STATE BAR OF MICHIGAN

MICHIGAN COMPUTER LAWYER

State Bar of Michigan Computer Law Section http://www.michbar.org/computer/ Volume 23, No. 6

Law Review - Biometrics: Its Applications and Concerns

By Fernando M. Vallés —Ed Langs Writing Contest Third Place Winner

Introduction

Larry Johnson, a second-year law student, wanting to get his mind off the books and the rigors of law school, decides to watch one of his favorite comic-based movies: X-men®.[1] Larry assumes that the movie will allow his mind necessary rest from the usual legal mindset. Excited about enjoying a good movie, Larry fixes himself some popcorn and hits play on his multi-media DVD player. He sits on his couch and allows the movie to transport him back to his days as a kid when he envisioned being a superhero just like Cyclops. He intently watches the scene where Cyclops is granted access to Professor Xavier's office via a retinal scan. At this point; however, rather than enjoying the high-tech factor that fantasy movies possess, he recalls a lecture his computer law professor gave on privacy issues and biometrics. Much to Larry's surprise, X-men® sparked an interest in this issue and he wanted to learn more.

The reality is that this technology, named biometrics, is already being used in some applications. For example, it is implemented in many personal electronic devices, such as the IBM ThinkPad T42®. This laptop has a finger-scanning unit incorporated within the frame of the computer, where the user can log into the system by swapping his finger over the infrared scanning device. This technology has re-gained popularity, especially after September 11, 2001.

The United States government has made a big push under the USA Patriot Act[2] to implement new security measures. At first glance, it seems that biometrics would be the next logical step in a world where technology has become more and more part of our lives. For instance, computer technology is ever present in our society from the way children learn to read to the systems used by global banks to control currency. It seems appropriate

Continued on next page

Michigan Computer Lawyer is published bi-monthly. If you have an article you would like considered for publication, send a copy to:

Matthew M. Jakubowski
Brooks Kushman, P.C.
1000 Town Center
Floor 22, Suite 2200
Southfield, MI 48075-1183
e-mail: *mjakubowski@brookskushman.com*

to implement a computerized identification system that will allow a person to be distinguished by the tone of his or her voice or by the retinas in his or her eyes. Yet, a technology like biometrics has legal implications that need to be analyzed before being implemented. Specifically, one needs to examine how our privacy rights and other constitutional rights protected under the U.S. Constitution, can be affected by biometrics.

The purpose of this article is to explore, identify, and examine the legal implications, specifically constitutionally, of a technology of this type. Part I describes the biometric system and how its applications function. Part II discusses the constitutional issues with the biometric system, while describing the emerging principle of privacy extrapolated from the U.S. Constitution. Part III applies the different constitutional issues, such as due process, to the biometric system. Lastly, Part IV examines whether the biometric system can withstand Constitutional scrutiny by looking at current privacy acts. Hopefully, the reader will be able to understand and be better informed of the legal issues that face the implementation of a biometric identification system.

Biometrics: Its Applications and Concerns

The term biometrics refers to the study of automated methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits.[3] In actuality, this identificaiton system has been around for a long time. Fingerprinting is likely the most well-known biometric identification measure. This identification method involves the examination of the unique characteristcs of a person's fingerprints. However, this new method of biometrics goes further than your typical fingerprint at a police station. It can recognize a wide variety of physical characteristics and store those characteristics into a database. In essence, biometrics refers to technologies that measure and analyze human physical and behavioral characteristics for authentication purposes.[4]

A person's biometric measurements are scanned and integrated into a computer system.[5] Some of the physical characteristics used in biometrics are: personal traits, chemical compositon of body odor, unique features of the eye (retina), hand geometry, voiceprint, and many others.[6] The way biometrics is implemented generally is by the following steps: (1) the physical characteristic or trait of an individual is scanned into a computer database; (2) the individual's unique features are converted into a digital code; (3) this newly transformed digitial code is stored in a database; and (4) when the person again tries to seek access into the system, he is scanned and compared to the stored digital code of the individual's distincitive trait or characteristic.[7]

Biometrics allows for an identification system to be established by comparing a person's unique individualities to those saved in the database. The retina, iris, or fingerprint scan provides the greatest reliability and accuracy for biometrics.[8] These are known as "High Biometrics" since they are distinguished by their high accuracy.[9] For example, the retinal scanning, as seen in the movie X-Men®, is performed by electronically scanning a person's innermost layer of the wall of the eyeball (retina). The reason why the retina is unique to every individual is due to the blood vessel pattern found in this part

of the eye. An incandescent beam of light is passed over a person's eye and the light bounces off the retinal vascular structure and returns back to the scanner. This information is recorded in an easily retrievable digitized database. The slight disadvantage to this type of scanning is the close physical contact with the scanning device and the potential change of the retinal vascular structure due to diseases like diabetes.

Unfortunately, the system is only as good as the type of physical characteristic used and the information contained in the database. Nevertheless, the advantages of a system using unique physical characteristics can benefit law enforcement and government officials to protect its citizens' safety. In the past, biometrics has been applied for certain applications and the U.S. government presently hopes to use it more to help fight the war against terrorism.

