection of biometric data is considered human subject research and either (a) the biometric data is publicly available or (b) the subject gives informed consent, it will satisfy the limitations of the Order.

Part 3.2 places the responsibility of issuing directives and procedures in accordance with this Order in the hands of the NSC, the Secretary of Defense, the Attorney General, and the Director of Central Intelligence. Heads of the agencies within the Intelligence Community have the authority to issue supplemental directives and procedures. Until these directives and procedures are issued, Part 3.3 provides that the above parties are required to follow Executive Order 12036 (which is revoked by Executive Order 12333).

A critical point of interest with respect to Executive Order 12333 is the definition in the Order of "publicly available information." Section 2.3(a) states that the procedures established by the head of the relevant federal agency and approved by the Attorney General "shall permit collection, retention and dissemination of" information that is "publicly available." Although this may seem obvious, what is "publicly available" is subject to interpretation, especially with respect to biometric information.

While most people would probably agree that a person's face is "publicly available information," and that blood samples or even retinal information is not, whether other types of biometric information are public information is not as clear. A face is generally recognizable and distinguishable by a person simply looking at it without any special training or technical equipment, whereas to use someone's blood type or retinal information to identify him requires a more invasive acquisition of such information and advanced technology to discern the information.

What about irises? While the color and general look of one's irises may be public information, the intricate patterns that make irises one of the most accurate biometric identifiers cannot be seen with the naked eye and cannot be understood by the human mind. Are those patterns, therefore, not "publicly available information" simply because a computer is required to positively identify a person by their iris? In other words, is it more important that something can technically be seen, but not necessarily identified? Or is the test of what makes biometric information publicly available whether the average person, without any special equipment, can view it and use it to identify a person? As noted above, Section 2.4 of Executive Order 12333 prohibits "unconsented physical searches." Is a scan of one's irises to obtain the unique identifying information without the subject's consent an "unconsented physical search" or is it obtaining information that is "publicly available"?

As NBSP has recommended in its study of the Order, the procedures developed by federal agencies, in particular the CIA and NSA, should be reviewed and, as necessary, amended, to specifically address biometric information and the collection, retention, and dissemination thereof.[200] In the meantime, the Order can be satisfied by obtaining proper consent prior to collecting biometric information.

[200] National Biometric Security Project, *Biometrics for National Security (BiNS), TECHNICAL REPORT* (January 30, 2004).

Section Highlights: *Summary of Executive Order 12333*

There are several issues that must be considered with respect to Executive Order 12333 and its application to biometrics:

- Is biometric data "information concerning a person?"
- Is biometric data one of the "types of information" covered under the Order?
- Does Part 2.4 restrict the procedures in which biometric data may be collected?
- Is biometric data considered publicly available information?

Presumably biometric data would be considered "information concerning a person" and of the "type of information" covered under the Order. Accordingly, the methods and procedures by which biometric information may be collected are restricted by the Order. Most importantly, a subject's consent is required, unless the biometric data is considered public information. Most biometric data would probably not be considered publicly available information because special technology is required to capture and analyze the identifying information. Arguably, some types of biometric information, such as facial images, voice, and gait, might be deemed to be publicly available. Would drawing a distinction between types of biometric information as public vs. nonpublic hinder the use of certain types of biometric identifications, such as iris identification and fingerprinting? In any case, much the same as was previously noted in the section of this report on the Privacy Act, it is advisable to err on the side of caution and follow the procedures of Executive Order 12333, both from a liability standpoint and from a public relations standpoint.

"A lie can travel halfway around the world while the truth is putting on its shoes."

Mark Twain

III. PRIVACY AND NATIONAL SECURITY

The attacks of September 11th brought national security and border control to the forefront of Americans' minds. Changes in security measures can be seen in airports across the country where travelers must wait in long lines at security checkpoints and remove their shoes for inspection by airport security. Like the privacy laws governing the private sector, many of the airport security measures used today were enacted in response to specific events. Passenger shoe inspection followed the arrest of Richard Reid (known as "the shoe bomber") who had explosives hidden in his shoes. Following the bombing of Pan Am Flight 103, when a terrorist surreptitiously packed a bomb in his girlfriend's suitcase, passengers are now asked whether they packed their own bags.

Today, with falsification of identity a choice tool for terrorists, biometric recognition technology has tremendous potential for thwarting terrorists. Its use in border security in the United States has already been implemented and further uses are planned. Biometric passports have the potential to obviate the need to inspect each passenger and allow airport personnel to focus more attention on "high risk" passengers.

This section discusses the application of biometric recognition technology in national security and the laws that could impact such use. This section examines some of the laws geared towards improving national security and certain recommendations made by the 9/11 Commission. This section also looks at immigration law and how the legal status of immigrants ties in to national security measures, including the use of biometrics. Finally, this section briefly reviews some international considerations and how the policies of other countries and of the international community as a whole impact our use of biometric recognition technology in national security.

A. NATIONAL SECURITY LAWS

When it comes to individual privacy rights, national security is in a category of its own. Certain measures that would be considered privacy invasive in almost any other context are permissible in the context of national security. The Patriot Act brought into the question of the minds of many American whether the government was going "too far" and overly broadening what was considered "national security." However, even prior to the Patriot Act, there were different rules with respect to privacy when it came to national security.

Wiretapping and Surveillance

One year after the *Katz*[201] decision, Congress passed the Federal Wiretap Act of 1968 to protect the privacy of conversations against both government and private intrusions.[202] Under the Act, the government must have a warrant based on probable cause that a crime has been or is about to be committed in order to eavesdrop on conversations. The restrictions under the Act were loosened by the Patriot Act to allow the FBI to obtain wiretap warrants to investigate terrorism and computer fraud and abuse.[203] However, even prior to the Patriot Act, there was a special law governing wiretaps used for national security purposes that was enacted following the 1972 case of *United States v. United States District Court*. [204]

In *United States v. United States District Court*, the Court held that the President of the United States was required by the Constitution to obtain a search warrant before wiretapping the telephones of Americans suspected of domestic crimes related to national security. In response to that case, Congress enacted the Foreign Intelligence Surveillance Act of 1978 ("FISA").[205] FISA essentially provides for a "closed judicial process to balance individual rights and Government secrecy needs in determining whether wiretapping is justified."[206] FISA established special courts to issue court orders for electronic surveillance to obtain foreign intelligence information through electronic surveillance of a foreign power or agent of a foreign power. As defined under FISA, "foreign power" includes groups engaged in international terrorist activities. Unlike traditional warrants, FISA does not require probable cause that a crime has been committed. The requirements for a FISA court order "are dramatically softer than

---

[201] 389 U.S. 347 (1967), discussed *supra* at Section II.A.2.b.
[202] 18 U.S.C.A. § 2510 et seq.
[203] John W. Whitehead & Steven H. Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AM. U.L. REV. 1081, 1108 (2002).
[204] 407 U.S. 297 (1972).
[205] TURKINGTON & ALLEN, *supra* note 19, at 210.
[206] *Ponte v. Real*, 471 U.S. 491, 515 (1985).

requirements for a wiretap to investigate domestic crimes under … the federal wiretap act."[207]

The Patriot Act further expanded the federal government's investigative powers under FISA. As amended, the government need only certify that obtaining foreign intelligence information is a "significant," rather than a "primary" purpose. According to Attorney General Ashcroft, this change allows FISA to be used even if the primary purpose is law enforcement, as long as there is a significant foreign intelligence purpose as well.[208] Additionally, federal officers are no longer restricted from sharing information obtained through a FISA surveillance with law enforcement officials.

In a 1980 Fourth Circuit case,[209] the court rejected the government's argument that if surveillance was in any way related to gathering foreign intelligence information, the government was not subject to Fourth Amendment requirements applicable to domestic criminal procedure. The court held that where the primary purpose of the surveillance is a criminal investigation, the Fourth Amendment requirements of probable cause apply.[210] The Supreme Court has never ruled on the constitutionality of FISA and its curbing of the Fourth Amendment requirements.

International Travel

Travel, in particular air travel, raises a myriad of issues, including passenger safety, terrorism, ease of travel, international tourism, and the rights of travelers. Many of these issues inherently conflict with one another. International air travel raises additional issues, such as immigration and fleeing felons. The goal is to address the many security issues without compromising the rights of travelers or making travel unduly burdensome.

Under the Aviation and Transportation Security Act,[211] for all inbound international flights, airlines are required to provide to the Commissioner of Customs "passenger manifests" containing the name, citizenship, date of birth, gender, and passport or visa or resident alien card number of each passenger. This information, which is embedded in the passport, is sent from the port of departure to the port of arrival to be checked by immigration at the destination country. This information may also be shared with other federal agencies upon request for national security purposes. Adding biometric information to passports and having such information transmitted along with the information that is already being transmitted, raises no additional legal issues. A program to develop and implement the use of biometric passports is currently underway.

On October 24, 2005, all 27 "Visa Waiver Program" countries (which includes the United Kingdom, France, Italy, Germany, Spain, Japan, Australia, and New Zealand

[207] TURKINGTON & ALLEN, *supra* note 19, at 212.
[208] RICHARD C. TURKINGTON & ANITA L. ALLEN, PRIVACY LAW: CASES AND MATERIALS, 3 (Supp. 2003).
[209] *United States v. Truong Dinh Hing*, 629 F. 2d 908 (4th cir. 1980).
[210] *Id*. at 916.
[211] 49 U.S.C. §44909.

to name but a few) will be required to issue biometric passports in order for its citizens to be granted entry into the United States. This date was recently extended from the original deadline of October 24, 2004, which was supposed to coincide with a separate but related program whereby such passports must be machine-readable. Under these two programs, all passports issued on or after the deadline must be machine-readable and must be embedded with biometric information in compliance with standards issued by the International Civil Aviation Association (ICAO). In May 2003, ICAO determined that facial recognition would be the standard passport biometric. Passports issued before that date will not have to contain biometric data, but will have to be machine-readable. If a passport issued on or after the deadline does not contain the requisite biometric data, or if on or after that date any passport is not machine-readable, citizens traveling from those countries will be required to obtain a visa.[212]

There are many issues and concerns surrounding the Visa Waiver Program. There are interoperability issues (e.g. can a United States scanner read another country's biometric chip?) and technological and logistical difficulties of a large-scale implementation of biometric passports. The 9/11 Commission, in supporting the use of biometric passports, has recommended that the United States work with other countries to "improve passport standards and provide foreign assistance to countries that need help in making the transition [to biometric passports]."[213] The 9/11 Commission believes that the use of biometric passports will serve the dual purposes of enhancing security and easing travel.[214]

Biometric information of passengers is subject to the same rules and afforded the same protections as all other passenger information. On September 22, 2003, the Electronic Privacy Information Center (EPIC) filed a complaint against JetBlue Airlines Corporation contending unfair and deceptive practices in violation of the Federal Trade Commissions Act (the "FTC Act") for disclosing passenger information in September of 2002.[215] The EPIC is basing its argument on the fact that JetBlue provided in its privacy policy that no personal passenger information would be shared with third parties. EPIC contends that by sharing such information with other parties in connection with a Pentagon study, JetBlue violated its policy and mislead its customers into believing their information would not be disclosed as it was.[216] According to EPIC, the FTC is investigating this complaint.[217]

In other pending litigation against Jetblue, consumers have filed claims for privacy violations in connection with Jetblue's release of their passenger information, which they claim is in violation of state and federal privacy rights. Nine separate class actions were filed around the country. These cases were subsequently consolidated into one case, *In re: Jetblue Airways Corp. Privacy Litigation*, and transferred to the United

---

[212] Visa Waiver Program, U.S. Department of State: Bureau of Consular Affairs: Visa Services, *at* http://travel.state.gov/vwp.html#7 (last visited May 27, 2004).
[213] THE 9/11 COMMISSION REPORT at 389.
[214] *Id.* at 388-389.
[215] EPIC Complaint, at http://www.epic.org/privacy/airtravel/jetblue/ftccomplaint.html.
[216] *Id.*
[217] EPIC Litigation Docket, at http://www.epic.org/privacy/litigation/.

States District Court for the Eastern District of New York on Feb 24, 2004. The case is currently pending.[218]

However, a similar case against Northwest Airlines filed a couple of months after the JetBlue claim was recently dismissed. On January 20, 2004, EPIC and Minnesota Civil Liberties Union (MCLU) filed a complaint against Northwest Airlines saying they engaged in unfair and deceptive practice in violation of the FTC Act in giving out passenger information as part of a government study in 2001.[219] In Northwest's Answer to the Complaint, Northwest stated as its defense that "the privacy rights advocated by EPIC and MCLU do not exist in the rules, precedent or practices of the Department [of Transportation]," that there is "no applicable right to privacy imposed by any other federal law," that "passengers have no inherent right or expectation of total privacy in the information they provide when traveling on commercial airlines," and that "the only basis for any right to privacy on the part of customers of Northwest" is Northwest's privacy policy.[220] On June 6, 2004, the United States District Court, District of Minnesota dismissed the case.[221] The court found no direct harm and held that the release of passenger information under the circumstances was not an unreasonable disclosure, stating:

> In this instance, Plaintiffs voluntarily provided their personal information to Northwest. Moreover, although Northwest had a privacy policy for information included on the website, Plaintiffs do not contend that they actually read the privacy policy prior to providing Northwest with their personal information. Thus, Plaintiffs' expectation of privacy was low. Further, the disclosure here was not to the public at large, but rather was to a government agency in the wake of a terrorist attack that called into question the security of the nation's transportation system. Northwest's motives in disclosing the information cannot be questioned. Taking into account all of the factors listed above, the Court finds as a matter of law that the disclosure of Plaintiffs' personal information would not be highly offensive to a reasonable person and that Plaintiffs have failed to state a claim for intrusion upon seclusion.[222]

It will be interesting to see if the JetBlue case currently before the Eastern District of New York has a similar outcome. Both cases are primarily based on arguments of

---

[218] *In re: JetBlue Airways Corp. Privacy Litigation*, 2004 WL 385129, ---F.Supp.2d--- (J.P.M.L. 2004); *In re: JetBlue Airways Corp. Privacy Litigation*, Docket No. 1:04-md-01587 (E.D.N.Y. 2004).

[219] *In the Matter of Northwest Airlines, Inc.*, Docket OST-04-16939-1, Complaint and Request for investigation, injunction, and for other relief, 1 (January 20, 2004), *at* http://www.epic.org/privacy/airtravel/nwa_comp.pdf, also *available at* Department of Transportation, Docket Management System, http://dms.dot.gov/.
This complaint action is currently pending. *See* Department of Transportation, Docket Management System, Docket OST-04-16939, http://dms.dot.gov

[220] *Id*. at 3. A copy of the Answer of Northwest Airlines, Inc., can be found on EPIC's website at http://www.epic.org/privacy/airtravel/nwa_answer.pdf.

[221] In re Northwest Airlines Privacy Litigation, No. Civ. 04-126 (June 6, 2004).

[222] *Id.* at 5.

trade violations, and not of privacy laws, and are premised on violations of the airlines' own privacy policies. In June 2002, American Airlines acknowledged that it had shared approximately 1.2 million passenger itineraries with the Transportation Security Administration.[223] No lawsuits have been filed against American Airlines. Perhaps this is because at the time the itineraries were shared, American Airlines did not have a privacy policy expressly prohibiting the sharing of passenger data.

[223] Brad Foss, *Airline Admits Giving U.S. Passenger Data*, THE ASSOCIATED PRESS, April 9, 2004.

B. IMMIGRATION LAWS

Immigration law plays a key role in national security. Accordingly, it is worth examining how immigration law might impact the use of biometrics for national security.

The 9/11 Commission found that "had the immigration system set a higher bar for determining whether individuals are who or what they claim to be – and ensuring routine consequences for violations – it could potentially have excluded, removed, or come into further contact with several [of the 9/11] hijackers who did not appear to meet the terms for admitting short-term visitors."[224]

Generally, the courts have been reluctant to impose any limitations on the power of Congress to determine whether foreign nationals may enter the country, and have been unwilling to attribute any constitutional protections to those individuals.[225] As such, those individuals are afforded few if any of the protections offered citizens of the United States until such point as they are officially granted entry to the United States by border officials.

In contrast, non-citizens who have entered the United States, legally or otherwise, are generally considered to have a broader range of rights and protections, most importantly due process under the Fourteenth Amendment. Accordingly, the government has a great interest in scrutinizing who is seeking to cross the border before allowing such person to step over the threshold into a constitutionally protected zone. However, Congress may still expressly discriminate against non-citizens in certain circumstances.[226] Examples of such legal discrimination include laws limiting the ability of non-citizens to work in the United States, laws prohibiting the employment of foreign nationals in certain sensitive positions, and laws deeming the sharing of information with a resident foreign national an export for the purpose of certain export laws.

Ultimately, the result of this permitted discrimination is that many of the constitutional protections available to United States citizens would not necessarily be available to foreign nationals, whether in the United States or not. Accordingly, most limitations imposed on the privacy rights of foreign nationals that are intended as part of the country's immigration or national security law would be upheld. This could include the taking of any additional biometrics deemed necessary by Congress (or, by delegation, the Executive Branch). Conversely, statutes that expressly apply to foreign nationals, such as the Privacy Act, which is applicable to United States citizens and legal permanent residents,[227] would certainly be enforceable as such.

---

[224] THE 9/11 COMMISSION REPORT at 384.
[225] *Chae Chan Ping v. U.S.*, 130 U.S. 581, 9 S.Ct. 623, 32 L.Ed. 1068 (1889).
[226] STEPHEN H. LEGOMSKY, IMMIGRATION AND REFUGEE LAW AND POLICY, 1170-1174 (3d. Ed. 2002).
[227] 5 U.S.C. 552a(a)(2).

One of the most important new programs relating to the use of biometrics is the US-VISIT program. The program is the culmination and implementation of a number of different legislative acts intending to ensure the accurate tracking of foreign nationals entering and exiting the United States.[228] Although originally limited to holders of certain nonimmigrant visas at certain air and sea ports of entry, within weeks of its implementation earlier this year, the program was expanded to include many non-visa countries, including Canada and the United Kingdom. US-VISIT is intended to eventually encompass the bulk of all entries into the United States and will result in an unprecedented flood of data about foreign nationals. Currently, US-VISIT requires covered foreign nationals to submit digital photographs and fingerprints. This data will be maintained in the United States. Foreign nationals covered under the program who refuse to provide the requested biometric information upon entry may be deemed inadmissible to the United States for failure to provide the required documentation. A foreign national who intentionally fails to provide biometric information on exiting the United States may be found to have violated the terms of his or her immigrant status, which can have significant repercussions up to and including possible denial of future visas.

The 9/11 Commission has recommended that the US-VISIT program be expanded, that it include exit data as well as entry data, and that Americans not be exempt from the program. To enable wider screening capabilities and ease travel, the Commission recommends that there be a pre-enrollment capability for frequent travelers and that all of the border systems be consolidated into an integrated system. [229] The Commission believes that if effectively implemented and used, such a system could help reverse the trend of declining travel to the United States since the September 11th attacks.[230]

[228] For a complete recitation of the background and the planned implementation of US-VISIT *see* Federal Register / Vol. 69, No. 2, Implementation of the United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Biometric Requirements; Notice to Nonimmigrant Aliens Subject To Be Enrolled in the United States Visitor and Immigrant Status Indicator Technology System; Interim Final Rule and Notice.

[229] THE 9/11 COMMISSION REPORT at 388.

[230] *Id*. at 389. The Commission found that the present air travel security system is disrupting travel to the United States, citing reports that visa applications in 2003 were down over 32 percent since 2001, and in the Middle East visa applications were down approximately 46 percent.

C. INTERNATIONAL CONSIDERATIONS

While United States law may not offer much in the way of protection to foreign nationals, this is not to say that those nationals have no protection whatsoever. As discussed above, US-VISIT requires the collection of data and biometrics on many travelers to the United States. Although the program is replete with privacy protections, which include security mechanisms to ensure that sensitive data is not improperly disseminated,[231] and despite a preliminary determination that the tentative agreement reached between the European Union and the United States to protect data was adequate, many politicians and European Union officials continue to push for further limitations on the use of data collected on Europeans under US-VISIT.[232] The primary concern is that the requirements under US-VISIT conflict with the provisions of European law dealing with privacy rights of European citizens, particularly the European Union Privacy Directive and the Charter of Fundamental Human Rights.[233] The privacy rights afforded by the European Privacy Directive are much more extensive than those granted under the United States Constitution and the United States statutory scheme, and impose significant limitations on the storage, transfer, and disclosure of personal information on European citizens.

Given the number of Europeans traveling to the United States each year, this is not an insignificant matter. Indeed, one estimate puts the number of annual European travelers from whom data (including biometric data) will be collected at over 10 million.[234] That volume of travelers will put significant pressure on the United States and European governments, as well as other governments who are considering implementing similar programs, to attempt to find a way to reconcile such programs with the privacy laws of other nations. The OECD Guidelines, which were adopted on September 23, 1980, provide guidance on the collection and management of personal information, including with respect to transnational data.[235] The premise of the Guidelines is the recognition of a common interest among member nations (which includes the United States and many European countries) in protecting privacy and civil liberties and

---

[231] US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary (December 18, 2003), http://www.dhs.gov/interweb/assetlibrary/VISITPIAfinalexecsum3.pdf.

[232] Ryan Singel, *EU Travel Privacy Battle Heats Up*, WIRED NEWS, Dec 22, 2003, http://www.wired.com/news/politics/0,1283,61680,00.html.

[233] Council Directive 95/46/EC, art. 8, 1995 O.J. (L 281/40)(Article 8 of the European Convention on Human Rights)(hereinafter "the Privacy Directive"), as well as The Charter of Fundamental Rights of the European Union, art. 7, art. 8, 2000 O.J. (C 364).

[234] Article 29 Data Protection Working Party, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the [Passenger Name Record] PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP), 10019/04/EN at 3 (January 29, 2004), *available at* EUROPA, The European Commission, Internal Market, at http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm#wp87.

[235] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

"reconciling fundamental but competing values such as privacy and the free flow of information."[236]

The European Union Privacy Directive established, among other things, a committee[237] responsible for advising the European Union on privacy issues (the "Committee"). Echoing previous reports in June 2002 and April 2003, the Committee, in a report issued earlier this year,[238] reached the conclusion that the US-VISIT program violates the European Union Privacy Directive in a number of different ways. Particular concerns included the quality and reliability of the data and the limitation of its use to fighting terrorism and narrowly defined terrorism related crimes. The Committee further noted that the storage and transfer of such data should be as limited as possible, and that such data should not be used for the Computer-Assisted Passenger Prescreening System (CAPPS) or similar programs, including the processing of biometric data. As required under the European Union Privacy Directive, the Committee also wished to ensure that the passengers be kept informed as to the use of their data, and that they would have access to the data for correction purposes.

CAPPS II is the successor to the original CAPPS system, which was in place on September 11, 2001 and is still used for airport security today. At the time of the September 11th attacks, passengers flagged by the CAPPS system (including more than half of the 9/11 hijackers) were not searched. Instead, their check-in luggage was screened for explosives and held off the plane until the passenger had boarded. Under the new CAPPS system, flagged passengers now undergo searches that include a search of the individual and of any carry-on luggage.[239] CAPPS II will go even further and seek to authenticate passengers' identity and assess risk using available data and intelligence information.[240] Due to privacy concerns, the implementation of CAPPS II has been delayed and an interim program has been used since March 2003 when the program was to originally start. On May 28, 2004, an agreement that reportedly satisfies European concerns over privacy was signed between the United States and the European Union for sharing information on airline passengers under CAPPS II. It has been reported that "[t]he agreement allows U.S. authorities to check passenger information against U.S. data bases to determine whether any travelers are terrorist threats" and "also allows the U.S. government to use the data base as part of an antiterrorism program that would use personal information to assign threat levels to all airline passengers."[241]

---

[236] Recommendation of the Council Concerning Guidelines Governing the protection of Privacy and Transborder Flows of Personal Data (September 23, 1980), published in OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

[237] Article 29 of the Privacy Directive, Council Directive 95/46/EC, 1995 O.J. (L 281) 40, established the Data Protection Working Party, Council Directive 95/46/EC, art. 29, 1995 O.J. (L 281) 40.