Applications of The Biometrics System

Since the tragedies of September 11th, 2001, biometrics has taken center stage in the media and on Wall Street as a means to improve homeland and airport security.[10] As mentioned earlier, fingerprints have been used for many years now. The biometrics system allows for the storing of a person's fingerprint in a database.[11] This information can be used for different purposes.

For instance, the majority of fingerprint searches are not used to solve crimes, but rather to perform background checks.[12] Also, as the incidents of identity theft continue to increase, the Federal Trade Commission (FTA) has been pushing for biometrics to be used to deter ID theft by implementing an individual's biometric identifier to their accounts (i.e. bank accounts).[13] In other words, biometrics has great potential in a government enforcement setting.

Privacy activists in this country have criticized the technology's use; its potential harm to civil liberties, privacy, and the risk of identity theft. Currently, there is some apprehension in the United States (and the European Union) that the information can be "skimmed" and used to identify people's citizenship remotely for criminal intent, such as kidnapping.[14] There are also technical difficulties currently delaying biometric integration into passports in the United States, the United Kingdom, and the rest of the European Union.[15] These difficulties include compatibility of reading devices, information formatting, and nature of content.

Biometrics can also be used in the private sector for several applications. The most common use has been at sporting events or banks. Walt Disney World® in Orlando, Florida, has been using a system of hand scanning to prevent unauthorized use of season passes.[16] Banks have been using this system in order to offer customers without a bank account a method of cashing a payroll check by providing a fingerprint or thumprint. It has also been implemented in some banks that provide safe deposit boxes. An individual has to provide his/her thumbprint, in order to access the deposit box.[17] The applications to the biometrics system are endless, but also bring many concerns.

Potential Concerns with Biometrics

Although the benefits of a biometric system seem progressive, there are those who believe that the U.S. government is trying to push this technology as a "silver bullet" for the fight against terrorism. Deploying a biometric system without sufficient attention to its dangers could likely infringe upon a person's civil liberties. Some of the problems with this system are the following:[18]

- The system must be created to specifically target a certain group of the population (i.e. terrorists).[19]
- The system is only as good as the initial identification, which in any foreseeable system, will be based on exactly the document-based methods of identification upon which biometrics are supposed to be an improvement. In other words, a person with a fake identity that implements his/her biometrics into the system is still not the correct person.[20]
- There is a subset of the population in which biometrics will not work. For example, there are people who do not have fingerprints that print well.[21]
- The risk of error and theft is significantly higher than any current identification system. If your credit card is stolen, you can always get a new one. However, if your biometric is stolen it is not as easily recoverable.[22]

- Lastly, the biggest problem with the biometric system is privacy. The system must make a person's privacy the most important and protected aspect of the system.[23]

Constitutional Issues with Biometrics: The Right to Privacy and the U.S. Constitution

Whenever a new technology is introduced into our society, it must conform to the standards of the current legal system. Before the biometric system is officially implemented in our society, it must pass constitutional muster. Most importantly, the government must be certain that a technology like biometrics does not prevent its citizens from enjoying their privacy rights.

History of Privacy Rights

The reality is that the word privacy is not actually found in the text of the United States Constitution, but it has been an "evolving standard" that has changed over the centuries according to our society.[24] During the early days of our Republic, the colonies recognized a right of physical privacy centered in the home where a person could be free from contract with others.[25] At the time the Constitution was drafted by our forefathers, the idea of privacy interests was incorporated in the Bill of Rights without an explicit reference to privacy.[26] The First Amendment mentions rights of freedom of speech, press, and association.[27] The Third Amendment prohibits against the quartering of soldiers in one's home.[28] The Fourth Amendment mentions the right to be free from unreasonable searches and seizures.[29] The Fifth Amendment states the right against self-incrimination.[30] The Ninth Amendment provides that "the enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage those others retained by the people."[31] Lastly, the Tenth Amendment states that "the powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people."[32] As our country continued to evolve after its inception, the states added more legislation to protect its citizens' rights.

For example, in 1844 Samuel F.B. Morse invented a new technology that changed the way people communicated.[33] Mr. Morse created the telegraph. This new technology brought new privacy challenges to the legal system. Not long after its inception, the telegraph was used as the unscrupulous perfected wiretapping to intercept telegraphic messages of other people.[34] State legislatures reacted to this privacy intrusion by passing statutes prohibiting unauthorized interception of telegraph communications and the cutting of telegraphs lines.[35] However, privacy laws continue to change by focusing more on a person's privacy rather than place of privacy (i.e. home).

In 1879, Judge Thomas M. Cooley, in his treatises on torts, included "the right to be let alone as a class of tort rights, contending that the right to one's person may be said to be a right of complete immunity."[36] Judge Cooley's phrase "the right to be let alone" was re-stated by Warren and Brandeis in their article called "The Right to Privacy."[37] Brandeis, as a U.S. Supreme Court Justice, would later use the phrase in *Olmstead v. United States,* 277 U.S. 438 (1928).

In *Olmstead,* the defendants' telephones were tapped by the police without trespassing upon defendants' property and the defendants were convicted of conspiracy in violation of the National Prohibition Act.[38] The Court held that there was no room for applying the Fifth Amendment, unless the