[238] Article 29 Date Protection Working Party, Opinion 2/2004 at http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm#wp87.

[239] THE 9/11 COMMISSION REPORT at 392-393.

[240] The Department of Homeland Security website at http://www.dhs.gov/dhspublic/display?content=3162.

[241] Leslie Miller, *U.S., EU Sign Deal on Airline-passenger Data*, PHILA. INQUIRER, May 29, 2004, at A2, *available at* http://www.philly.com.

Although the impact of the Committee's report on the biometric industry is indirect at best, the Committee's report evidenced a distinct distrust of CAPPS II and of the processing of biometric data.[242] Rumors of a merger of the CAPPS II and US-VISIT programs have raised additional concerns that it would impact United States citizens as well, although United States officials have denied any such intentions.[243] Ironically, some European countries have proposed anti-terror legislation that would also involve the collection of biometric data.[244] Ultimately, although negotiations continue, European pressure to limit the collection, transfer, and storage of personal data, including biometric data, on European Union nationals will likely continue.

Section Highlights: *Summary of Privacy and National Security*

Although individual privacy rights are still a concern, the laws protecting privacy are much less stringent in the context of national security, particularly in the areas of international travel and terrorist intelligence. Still, public resistance to biometric recognition technology abounds, even in the face of international terrorism. Such public resistance can be as much of an impediment to the implementation of biometric recognition technology as the law. In addition to the American public, there is also resistance from other countries, whose cooperation is key to a successful implementation of any biometric identification program that will impact international travel, such as the biometric passport initiative and even the US-VISIT program. In implementing any such program, it is essential that the United States look not only to its own privacy laws, but also take into consideration the privacy laws and public sentiments of other countries.

---

[242] Article 29 Date Protection Working Party, Opinion 2/2004 at http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm#wp87.

[243] Ryan Singel, CAPPS II Stands Alone, Feds Say, WIRED MAGAZINE, January 13 2004, http://www.wired.com/news/privacy/0,1848,61891,00.html.

[244] German Interior Minister Otto Schilly's anti-terror legislation, for example, Frankfurter Allegemeine Zeitung, English Edition, System Does Not Meet EU Standards, Jan 23, 2004.

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account must spread abroad, I will keep to myself, holding such things to be shameful to be spoken about."

Excerpt from the Hippocratic Oath

IV. PRIVACY LAWS APPLICABLE TO THE PRIVATE SECTOR

The previous section addressed laws applicable to the public sector. This section of the report discusses laws governing the private sector, which includes individuals and private entities.

As stated in the Introduction to this report, statutory privacy law has developed piecemeal in reaction to social and political events. This is especially true in the private sector, where there is no one privacy statute that governs private entities and individuals. This section of the report explores some of the privacy statutes governing the private sector, including HIPAA (in Part A), which governs the health care industry, several laws governing the financial industry (in Part B), and two laws governing the computer industry (in Part C). The inclusion of the laws in this section is by no means an exhaustive list. The exclusion of the numerous other laws that impact the private sector is not because such laws are not important. The laws that were selected for inclusion in this report were chosen because of the implications such laws could have on the biometric industry.

As stated above, health care, finance, and computers are by no means the only private industries governed by specific privacy statutes. Other industries, such as education, telecommunications, telemarketing, cable, even the video rental industry, have specific statutes that have been developed to protect the privacy of consumers of such industries. Accordingly, if any industry or business that is subject to a specific privacy law were to implement biometric technology, the specific laws relating to that industry would have to be examined and analyzed. This report does not seek to address those issues.

A. HIPAA

HIPAA is an acronym for the Health Insurance Portability and Accountability Act of 1996. HIPAA was originally enacted to create portability of health insurance, e.g. when an employee changes jobs. However, Congress recognized the need to standardize the electronic transmission of health care information while at the same time protect the privacy of health information. HIPAA contains certain administrative simplification provisions designed to increase the efficiency of health care plan administration and to decrease health care costs by encouraging the use of electronic data interchange. All health care plans will be required to accept and transmit health information electronically using a format and codes prescribed by the government. HIPAA also contains regulations relating to the privacy of health care information and separate rules relating to the security of systems on which health care information is maintained. The privacy regulations are known as the HIPAA Privacy Rule.[245]

Prior to the implementation of the HIPAA Privacy Rule, state law governed the privacy of health information and medical records. HIPAA created a floor, or a minimum standard of privacy, with respect to health information. HIPAA does not preempt any state law that is stricter than the HIPAA Privacy Rule. For example, Pennsylvania has a law governing HIV and AIDS information, which is much stricter than anything contained in HIPAA. Thus, health care professionals in Pennsylvania must adhere to both HIPAA and to Pennsylvania's law with respect to HIV and AIDS information.

HIPAA is an interesting statute because it requires the use of technology to protect and safeguard health information, while at the same time recognizing that such technology has the potential to compromise the security of such information. In this way, the concerns Congress faced in enacting HIPAA are similar to the concerns surrounding biometric technology. On the one hand, biometric technology is viewed as privacy enhancing because it can be used to secure private information, while on the other hand, it is also viewed as privacy-adverse in that it can be used in a privacy-invasive manner. Because the HIPAA Privacy Rule is one of the most comprehensive privacy laws ever enacted, it is worth examining, even though its impact on the biometric industry may, at least in the foreseeable future, be minimal. Further, it is possible that the same or similar systems designed to securely handle health information can be used for securely handling biometric information.

The HIPAA Privacy Rule (which is merely one component of HIPAA, but by far the most well-known) contains restrictions and requirements that "covered entities" (e.g. primary health care providers and health insurance companies) and related "business

[245] The HIPAA Privacy Rule is found at 45 C.F.R. pts 160 & 164, 65 Fed. Reg. 82462-01 (December 28, 2000).

associates" must follow in protecting the privacy of an individual's health information. These privacy regulations could be relevant to the biometric industry because of the potentiality for health information to be identifiable through biometrics (e.g. detecting AIDS, diabetes, or pregnancy through someone's iris or retina). However, because HIPAA only applies to certain "covered entities," it is questionable whether or how such health information, if in fact detectable through biometrics, would come under the scope of HIPAA. On the other hand, if a hospital or other "covered entity" were to use biometric identification for nearly any purpose, then HIPAA would certainly have to be considered.[246] For example, as part of its security measures, a hospital might use biometrics to control access to HIPAA-covered medical records.

The following excerpt from an op-ed article in *The New York Times* demonstrates the tension between privacy and security, as well as the malleability of what is considered a reasonable expectation of privacy.

> …. As reported last week by Robert Pear and Eric Lichtblau in The Times, the Justice Department said that medical patients "no longer possess a reasonable expectation that their histories will remain completely confidential."
>
> This abhorrent philosophy underlies a counterattack launched by Justice at doctors who went to court to challenge the federal Partial Birth Abortion Ban Act….
>
> Justice issued subpoenas to hospitals in several cities across the nation for the medical records of hundreds of women who had undergone abortions. After hospitals protested that the order flew in the face of federal and state privacy laws, Justice offered to allow the individual names to be blotted out. In Chicago, Northwestern Memorial argued in court that patients would not trust such redaction of their records — copies of which would pass through hundreds of hands — to keep private such an intimate procedure.
>
> The judge quashed the subpoena, but Justice is appealing. "Congress created a zone of privacy relating to medical information," says Chicago Congressman Rahm Emanuel. "Who would have thought the first one to violate it would be the federal government?" Medical records contain dates of treatment, doctors' names, prescriptions — all clues to identity. Who would not be deterred from going to a hospital that meekly passed along those records?
>
> This intrusion cannot be justified by a claim to protect the nation from a terror attack. In Pittsburgh, however, the F.B.I. has set up a pilot Strategic

[246] Columbia Presbyterian Hospital in New York has used a hand geometry scanner since 1997 to control physical access and to monitor employee attendance. JOHN D. WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS: IDENTIFYING AND ADDRESSING SOCIAL CONCERNS, 96 (2001).

> Medical Intelligence unit under that very rubric. Doctors in Pennsylvania and West Virginia are expected to notify S.M.I. bioterror experts of any "suspicious event," from an unusual rash to a finger lost in an explosion, identifying but not informing the patient.
>
> It's proper for a doctor to report a case of spousal or child abuse to the police, or to query the Centers for Disease Control about a mysterious infection. But how do patients feel about their doctors first secretly calling the F.B.I.? Where is the oversight to protect the innocent injured or ill? Where is the patient's informed consent?[247]

It is especially significant that the actions described in the above article are taking place following the enactment of HIPAA's privacy protections. This highlights the ability of the government to further a public interest (i.e. ensuring compliance with a federal law) even in the face of laws designed to protect the privacy of individuals.

[247] William Saffire, *Privacy in Retreat*, N.Y. TIMES, March 10, 2004 (Op-Ed). On March 18, 2004, a federal judge in Manhattan ordered New York-Presbyterian Hospital to turn over to the Justice Department records on abortions performed there, which the Department of Justice says it needs to defend the Partial-Birth Abortion Ban Act passed by Congress last year. The Department of Justice says the disclosure would not unduly harm the hospital or the privacy of its patients. Eric Lichtblau, *New York Hospital Is Ordered to Release Abortion Records*, N.Y. TIMES, March 20, 2004.

B. STATUTES GOVERNING BANKS AND OTHER FINANCIAL INSTITUTIONS

There are several statutes aimed at protecting the privacy of individuals with respect to information they share with their banks and other financial institutions. Because almost every adult American does business with a bank and shares personal information with a bank, and because of the likelihood of more widespread use of biometrics in the banking industry (e.g. in connection with ATM access), such laws deserve some attention in this report.

1. The Gramm-Leach-Bliley Act

The Financial Modernization Act of 1999,[248] more commonly known as the Gramm-Leach-Bliley Act (the "Act"), regulates the sharing of personal information about individuals who obtain financial products or services from financial institutions.

As described in the introductory section of the Act, its purpose is to "enhance competition in the financial services industry by providing a prudential framework for the affiliation among banks, securities firms, insurance companies, and other financial service providers." Title V of the Act is aimed at ensuring that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' personal information. In furtherance of this policy, financial institutions must meet certain standards relating to administrative, technical, and physical safeguards to (1) insure the security and confidentiality of customer records and information that is "nonpublic information;" (2) protect against any anticipated threats or hazards to the security or integrity of such records; and (3) protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.

Under the Act, financial institutions must comply with procedures concerning the disclosure of information to a nonaffiliated third party. Such procedures include the financial institution providing adequate notice to its customers of its policies on sharing of personal financial information and giving consumers the option to direct that personal financial information not be disclosed or shared (i.e. the ability to "opt-out"). A party that receives nonpublic personal information from a financial institution in compliance with the Act is likewise prohibited from disclosing such information. There are exceptions to the nondisclosure rules, including disclosures for the prevention of fraud or pursuant to a subpoena. The Act also specifically permits law enforcement to obtain customer information (e.g. by making false representations or presenting forged documents) in connection with an investigation of the financial institute's compliance with the Act and its security procedures.

[248] Pub. L. No. 106-102, 113 Stat. 1338 (1999).

The term "customer information of a financial institution" is defined, for purposes of the section on fraudulent access to financial information, as any information maintained by or for a financial institution that is derived from the relationship between the financial institution and a customer of the financial institution and is identified with the customer. Clearly, if a bank obtains biometric information from a customer in connection with its relationship with such customer, such information would be considered "customer information."

The Act also defines the term "nonpublic personal information," for purposes of the section on disclosure of nonpublic personal information, as personally identifiable financial information that is provided by a consumer to a financial institution, resulting from any transaction with the consumer or any service performed for the consumer, or otherwise obtained by the financial institution. If biometric information is *not* considered public information, then the Act's restrictions on disclosure of nonpublic information will cover biometric information obtained by a financial institution. As discussed in the section of this report on Executive Order 12333, arguments can be made to support both sides of the position as to whether biometric information is public information.

2. The Right to Financial Privacy Act of 1978

Like the Gramm-Leach-Bliley Act, The Right to Financial Privacy Act of 1978[249] also protects the confidentiality of personal financial records contained in bank records. A financial record means any record, or information derived therefrom, held by a financial institution relating to a customer's relationship with the financial institution. Thus, any biometric data of a customer maintained by a financial institution would be subject to the Right to Financial Privacy Act, which requires a government agency to obtain an administrative subpoena or summons, a qualified search warrant, or a qualified judicial subpoena, or to make an appropriate written request in order to obtain such information from the financial institution. Although the customer must receive notice of such release, notice may be delayed up to 90 days for a specific reason, e.g. if there is reason to believe that notifying the customer could jeopardize an investigation or endanger someone's life.

The Right to Financial Privacy Act of 1978 was recently amended by the Patriot Act to allow law enforcement agencies to obtain financial data in connection with protection against international terrorism.

[249] 12 U.S.C. §§3401-3422 (1978).

3. The Bank Secrecy Act

As originally enacted, the Bank Secrecy Act[250] required insured banks to maintain appropriate records of information with respect to the ownership, control, and management of the bank or institution. This information has a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings. The Bank Secrecy Act was extended by the Patriot Act to include uninsured banks, uninsured institutions, and any financial institutions in furtherance of conducting intelligence and counterintelligence activities. The information to be maintained by these institutions includes evidence of the identity of each person either having an account with such institute or authorized to take any actions with respect to such account. The Secretary of the Treasury may request this information when he determines that it would be useful for the purposes specified above, e.g. in protecting against international terrorism. Clearly, biometric information is evidence of identity and would come within the parameters of the Bank Secrecy Act.

4. The Electronic Fund Transfer Act

The Electronic Fund Transfer Act[251] requires institutions operating banking services to inform customers of the circumstances under which automated banking account information will be disclosed to third parties in the ordinary course of business. It does not, however, mandate when information may or may not be disclosed. Presumably, if biometric recognition technology were used for automated banking (e.g. for access security), such information would be subject to the Electronic Fund Transfer Act.

5. The Fair Credit Reporting Act

The Fair Credit Reporting Act[252] governs consumer-reporting agencies, which are agencies that regularly engage in the practice of assembling or evaluating consumer information for the purpose of furnishing consumer reports to third parties. Such consumer information often includes names, addresses, and detailed credit histories. Credit reporting agencies are required to release such information (1) pursuant to a court order or subpoena or (2) to a government agency authorized to conduct investigations of intelligence or counterintelligence activities or international terrorism.

The Fair Credit Reporting Act was also amended by the Patriot Act to allow law enforcement agencies to obtain financial data in connection with protection against international terrorism.

If a biometric, such as a fingerprint, were used in lieu of or in addition to a Social Security number, then the Fair Credit Reporting Act would presumably govern such information.

---

[250] The Bank Secrecy Act, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended in scattered sections of 12 U.S.C.S. and 31 U.S.C.S.).
[251] 15 U.S.C. §§1693-1693r.
[252] 15 U.S.C. §§1681-1681t.

C. STATUTES GOVERNING COMPUTERS

There are many laws governing computer use, including several that specifically address Internet use. This report briefly looks at two computer laws that could have implications in the biometric industry.

1. The Computer Security Act of 1987

The Computer Security Act of 1987[253] was enacted to protect sensitive information by creating and establishing minimum standards of security practices for federal computer systems. It requires NIST[254] to develop such standards. It also mandates the establishment of "security plans" for federal systems that contain "sensitive information." It defines "sensitive information" as data that could "adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled" under the Privacy Act of 1974.

Accordingly, if a federal computer system contains biometric information, it arguably must meet the standards developed by NIST to safeguard such information.

2. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act[255] makes it a criminal offense to access federal computers without authorization, either to obtain information or to cause harm to such computers (e.g. transmitting a virus). The crime is punishable by fines and up to twenty years in prison. The Patriot Act increased the fines.

The Patriot Act also adding a new offense under the Computer Fraud and Abuse Act for damaging computers used for national security or criminal justice. Accordingly, any system containing biometric or other information used for national security or criminal justice would be protected by the Computer Fraud and Abuse Act.

[253] 40 U.S.C. §759.
[254] NIST is an acronym for the National Institute of Standards and Technology, which, at the time of the passage of the Act, was the National Bureau for Standards.
[255] 18 U.S.C §1030.

Section Highlights: *Summary of Private Sector Privacy Laws*

There are numerous privacy laws governing the private sector. Nearly every such law was enacted to address the specific privacy concerns of the industry it targets. No single statute governs the entire private sector as a whole. The privacy laws examined in this section were chosen because of their impact on large industries – the healthcare, financial, and computer industries.

In addressing the privacy considerations of any particular industry, it is important to take into consideration all of the laws that govern such industry. Accordingly, if biometric recognition technology were to be used in a particular industry, it would be wise to first find out what privacy laws exist that govern such industry to ensure that any proposed use would be in compliance with all such laws.

"Reputation, reputation, reputation! Oh, I have lost my reputation! I have lost the immortal part of myself, and what remains is bestial."

William Shakespeare, *Othello. Act ii. Sc. 3.*

V. COMMON LAW TORT PRIVACY RIGHTS

This section briefly examines the privacy rights recognized in tort law. Tort law provides a means for an individual (or entity) to bring a claim for damages against another individual or entity and collect damages (i.e. compensatory and, in some cases, punitive damages). Because tort law is a matter left to the courts of each state, application of such laws varies greatly. A full analysis of such torts is well beyond the scope of this report. However, it is important to understand their existence. If, for example, a person's personal information were improperly disseminated, whether or not in violation of an existing law, such person could bring an action seeking damages against the individual, entity, or government agency responsible for such dissemination. Below is a brief description of each of the four recognized areas of common law tort privacy rights.

There are four general privacy torts recognized by courts and discussed in Section 652 of the Second Restatement of Torts: (1) Public Dissemination of Private Information; (2) Intrusion upon Seclusion; (3) Appropriation of Name or Likeness; and (4) Publicly Placing a Person in a False Light.[256]

Public dissemination of private information involves publicly disclosing someone's private (non-public) personal information without consent or authorization,

[256] TURKINGTON & ALLEN, *supra* note 19, at 537.

which disclosure would be offensive or embarrassing to a person of ordinary sensibilities. The dissemination of information contained in a public record, however, is not an actionable offense because the information is already rightfully in the public domain (e.g. a criminal or court record). Often claims on this basis of privacy violation are brought against the media, which asserts the First Amendment as its defense. Of the four recognized privacy torts, this is the one that would be most applicable to biometrics since biometrics is arguably non-public information.

Intrusion upon seclusion relates to interfering with a person's right to secrecy in his affairs and in his person. Examples of this tort are entering into a person's home without his permission, rummaging through someone's purse, reading someone's diary or mail, or peering into someone's home or other secluded spaces, such as a dressing room, a public bathroom, or a locker room ("Peeping Tom").

Appropriation of name or likeness involves the use of someone else's name or likeness for one's own personal gain or benefit without such person's consent or other authorization. The theory behind this tort is the recognition that a person has the right to exclusively benefit from his or her own name and being. An example of an appropriation of name and likeness would be a company putting a celebrity's name and photograph on an advertisement for the company's product without such celebrity's consent.

Finally, publicly placing someone in a false light involves intentionally or recklessly disseminating to the public information about a person that is both false and would be considered highly offensive to a reasonable person. This invasion of privacy tort is similar and related to the torts of defamation, libel, and slander, and often a claim of one or more of these latter torts accompanies a false light claim.

Section Highlights: ***Summary of Common Law Tort Privacy Rights***

The significance of the existence of common law tort privacy rights is the fact that it provides a means for significant financial redress. Even though a law has not necessarily been broken, an individual may have been harmed is seeking redress for that harm.

Accordingly, any agency, such as NBSP, that publicly disseminates private information (e.g. biometric information) without authorization or consent, could be subject to a civil tort claim for damages even if no law has been broken.

"This 'telephone' has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us."

Western Union Internal Memo, 1876

VI. CONCLUSION: IMPACT OF UNITED STATES PRIVACY LAWS ON THE USE OF BIOMETRIC RECOGNITION TECHNOLOGY

Biometric recognition technology has awesome potential to defend the United States and its citizens from terrorists, criminals, identity thieves, computer hackers, and other villains. Knowledge is power, and by being able to positively identify humans through unalterable physiological information, biometrics will be able to tap into this power like never before. As this technology readies itself to soar, it must wait for the slow and deliberate legal machinery and societal acceptance to catch up.

There is nothing about biometric recognition technology itself that makes its use unlawful. It is the application of such technology that could be subject to legal scrutiny and could ultimately be found to be unconstitutional or otherwise unlawful. While no legal issues exist with respect to the voluntary use of biometrics for verification purposes, there are issues that need to be understood with respect to the use of biometrics for identification purposes. Additionally, social resistance to biometric recognition technology must be confronted and addressed.

It is important to distinguish between biometric recognition technology being used merely to verify a person is who he states to be and biometric recognition technology being used to solve crimes. Under the current state and structure of United States law, biometrics can legally be used to verify people. As long as biometrics obtained for verification purposes (or even for identification purposes) are used only for such purposes and not for other purposes, such as a criminal investigation, such use, while it may be subject to legal and non-legal challenges from groups such as the ACLU, should ultimately pass legal muster.

Nevertheless, there is resistance to biometric recognition technology and, in particular, to using biometrics for such things as travel (e.g. requiring biometrics to be embedded in passports), entitlement programs (to prevent fraud and double dipping in government benefits), and national identification cards. Any use of biometrics that involves a databank that can be accessed by anyone other than the individual whose biometric templates are embedded in such databank will require a balancing of public interest against privacy and civil liberties. If biometric data and other information contained in a "one to many" databank can be properly safeguarded (and, to the extent possible, made anonymous) and the public could be assured that the data would not be used for any other purpose and that there would be serious repercussions for violators, this would help tip the scales in favor of the government's use of biometric recognition technology for any legitimate purpose.

One of the social obstacles is that fingerprints, by far the most utilized and understood biometric, have been historically used in criminal investigations. This is not by accident. Fingerprints can be left behind at a crime scene.[257] Therefore, fingerprints, more than any other biometric, have the capacity to be used to not only identify a person or verify that a person is who he says he is, but can also be used as evidence to associate an individual with a crime. This potential may be an argument for the use of other types of biometric identifiers, such as irises or retinas, which are not "left behind" and currently cannot be used in criminal investigations the way fingerprints can. This is not to suggest that irises and other biometrics could not still be used for criminal investigations and that using irises instead of fingerprints would obviate the need for safeguards. In fact, many forms of biometric recognition technology, including iris and facial recognition, raise concerns about covert identification, such as the covert use of facial recognition at the 2001 Super Bowl. However, their use as evidence of a crime is much more limited and heads off the argument that the data could be misused to associate an individual with a crime.

The right of the public (e.g. the police) to positively know who a person is versus the right of the individual to remain anonymous is at the center of the discussion of biometrics. This issue was at the core of the recently decided Supreme Court case of

[257] Another biometric that is often left at a crime scene is a DNA sample of an individual. However, because the time required to process a DNA sample takes days, as opposed to seconds, it is not conducive for the biometric recognition functions under consideration covered by this report. However, someday there will likely be technology that can process DNA samples in seconds.

Hiibel v Sixth Judicial District Court of Nevada, Humboldt County, et. al., discussed earlier in this report at Section II.A.2.a. The premise of *Hiibel* is that the officer suspected Hiibel might have committed a crime (i.e. battery). The law makes a critical distinction between people suspected of committing a crime and those who are not criminal suspects. The right to remain anonymous is much stronger for someone not suspected of committing a crime. In other words, there is a difference between a police officer randomly walking up to a person and asking for identification and a police officer asking a particular person for identification when that officer reasonably suspects that person may have committed a crime.

Now that the *Hiibel* Court has determined that an individual *may* be required by state law to identify himself to a police officer, the next issue to consider is: under what circumstances must someone comply with such a request? In other words, where is the line between having and not having reasonable suspicion? If instead of the report describing the suspect in the *Hiibel* case as a man hitting a woman in a truck on a particular country road, suppose the caller had described him as a black man hitting a woman while they were walking down a busy city street? Would it be permissible for the police to stop every black man within a certain radius walking with a female companion and ask for identification?

Clearly, it is not only the *requirement* of a national identification card, but also under what *circumstances* the procurement of such an identification card may be required, that will be subject to constitutional scrutiny. However, this issue has little to do with biometrics; biometrics are merely another and generally superior means of identifying someone. If requiring a national ID card is found to be constitutional, then requiring a national ID card that includes biometrics would likely be found to be constitutional and in compliance with all applicable federal laws.

The answer to the question of when and under what circumstances a national ID card (whether or not it contains biometrics) may be required to be produced is far more complicated and will likely depend on a determination of what situations reach the level of an important public interest (i.e. a "special need") that outweighs the individual's right to privacy (i.e. the right to remain anonymous). In the public sector, can a biometrically embedded national ID card be required for travel? for obtaining a government benefit? for purchasing a gun? In the private sector, can a biometrically embedded national ID card be required for opening a bank account? for using a credit card? for renting a car? Again, these questions do not hinge on the legality of biometric identification but whether and when it is legal to demand proof of identification, especially by government authorities. If mandatory proof of identification is found to be legal due to an important public interest, then biometrics can legally be used as part of that identification system. What situations might rise to the level of an important public interest to justify mandatory proof of identification is beyond the scope of this paper and, in any event, not for NBSP to determine.

If it is legal to require identification of an individual in a given circumstance, then there is nothing illegal about the use of *biometrics* as a means of identification. In all likelihood, existing law will not be the biggest obstacle biometric recognition technology faces. The greatest challenge will likely lie in public acceptance of the technology. Public resistance, whether or not based on misinformation or irrational fears, could lead to new laws restricting the use of biometrics beyond the confines of current law. These concerns have already led to a push for new privacy legislation to control biometric use. Vermont and New Hampshire recently passed laws prohibiting the use of biometrics on most driver licenses.[258] Organizations like the American Civil Liberties Union, Privacy International, and the Electronic Frontier Foundation are calling for biometric controls.[259] Even pro-biometric groups agree that controls in the collection and methods of using biometrics are needed. The International Biometric Industry Association advocates that clear legal standards be developed.[260] Certainly, the emergence of biometric recognition technology and its increasing use following September 11th has spurred much debate. This has led to the creation of new bills to address the use of biometrics. Appendix A to this report provides a list of pending legislation that, if enacted, could impact the biometric industry and privacy in general.

One of the fears with any databank is that it will be misused. The purpose of a national identification card may be to positively verify a person's identity and protect the public by avoiding future terrorist attacks. However, if such a card is used to not only verify identity, but to identify a person by comparing his biometrics to the biometrics contained in a databank of biometric templates, the privacy concerns are heightened. The very existence of a central databank concerns people who recall times when the government used databanks of information on people for purposes far beyond their original intent. Examples of reported misuses include the use of confidential information from the Census Bureau during World War II to locate and intern Japanese-Americans and the use of confidential information from the National Crime Information Center to monitor people opposed to the Vietnam War.[261]

Both of these reported misuses of information contained in confidential databanks took place when the country was at war. Accordingly, during today's time of instability when fears of future terrorist attacks abound, it is not unreasonable to anticipate that some people will be concerned that in the future, biometric data gathered to screen for terrorists could be used for other purposes or associated with other data about the individual. For example, there is concern that biometric data could be used for racial profiling or detecting past drug use,[262] or that insurance companies could use biometric data to gauge the health of people before deciding whether to provide them with

[258] H. 199, 2003-2004 Leg., (Vt. 2004); H.B. 1243, 2004 Leg. 158th Sess. (N.H. 2004).

[259] Privacy International's website is at http://www.PrivacyInternational.Org. The Electronic Frontier Foundation's website is at http://www.EFF.Org.

[260] The International Biometric Industry Association announced its Privacy Principles on March 24th, 1999 and they can be viewed at its website, *available at* http://www.IBIA.Org.

[261] Neda Matar, *Are You Ready For A National ID Card? Perhaps We Don't Have To Chose Between Fear of Terrorism and Need For Privacy*¸ 17 EMORY INT'L L. REV. 287, 310 (Spring 2003).

[262] Facial structure can be used to identify race. Hair and sweat samples can be used to determine drug use. Beverly Potter, *Drug Testing at Work: A Guide for Employers*, 115-119 (1998).

coverage. As was previously mentioned in the discussion of HIPAA at Section IV.A, the government is currently seeking to use hospitals' medical information to search for women who had abortions. While this use may be justified and legal, it is nonetheless alarming to many people. It is these potential uses and misuses, whether or not based in the realities of biometric recognition technology's capabilities, which have some people concerned. To alleviate these concerns, appropriate safeguards need to be implemented and enforced and the public needs to be educated about the benefits, the capabilities, and the limitations of biometric recognition technology.

One of the biggest fears about biometrics is that personal information collected in connection with or for purposes of biometric identification will be used for reasons other than the original intent. This concern is often referred to as "function creep" or "mission creep." The classic example of function creep is Social Security numbers, which were created for the sole purpose of administrating Social Security benefits but are now used as the de facto numeric identities for Americans. Some people fear that function creep in biometric use could lead to an omniscient government with unprecedented and unlimited surveillance powers.

These anxieties would probably be significantly allayed if Americans had more trust in their government. Unfortunately the three government agencies that would likely use biometrics to protect against terrorism are reportedly also the least trusted by Americans. In a recent poll that asked people their opinion on which government organizations are committed to protecting their personal information, the Department of Justice was the least trusted, followed by the Department of Homeland Security, and the Central Intelligence Agency.[263]

Although a distrust of government may cause some resistance to biometric use, that same distrust could also be used to promote biometric use. In 1995 more than 500 Internal Revenue Service agents were caught illegally looking at thousands of tax records. Although the IRS instituted new privacy protection measures in response to the violations, these measures proved ineffective as hundreds of agents were caught doing the same thing in 1997.[264] If the IRS were to implement a security system that required employees to use biometric verification to gain access to taxpayer records, it would be able to determine which employees accessed which files, and would presumably deter future violations. It is these types of implementations of biometric recognition technology that can be used to enhance privacy and could ultimately lead to broader public acceptance (and even embracement) of biometric recognition technology and laws supporting its use.

---

[263] *The Privacy Trust Survey*, Ponemon Institute and Carnegie Mellon University's CIO Institute report (January 2004). Interestingly, according to that survey report, the most trusted governmental organization is the U.S. Postal Service.

[264] Solveig Singleton, *Privacy Issues In Federal Systems: A Constitutional Perspective*, National Institute of Standards and Technology Computer System Security and Privacy Advisory Board Meeting (17 March 1999).

Another reason for some of the public resistance to biometric recognition technology is that hanging over much of the privacy debate is the fear that it could open the door to an Orwellian "Big Brother" society where governments and private corporations can track our every move by the fingerprints and odors we leave behind. Yet another concern is that biometrics is the "Mark of the Beast" warned about in the New Testament of the Bible.[265] While these two fears may be alarmist, they combine with more rational concerns about the impact that uses and abuses of new technology may have on privacy and civil liberties to generate public fear and resistance to biometric initiatives.

The government is not the only source of public distrust. Over the past decade, there has been a sharp decline in the public's trust in the private industry to protect consumers against identity theft.[266]

Public resistance and mistrust has already impacted the development and implementation of several government security programs and has lead to the enactment of laws restricting the use of biometric recognition technology, such as the anti-biometric driver's license laws in Vermont and New Hampshire. Funding for the Total Information Awareness Program, which was designed to create a centralized national database of information on people to detect potential terrorist activity through intelligence analysis, was frozen in 2003 in response to public outcry over privacy concerns.[267] Similarly, interest in the Matrix (a program designed by a private company to cull publicly-available information into a single database to help law enforcement locate criminals and terrorists) has been waning as more and more states are dropping out.[268]

As this report is being prepared, the Computer-Assisted Passenger Prescreening System program known as CAPPS II[269] continues to be heavily scrutinized, and several organizations, including the ACLU and the Electronic Frontier Foundation, have been campaigning to stop CAPPS II from being implemented because of privacy and civil liberties concerns.[270] The Air Transport Association has expressed its support for the

---

[265] This "Mark of the Beast" fear should not be underestimated. Pat Robertson subscribes to this concern, and the Christian Coalition, the organization Robertson co-founded, helped defeat a plan in Alabama to make fingerprinting a mandatory part of its driver's license issuance system in 1997. JOHN D. WOODWARD, JR. ET AL., *supra* note 242, at 28.

[266] New Consumer Segmentation and Activism Survey (Harris Interactive), commissioned by Privacy & American Business, sponsored by Microsoft. This survey polled people in 1995, 2000, 2003, and 2004 regarding concerns over identity theft and the ability of private industries to protect against it.

[267] John Schwartz, *Privacy Fears Erode Support for a Network to Fight Crime*, N.Y. TIMES, March 15, 2004.

[268] *Id*. The number of states interested in participating in the program has dropped from 16 to 5 over the past year. William Welsh, *Feds Offer to Mend Matrix*, WASHINGTON TECHNOLOGY, Vol. 19 No. 4, May 24, 2004.

[269] CAPPS II is discussed *supra* at Section III.C.

[270] The passenger-screening program would check information such as a name, address, and birth date against commercial and government databases. Each passenger would be given one of three color-coded ratings. Suspected terrorists and violent criminals would be designated as red and forbidden to fly. Passengers who raise questions would be classified as yellow and would receive extra security screening. The vast majority would be designated green and allowed through routine screening.

concept of CAPPS II, provided the government follows seven "privacy principles."[271] These principles would require that only information pertaining to aviation security is obtained, passengers would be fully informed about the information collection process and would be allowed to access their individual information and correct any errors, and the information would be secure and would be disposed of as soon as travel is completed.[272] These principles, or methods of control, are typical of those being promoted by the biometric industry for all applications and are supported by NBSP.

Of the nineteen September 11th hijackers, ten were flagged by the CAPPS systems (the predecessor system to CAPPS II).[273] At that time, the security measures that were in place only required that a flagged passenger's luggage be screened for explosives and held off the plane until it was confirmed that the passenger had boarded. As stated in the 9/11 Commission Report, CAPPS was "designed to identify passengers whose profile suggested they might pose more than a minimal risk to aircraft," but because of potential discrimination concerns and the impact on screening time, selected passengers "were no longer required to undergo extraordinary screening of their carry-on baggage as had been the case before the system was computerized in 1997."[274]

The 9/11 Commission Report concludes that in order to secure the United States against future terrorist attacks, we need to implement a comprehensive screening system that includes biometrics.[275] More than 330 million non-citizens cross into the United States of America each year, passing through countless security checkpoints, from seeking passports and visas, to stopping at ticket counters and inspection points.[276] Each of these checkpoints is a chance to establish identity and verify that people are who they say they are.[277] Biometric verification can be used as part of a comprehensive system to verify identity and prevent identity fraud.

The 9/11 Commission points out that travel documents and traveling clandestinely are as important to terrorists as weapons. Altered and counterfeited travel documents are used to hide identity and circumvent security.[278] The Commission has recommended that a comprehensive biometric screening system be designed and integrated into a larger network of screening points, which includes transportation and vital facilities.[279] The Commission notes that a screening system will look for identifiable and particular suspects or indicators of risk.[280] The Commission recommends that Americans, Mexicans, and Canadians should all have to carry biometric passports and that Americans

[271] *Congress Seeks Answers on Screening Program*, THE ASSOCIATED PRESS, March 17, 2004.
[272] *Seven Passenger Privacy Principals from the Airline*, www.CNN.com (March 17, 2004).
[273] THE 9/11 COMMISSION REPORT at 1-4 n.2 to Chapter 1.
[274] *Id*. at 84.
[275] *Id*. at 385.
[276] *Id*. at 383.
[277] *Id*. at 385.
[278] THE 9/11 COMMISSION REPORT at 384.
[279] *Id*. at 387.
[280] *Id*.

not be exempt from carrying a biometric passport when returning from Canada, Mexico, or the Caribbean.[281]

The 9/11 Commission noted the importance of privacy and civil liberties, and the need for balance between protecting the homeland and protecting personal and civil liberties.[282] The Commission admits that such a balance is "no easy task", and makes the following three recommendations to facilitate this delicate balancing: (1) the President should determine the guidelines for agency information sharing while safeguarding the privacy of individuals; (2) the executive branch of government should have the burden of proof to justify the need for a specific government power under the Patriot Act to demonstrate that it materially enhances security and that there is adequate supervision of the government's use of it to ensure protection of civil liberties; and (3) that there should be an executive branch authority to monitor the government to make sure they are committed to defending civil liberties.[283] Many countries (including Canada, Australia, and Germany) have a federal privacy commissioner to oversee that the country's privacy laws are being upheld and that individual privacy rights are being protected.

The 9/11 Commission has noted that successfully falsifying identity is a key element to the execution of a terrorist plan.[284] Biometric identifiers make falsifying identification far more difficult.[285] The Commission has, in essence, recommended the use of both a one-to-one verification system to verify that people are who they claim to be, as well as a one-to-many identification system to check available information to determine whether someone is a terrorist.[286] The Commission recommends biometric passports and asserts that linking biometric passports to sound data systems is essential to detecting terrorists and deterring future attacks.[287]

Public perception and sentiment play as much of a role in determining the future of biometric recognition technology in the United States as does federal privacy law. Accordingly, an important step to paving the way for government use of biometrics is educating the public about biometric recognition technology, perhaps in the form of a program aimed at gaining public acceptance through education and demystification. The public needs to understand that biometrics can be used to protect not only our national security, but our privacy as well. The public also needs to be assured that proper and effective safeguards, perhaps in the form of new legislation, will be in place to shield against misuses of biometric recognition technology with civil and criminal sanctions for violators. The public needs to be satisfied that the use of biometric recognition technology will not lead to a "Big Brother" society.

---

[281] *Id.* at 388.
[282] *Id*. at 394.
[283] THE 9/11 COMMISSION REPORT at 394-395.
[284] *Id.* at 388.
[285] *Id.*
[286] *Id.* at 390.
[287] *Id.* at 389.

Another important step towards implementation of a comprehensive screening system that includes biometrics is consideration for the laws and public sentiments of other countries. The 9/11 Commission recommends that the United States work with other countries to arrive at national standards and ensure effective security regimes.[288] It is critical to the success of biometric recognition technology in United States national security that the international community act together in seeking solutions that will respect individual privacy on a global scale.

As previously stated, if there is no databank and biometrics are used simply to verify an individual's identity in situations where verification of identity is permissible, there are no issues under current United States federal law. Further, biometrics may be used to identify a person (i.e. using a central databank) in circumstances where the public has a justifiable need to know who a person is and whether that person poses a threat. If proper safeguards are both implemented and are strictly enforced to protect biometric information contained in databanks from improper disclosures and uses, there should be no privacy issues. Covert uses of biometrics for identification raise privacy concerns to an even greater level and, from a constitutional standpoint, would likely require a profound public need. National security is arguably such a profound public need.

As a general rule, privacy issues are more likely to arise when identification is covert or when the biometric is attached to highly sensitive information, such as in the case of identifying people through DNA or linking a biometric to criminal, medical, or financial information. However, most of the activities where biometrics are expected to be used for national security are innocuous and would be done with the full knowledge and consent of the individual. For example, the identification of an airline passenger is hardly considered highly sensitive information, especially considering that passengers are already required to identify themselves to airport personnel, and considering further that potentially hundreds of other lives could be at stake. Air travel safety is clearly an important public issue. Although under certain circumstances it is possible that such travel information when available to others could compromise someone's need to travel secretly, such isolated and remote circumstances cannot justify compromising national security and can be dealt with by the individual.

Biometrics merely enhance the ability to positively verify a person's identity and minimize the human error factor in trying to match a person to his identifying information. If biometric templates are embedded in passports, they can be used to verify passenger identity and, under permitted circumstances, to check against other information in a databank. No databank is necessary for its use as a means of verifying that the person holding the passport matches the person identified in the passport when the holder's biometric template is securely embedded in the passport. If the biometrics of the holder does not match the biometric information embedded in the passport, the person will not be granted access to the airplane, although he may be arrested for presenting false documentation. This is no different than a person trying to travel using someone else's passport. The use of a biometric identifier does not present any new legal issues.

[288] THE 9/11 COMMISSION REPORT at 389.

On the other hand, if the biometric information is contained in a central databank so that the biometrics of a passenger can be compared to other entries in that databank, privacy concerns arise. If, however, the passenger inserts a user name to retrieve just his biometric template from the central databank of templates, the general concerns regarding a central databank are arguably diminished or eliminated because the system only operates for this purpose (verification mode, not identification mode) and the biometric cannot be otherwise traced to the individual. Thus, the mere fact that there is a databank does not necessarily mean that there will be privacy concerns. If the databank is being used to merely confirm that the person is who he is purporting to be and is not carrying a falsified passport, and such databank is safeguarded, such use is really just an expanded form of verification and should be permissible.

This in no way means that biometric passports, and biometric recognition technology in general, cannot be legally used for identification purposes, as the 9/11 Commission recommends. However, such use does raise privacy issues and requires a legitimate and important purpose. We are merely emphasizing that the use of biometric passports for verification raises no legal issues and does not require any justification.

The first question raised in any analysis of whether a proposed use of biometric recognition technology is constitutional is: what is privacy and how far does it extend? For purposes of this report, we can assume that, using the broadest interpretation of the right to privacy, anything *about* a person may be considered private such that its disclosure would be a violation of that person's privacy. In the *Hiibel* decision, United States Supreme Court Justice Breyer described the disclosure of a person's name as a violation of one's privacy, albeit a minor one. Others have described privacy as the right to be let alone or to remain anonymous. Disclosure of one's name, while it eliminates anonymity and thus impinges upon privacy, might be justified depending upon the circumstances under which it is required to be disclosed, for example, as a condition to boarding a plane.

Biometrics (like a name) are another identifier of an individual. However, unlike a person's name, having one's biometric data could allow the holder of the biometric to identify that individual without that individual's knowledge (as was done at the 2001 Super Bowl). Additionally, biometric information contained in a database could be linked to other information about the individual and/or could be used for purposes other than the original intent. It is these potential uses (or misuses) of biometric recognition technology that raise privacy concerns.

Biometrics is a means of identification. It is the securing of an individual's identification that presents privacy issues. Once it has been determined that a person's identification may be obtained, biometrics is a legal method of identification. The collection of biometrics and maintenance in a database creates a privacy concern if the database is misused or not properly safeguarded. This is because biometrics alone can be used to identify an individual in a situation where it might be either unauthorized or unconstitutional to identify that person. Thus, once identification of the person is found to

be permissible, then the use of biometrics as a means of identification or verification creates no more of a privacy issue than any other available method of identification.

Anyone who uses a credit card leaves a continuous trail of their travels, tastes, and habits through their purchases without objection or grave concern for their privacy. This "Big Brother"-like phenomenon has created far less stir than the advent of biometrics. This is probably at least partly due to the convenience enjoyed by using credit cards and partly due to the familiarity that has come with its widespread use. Perhaps more widespread use of biometrics will eventually lead to greater public acceptance. The isolated uses of biometrics for air travel and other national security purposes is far less revealing of one's personal life than daily credit card transactions. As the 9/11 Commission points out, while it is nearly impossible to hide one's debt by acquiring a credit card using a slightly different name, even today, in our post-9/11 world, "a terrorist can defeat the link to electronic records by tossing away an old passport and slightly altering the name in a new one."[289] Most people would undoubtedly agree that national security is far more important than the convenience of using a credit card.

Nearly every technological innovation has been met with skepticism, cynicism, and very often fear. If the nay-sayers had been heeded, there would be no personal computers, airplanes, automobiles, televisions, or telephones. Virtually every technological innovation carries with it certain drawbacks, burdens, and risks. One might argue that the automobile was a "bad" invention because of the thousands of lives lost each year to automobile accidents and the increased dependency on oil. Yet because of the immense benefits of the automobile, society seeks ways to mitigate those problems rather than do away with cars. In this same vein, biometric recognition technology should not be stopped merely because of the risks to people's privacy due to poorly safeguarded systems and potential misuses. As the 9/11 Commission asserts, "funding and completing a biometric-based entry-exit system is an essential investment in our national security."[290] However, people's concerns need to be taken seriously and steps need to be taken to alleviate these concerns and mitigate inherent risks.

From a practical standpoint, public opinion or confidence in any system of identification is critically important because the public's view can make or break a system. Therefore, it is essential that issues of individual privacy be taken into account in any system that is employed regardless of whether the law requires it. The information must be made anonymous to the greatest extent possible. Databanks should be used only when necessary and only relevant information should be kept in any databank and disposed when it is no longer needed. Individuals should be fully informed about the collection process, allowed access to their information, and have the ability to correct any errors. There must be oversight and strict controls and procedures in place governing how the information is used and shared. Except for very special situations, biometric recognition technology should only be used for verification purposes; identification uses, particularly covert uses, must be used only under very limited and highly controlled circumstances involving public safety. Finally, there must oversight and there must be

[289] *Id.*
[290] *Id.*

consequences for violations; any abuses, misuses, or violations of the controls or procedures must be adequately redressed (e.g. fines, termination of employment, and in severe situations, imprisonment) to help assure public confidence. Every effort must be made to eliminate the "slippery slope" argument against biometric recognition systems.

In sum, the recommended principles to be followed in any use of biometric recognition technology are as follows:

- Only necessary and relevant information is maintained
- Information is anonymous to fullest extent possible
- Individual is informed and has access to information and ability to correct
- Proper controls, procedures, and oversights are in place
- Adequate consequences and redress for violations of controls and procedures are enforced
- Used for verification purposes with individual's knowledge
- Identification and/or covert use requires stricter controls and limited use and circumstances

Biometric recognition technology is not a panacea. It will not, by itself, solve our nation's problems or thwart all future terrorist attacks. However, it should, as the 9/11 Commission has recommended, be implemented as part of a comprehensive national security system. Identification of a person through biometrics and matching identity to information in a central database can help identify terrorists and prevent future attacks. Such use arguably rises to the level of an important government and societal interest. Verification of a person's identity through biometrics provides the government with no more information about a person than it had before. Biometric recognition technology helps thwart falsifying identification. The public needs to understand and accept these facts. The public also needs to be assured that biometric use will not be abused, that personal information will be safeguarded, and that privacy and civil liberties will not be jeopardized.

GLOSSARY OF TERMS

Biometrics. The terms "Biometrics" and "Biometry" have been used since early in the 20th century to refer to the field of development of statistical and mathematical methods applicable to data analysis problems in the biological sciences. More recently, and as used in this report, biometrics refers to the automated systems developed for human recognition based on the measured physiological or behavioral characteristics of an individual. Examples of biometrics include fingerprints, iris recognition, facial recognition, hand geometry, gait, and voice.

Biometric Recognition. As used in this report, the term biometric recognition refers to the overall function of biometrics as a system designed to recognize a person based on their physiological or behavioral characteristics.

Biometric Identification. As used in this report, the term biometric identification refers to a type of biometric recognition system used to positively identify one person by matching the presented biometric with a stored template by automatic and exhaustive search of a database containing the biometric templates of many persons (one to many).

Biometric Verification. As used in this report, the term biometric verification refers to a type of biometric recognition system used to verify a person's identity by matching the person's presented biometric to a stored template of that same person which may be automatic if only one template is stored or recalled from a database by another device (e.g. a number) assigned to that person (one to one).

BIBLIOGRAPHY

Books

Bacon, Francis. Meditationes Sacrae De Haeresibus (1597)

Legomsky, Stephen H. Immigration and Refugee Law and Policy, 3rd Ed. 2002.

Orwell, George. 1984 (1949).

Turkington, Richard C. & Anita L. Allen. Privacy Law: Cases and Materials, 2nd Ed. 2002.

Turkington, Richard C. & Anita L. Allen. Privacy Law: Cases and Materials, Supp 2003.

Woodward, Jr., John D., et al. Army Biometric Applications: Identifying and Addressing Social Concerns 2001.

Woodward, Jr., John D., et al. Biometrics: Identity Assurance in the Information Age 2003.

Legal Journal Articles

Matar, Neda. Are You Ready For A National ID Card? Perhaps We Don't Have To Chose Between Fear of Terrorism and Need For Privacy, 17 Emory Int'l L. Rev. 287 (Spring 2003).

Warren, Samuel D. & Louis D. Brandeis. The Right to Privacy, 4 Harv. L. Rev. 193 (1890).

Whitehead, John W. & Steven H. Aden. Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives, 51 Am. U.L. Rev. 1081 (2002).

Media Articles

"Congress Seeks Answers on Screening Program" Associated Press (March 17, 2004).

Foss, Brad. "Airline Admits Giving U.S. Passenger Data" Associated Press (April 9, 2004).

Gamboa, Suzanne, "Key Legislator, White House at Odds on a Passport Delay" (May 22, 2004).

Kristof, Nicolas D. "May I See Your ID?" N.Y. Times, March 17, 2004 (Op-Ed).

Lichtblau, Eric. "New York Hospital Is Ordered to Release Abortion Records" N.Y. Times (March 20, 2004).

Miller, Leslie. "U.S., EU Sign Deal on Airline-passenger Data" Philadelphia Inquirer, A2 (May 29, 2004).

Saffire, William. "Privacy in Retreat" N.Y. Times, Op-Ed (March 10, 2004).

Schwartz, John. "Privacy Fears Erode Support for a Network to Fight Crime" N.Y. Times (March 15, 2004).

Singel, Ryan. "CAPPS II Stands Alone, Feds Say" Wired Magazine (Jan. 13, 2004), http://www.wired.com/news/privacy/0,1848,61891,00.html.

Singel, Ryan. "EU Travel Privacy Battle Heats Up" Wired News (Dec. 22, 2003), http://www.wired.com/news/politics/0,1283,61680,00.html.

"US Government to Start Issuing Biometric Passports in October 2004" eGovernment News (March 10, 2004).

Welsh, William. "Feds Offer to Mend Matrix" Washington Technology, Vol. 19 No. 4 (May 24, 2004).

Cases

Baker v. Dep't of the Navy, 814 F.2d 1381 (9th Cir. 1987).
Bechhoefer v. United States Dep't of Justice Drug Enforcement Admin., 209 F.3d 57 (2d Cir. 2000).
Beck v. State of Ohio, 379 U.S. 89 (1964)).
Bell v. Wolfish, 441 U.S. 520 (1979).
Boyd v. Sec'y of the Navy, 709 F.2d 684(11th Cir. 1983).
Berkemer v. McCarty, 468 U.S. 420 (1984)
California v. Ciraolo, 476 U.S. 207 (1986).
California v. Hodari, 499 U.S. 621 (1991).
Carey v. Population Services International, 431 U.S. 678 (1977).
Chae Chan Ping v. U.S., 130 U.S. 581, 9 S.Ct. 623, 32 L.Ed. 1068 (1889).
Clarkson v. IRS, 678 F.2d 1368(11th Cir. 1982).
Crumpton v. Stone, 59 F.3d 1400 (D.C. Cir. 1995).
Crumpton v. United States, 843 F. Supp. 751(D.D.C. 1994).
Cruzan v. Director, Missouri Department of Health, 497 U.S. 261 (1990).
Delaware v. Prouse, 440 U.S. 648 (1979).Department of Justice v. Reporters Committee For Freedom of Press, 489 U.S. 749 (1989).
Doe v. Chao, 72 USLW 4178, 124 S.Ct. 1204 (2004).

Doe v. Herman, 1999 U.S. Dist. LEXIS 17302 (U.S. Dist., 1999).
Florida v. Royer, 460 U.S. 491 (1983)
Green v. Berge, 2004 U.S. App. LEXIS 236 (U.S. App., 2004).
Griffin v. Wisconsin, 483 U.S. 868(1987)).
Griswold v. Connecticut, 381 U.S. 479 (1965).
Groceman v. United States Department of Justice, 354 F.3d 411 (2004).
Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County, et. al., No. 03-5554, 542 U.S. __(2004), *aff'd* 59 P.3d 1201 (Nev.2002).
Illinois v. Wardlow, 528 U.S. 119(2000).
Ingerman v. IRS, No. 89-5396,(D.N.J. Apr. 3, 1991); 953 F.2d 1380 (3d Cir. 1992).
In re Crawford, 194 F.3d 954 (9th Cir. 1999).
In re D.L.C., 2003 Tex. App. LEXIS 10619 (Tex. App., 2003).
Jones v. Murray, 962 F.2d 302(4th Cir. 1992).
Katz v. United States, 389 U.S. 347 (1967).
Kyllo v. United States, 533 U.S. 27 (2001).
Maydak v. U.S., 363 F.3d 512 (D.C. Cir. 2004).
Murphy v. NSA, 2 Gov't Disclosure Serv. (P-H) ¶ 81,389 (D.D.C. Sept. 29, 1981).
NAACP v. State of Alabama, 357 U.S. 449(1958).
In the Matter of Northwest Airlines, Inc., Docket OST-04-16939, Department of Transportation (February 27, 2004).
Pierce v. Society of Sisters, 268 U.S. 510 (1925).
Ponte v. Real, 471 U.S. 491(1985).
Quinn v. Stone, 978 F.2d 126 (3d Cir. 1992).
Roe v. Wade, 410 U.S. 113 (1973).
Schmerber v California, 384 U.S. 757 (1966).
Shannon v. Gen. Elec. Co., 812 F. Supp. 308(N.D.N.Y. 1993).
Skinner v. Railway Labor Executives' Assn., 489 U.S. 602 (1989).
Smith v. Maryland, 442 U.S. 735 (1979).
State v. Steele, 802 N.E.2d 1127, 155 Ohio App. 3d 659(Ohio App., 2003).
Sullivan v. United States Postal Serv., 944 F. Supp. 191(1996).
Tehan v. United States ex rel. Shott, 382 U.S. 406(1966).
Terry v. Ohio, 392 U.S. 1 (1968).
Tobey v. N.L.R.B., 40 F. 3d 469(D.C. Cir. 1994).
Union Pac. R. Co. v. Botsford, 141 U.S. 250(1891)).
U.S. Dept. of Defense v. Federal Labor Relations Authority, 510 U.S. 487 (1994).
United States v. Kincade, 345 F.3d 1095 (9th Cir. 2003).
United States v. Mendenhall, 466 U.S. 544, 556 (1980).
United States v. Plotts, 347 F.3d 873(10th Cir. 2003).
United States v. Stegman, 295 F. Supp. 2d 542(U.S. Dist., 2003).
United States v. Truong Dinh Hing, 629 F. 2d 908 (4th cir. 1980).
United States v. United States District Court, 407 U.S. 297 (1972).
Unt v. Aerospace Corp., 765 F.2d 1440(9th Cir. 1985).
Vernonia School Dist., 47J v. Acton, 515 U.S. 646 (1995).
Washington v. Glucksberg, 521 U.S. 702 (1997).
Whalen v. Roe, 429 U.S. 589 (1977).
Williams v. VA, 104 F.3d 670(4th Cir. 1997).

Wilson v. Pennsylvania State Police, CA 94-6547, 1999 U.S. Dist. LEXIS 3165, ___ (E.D. Pa. March 11).
Winston v. Lee, 470 U.S. 753 (1985).
Zablocki v. Redhail, 434 U.S. 374 (1978).

Statutes and Executive Office Material

The Aviation and Transportation Security Act, 49 U.S.C. 44909.

The Bank Secrecy Act, 12 U.S.C.A. § 1951 et seq., Public Law 91-508, Title I.

The Computer Fraud and Abuse Act, 18 U.S.C §1030 et seq.

The Computer Security Act of 1987, 40 U.S.C. §759 et seq.

Department of Health and Human Services Rules, 45 C.F.R. pts 160 & 164, 65 Fed. Reg. 82462-01 (December 28, 2000).

The Electronic Fund Transfer Act, 15 U.S.C. §1693-1693r.
United Kingdom's Human Rights Act of 1998.

Convention for the Protection of Human Rights and Fundamental Freedoms (effective Sep. 3, 1953) 213 U.N.T.S. 222 (modified Nov. 1, 1998).

Charter of Fundamental Rights of the European Union, O.J. C364/1 (2000).

Executive Order No. 12333, 46 Fed. Reg. 59941, 87 Stat. 555 (1981).

The Fair Credit Reporting Act, 15 U.S.C. §1681-1681t.

The Federal Wiretap Act 18 U.S.C.A. § 2510 et seq.

The Financial Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

The Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §1801 et seq.

The Freedom of Information Act, 5 U.S.C. §552 et seq.

The Privacy Act of 1974, 5 U.S.C. §552a et seq.

The Right to Financial Privacy Act of 1978, 12 U.S.C. 3401-3422.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (The USA Patriot Act), Pub. L. No. 107-56, 115 Stat 272 (2001).

US-VISIT Program, Increment 1 Privacy Impact Assessment Executive Summary (December 18, 2003) http://www.dhs.gov/interweb/assetlibrary/VISITPIAfinalexecsum3.pdf.

Miscellaneous

Article 29 Data Protection Working Party. "Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the [Passenger Name Record] PNR of Air Passengers to Be Transferred to the United States' Bureau of Customs and Border Protection (US CBP)" (January 29, 2004), EUROPA, The European Commission, Internal Market, Data Protection, http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2004/wpdocs04_en.htm#wp87.

Booz Allen Hamilton. Application of Executive Order 12333 to Human Subject Research and Testing: A "Quick Look" (October 2003).

Department of Homeland Security. "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program ("US-VISIT"); Biometric Requirements; Notice to Nonimmigrant Aliens Subject To Be Enrolled in the United States Visitor and Immigrant Status Indicator Technology System; Interim Final Rule and Notice" Federal Register, vol. 69, no. 2 (Jan 5, 2004), 8 CFR 214, 215, 235.

Electronic Privacy Information Center. "In the Matter of JetBlue Airways Corporation and Acxiom Corporation: Complaint and Request for injunction, investigation and for other relief",http://www.epic.org/privacy/airtravel/jetblue/ftccomplaint.html (last visited June 8, 2004).

Electronic Privacy Information Center. The USA Patriot Act Webpage, http://www.epic.org/privacy/terrorism/usapatriot/ (Last visited June 8, 2004)

WWW.EFF.ORG (Last visited June 8, 2004).

WWW.IBIA.ORG (Last visited June 8, 2004).

National Biometric Security Project. Biometrics for National Security (BiNS), *Technical Report* (January 30, 2004).

National Commission on Terrorist Attacks Upon the United States, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (2004).

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).

Office of Mgmt. & Budget, Circular A-110, "Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations" 64 Fed. Reg. 54,926 (Oct. 8, 1999).

OMB Guidelines, 52 Fed. Reg. 12990 (1987).

OMB Guidelines, 40 Fed. Reg. 56,741 (1975).

OMB Guidelines, 40 Fed. Reg. 28,948 (1975).

Potter, Beverly. Drug Testing at Work: A Guide for Employers (1998).

"Prisoners' Privacy Act Suit Challenges BOP Photo Program" Privacy Times, vol. 24 no. 9, (May 4, 2004).

"The Privacy Trust Survey" Ponemon Institute and Carnegie Mellon University's CIO Institute Report (January 2004).

WWW.PRIVACYINTERNATIONAL.ORG (Last visited June 8, 2004).

"Seven Passenger Privacy Principals from the Airline" www.cnn.com (March 17, 2004).

Singleton, Solveig. "Privacy Issues In Federal Systems: A Constitutional Perspective" National Institute of Standards and Technology Computer System Security and Privacy Advisory Board Meeting (17 March 1999).

United States Department of Justice, Overview of the Privacy Act of 1974 (May 2002), http://www.usdoj.gov/04foia/04 7 1.html.

Visa Waiver Program, U.S. Department of State: Bureau of Consular Affairs: Visa Services, http://travel.state.gov/vwp.html#7 (last visited May 27, 2004).

Random House Webster's Unabridged Dictionary (2d ed. 2001).

APPENDIX A

"Laws are like sausages. It's better not to see them being made."

Otto von Bismarck

PENDING LEGISLATION

The following pages contain a selection of pending bills and legislation that pertain to privacy and/or biometrics. The bills are presented in a chart that shows the name of the bill (if known), the bill number, its stated purpose, the name of the legislator sponsoring the bill, the legislative committees (if any) involved with the bill, and the bill's status.

If passed, some of these bills could have an impact on the biometric industry and biometrics in general. A study of pending legislation also helps to understand the perceptions (and, often, misperceptions) that may exist (e.g. about biometric recognition technology) and can help to formulate plans to better educate the public and lawmakers.

Pending Legislation

Name of Bill	Bill Number	Stated Purpose	Sponsor	Committees	Status
The Aviation Biometric Badge Act	H.R.115	To amend title 49, United States Code, to improve airport security by using biometric security badges, and for other purposes.	Rep Hefley, Joel (R-CO)	House Transportation and Infrastructure	1/8/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Aviation.
Defense of Privacy Act	H.R.338	To amend title 5, United States Code, to require that agencies, in promulgating rules, take into consideration the impact of such rules on the privacy of individuals, and for other purposes.	Rep Chabot, Steve (R-OH)	House Judiciary	1/27/2003 Referred to House Committee on the Judiciary. Status 3/6/2003 Referred to the Subcommittee on Commercial and Administrative Law, 2/10/2004 Forwarded by Subcommittee to Full Committee (Amended by Voice Vote), 6/23/2004 Ordered to be Reported (Amended) by Voice Vote.

The Iris Scan Security Act of 2003	H.R.1171	To provide grants to law enforcement agencies to use iris scanning technology to conduct background checks on individuals who want to purchase guns	Rep Andrews, Robert E. (D-NJ)	House Judiciary	5/5/2003 Referred to House subcommittee on Crime, Terrorism, and Homeland Security.
The National Uniform Privacy Standards Act of 2003	H.R. 1766.	To make permanent the provisions of the Fair Credit Reporting Act and amend the Gramm-Leach-Bliley Act to establish a national uniform privacy standard for financial institutions.	Rep Tiberi, Patrick J. (OH)	House Financial Services	4/29/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Financial Institutions and Consumer Credit.
The Personal Information Privacy Act of 2003	H.R. 1931.	To protect the privacy of the individual with respect to the Social Security number and other personal information, and for other purposes.	Rep Kleczka, Gerald D. (D-WI)	House Ways and Means; House Financial Services	5/1/2003 Referred to House Financial Services, 5/12/2003 Referred to the Subcommittee on Financial Institutions and Consumer Credit, for a period to be subsequently determined by the Chairman.

The Data-Mining Moratorium Act of 2003	S. 188	To impose a moratorium on the implementation of data-mining under the Total Information Awareness program of the Department of Defense and any similar program of the Department of Homeland Security, and for other purposes.	Sen Feingold, Russell D. (R-WI)	Senate Judiciary	1/16/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
The Privacy Act of 2003	S. 745	To require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes.	Sen Feinstein, Dianne (D-CA)	Senate Judiciary	3/31/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary
The Citizens' Protection in Federal Databases Act	S. 1484	To require a report on Federal Government use of commercial and other databases for national security, intelligence, and law enforcement purposes, and for other purposes.	Sen Wyden, Ron (D-OR)	Senate Judiciary	7/29/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
The Library, Bookseller, and Personal Records Privacy Act	S. 1507	To protect privacy by limiting the access of the government to library, bookseller, and other personal records for foreign intelligence and counterintelligence purposes.	Sen Feingold, Russell D. (D-WI)	Senate Judiciary	7/31/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.

unknown	S. 1599	To require the Secretary of Homeland Security to conduct a study of the feasibility of implementing a program for the full screening of passengers, baggage, and cargo on Amtrak trains, and for other purposes	Sen Snowe, Olympia J. (R-ME)	Unknown	9/9/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.
unknown	H.R. 502	To require identification that may be used in obtaining Federal public benefits to meet restrictions ensuring that it is secure and verifiable.	Rep Tancredo, Thomas G. (R-CO)	House Government Reform; House Judiciary; House Administration	3/6/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
Identity Theft Penalty Enhancement Act	H.R. 1731	To amend title 18, United States Code, to establish Penalties for aggravated identity theft, and for other purposes.	Rep Carter, John R. (TX)	House Committee on Judiciary	6/24/04 Received in the Senate
Genetic Information Nondiscrimination Act of 2003	S. 1053	A bill to prohibit discrimination on the basis of genetic information with respect to health insurance and employment	Sen Snowe, Olympia J. (Me)	Committee on Health, Education, Labor, and Pensions	10/14/03 Passed Senate with an amendment by Yea-Nay Note. 95-0, 10/15/2003 Message on Senate action sent to the House, received in the House, held at the desk.

Social Security Number Privacy and Identity Theft Prevention Act of 2003	H.R. 2971	To amend the Social Security Act to enhance Social Security account number privacy protections, to prevent fraudulent misuse of the Social Security account number, and to otherwise enhance protection against identity theft, and for other purposes.	Rep Shaw, E. Clay, Jr. (FL)		8/8/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Commerce, Trade and Consumer Protection.
The Data-Mining Reporting Act of 2003	S.1544	To provide for data-mining reports to Congress	Sen. Feingold, Russell D. (R-WI)	Senate Judiciary	7/31/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
Social Security On-line Privacy Protection Act	H.R. 70	To regulate the use by interactive computer services of Social Security account numbers and related personally identifiable information	Rep Frelinghuysen, Rodney P. (NJ)		Referred to House subcommittee. Status: Referred to the Subcommittee on Commerce, Trade and Consumer Protection.

Social Security Number Misuse Prevention Act	H.R. 637	To amend title 18, United States Code, to limit the misuse of Social Security numbers, to establish criminal penalties for such misuse, and for other purposes	Rep Sweeney, John E. (NY)		3/5/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Crime, Terrorism, and Homeland Security.
BE REAL Act of 2003	H.R. 3534	To enhance border enforcement, improve homeland security, remove incentives for illegal immigration, and establish a guest worker program	Rep Tancredo, Thomas G. (CO)		3/11/04 Referred to House subcommittee. Status: Referred to the Subcommittee on 21st Century Competitiveness.
Nuclear Infrastructure Security Act of 2003	S. 1043	A bill to provide for the security of commercial nuclear power plants and facilities designated by the Nuclear Regulatory Commission	Sen Inhofe, Jim (OK)		11/6/03 Placed on Senate Legislative Calendar under General Orders. Calendar No. 372.
Visitor Information and Security Accountability (VISA) Act	H.R. 3452	To improve homeland security	Rep Sessions, Pete (TX)		12/10/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Immigration, Border Security, and Claims.

Unknown	H.R. 3522	To amend the Immigration and Nationality Act to bar the admission, and facilitate the removal, of alien terrorists and their supporters and fundraisers, to secure our borders against terrorists, drug traffickers, and other illegal aliens, to facilitate the removal of illegal aliens and aliens who are criminals or human rights abusers, to reduce visa, document, and employment fraud, to temporarily suspend processing of certain visas and immigration benefits, to reform the legal immigration system, and for other purposes	Rep Barrett, J. Gresham (SC)		12/10/03 Referred to House subcommittee. Status: Referred to the Subcommittee on Immigration, Border Security, and Claims

Medical Independence, Privacy, and Innovation Act of 2003	H.R. 2196	To improve the quality, availability, diversity, personal privacy, and innovation of health care in the United States	Rep Rohrabacher, Dana (CA)		6/12/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census.
Identity Theft Prevention Act of 2003	H.R. 220	To amend Title II of the Social Security Act and the Internal Revenue Code of 1986 to protect the integrity and confidentiality of Social Security account numbers issued under such title, to prohibit the establishment in the Federal Government of any uniform national identifying number, and to prohibit Federal agencies from imposing standard for identification of individuals on other agencies or persons.	Rep Paul, Ron (TX)	House Ways and Means	1/21/03 Referred to House subcommittee. Status: Referred to the Subcommittee on Social Security

Safeguard Against Privacy Invasions Act	H.R. 2929	To protect users of the Internet from unknowing transmission of their personally identifiable information through spyware programs, and for other purposes.	Rep Bono, Mary (CA)	House Committee on Energy and Commerce	6/24/2004 House committee/subcommittee actions. Status: Ordered to be Reported (Amended) by the Yeas and Nays: 45-5
Protecting the Rights of Individuals Act	S. 1552	A bill to amend Title 18, United States Code, and the Foreign Intelligence Surveillance Act of 1978 to strengthen protections of civil liberties in the exercise of the foreign intelligence surveillance authorities under Federal law, and for other purposes.	Sen Murkowski, Lisa (AK)	Committee on the Judiciary	7/31/03 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary

SAFE-ID Act	S. 2471	A bill to regulate the transmission of personally identifiable information to foreign affiliates and subcontractors.	Sen Clinton, Hillary Rodham (NY-D)		5/20/2004 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
Online Privacy Protection Act of 2003	H.R. 69	To require the Federal Trade Commission to prescribe regulations to protect the privacy of personal information collected from and about individuals who are not covered by the Children's Online privacy Protection Act of 1998 on the Internet, to provide greater individual control over the collection and use of that information, and for other purposes.	Rep Frelinghuysen, Rodney P (NJ)		2/3/2003 Referred to House subcommittee. Status: Referred to the Subcommittee on Commerce, Trade and Consumer Protection.

Department of Defense Appropriations Act, 2004	H.R. 2658 S.AMDT 1257 to H.R. 2658	Making appropriation for the Department of Defense for the fiscal year ending September 30, 2004 and for other purposes. (To make available from amounts available for Research, Development, Test, and Evaluation, Defense-Wide, $3,000,000 for Long Range Biometric Target Identification System.)	Rep Lewis, Jerry (Sen Voinovich, George V. (OH))		7/15/2003 Senate amendment agreed to. Status: Amendment SA 1257 agreed to in Senate by Voice.

The Data-Mining Moratorium Act of 2003	S. 188	To impose a moratorium on the implementation of datamining under the Total Information Awareness program of the Department of Defense and any similar program of the Department of Homeland Security, and for other purposes.	Sen Feingold, Russell D. (R-WI)	Senate Judiciary	1/16/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
The Privacy Act of 2003	S. 745	To require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes.	Sen Feinstein, Dianne (D-CA)	Senate Judiciary	3/31/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary
The Citizens' Protection in Federal Databases Act	S. 1484	To require a report on Federal Government use of commercial and other databases for national security, intelligence, and law enforcement purposes, and for other purposes.	Sen Wyden, Ron (D-OR)	Senate Judiciary	7/29/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.

The Library, Bookseller, and Personal Records Privacy Act	S. 1507	To protect privacy by limiting the access of the government to library, bookseller, and other personal records for foreign intelligence and counterintelligence purposes.	Sen Feingold, Russell D. (D-WI)	Senate Judiciary	7/31/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on the Judiciary.
Unknown	S. 1599	To require the Secretary of Homeland Security to conduct a study of the feasibility of implementing a program for the full screening of passengers, baggage, and cargo on Amtrak trains, and for other purposes	Sen Snowe, Olympia J. (R-ME)	Unknown	9/9/2003 Referred to Senate committee. Status: Read twice and referred to the Committee on Commerce, Science, and Transportation.

Unknown	H.R. 502	To require identification that may be used in obtaining Federal public benefits to meet restrictions ensuring that it is secure and verifiable.	Rep Tancredo, Thomas G. (R-CO)	House Government Reform; House Judiciary; House Administration	1/29/2003 Referred to House committee. Status: Referred to the Committee on Government Reform, and in addition to the Committees on the Judiciary, and House Administration, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned.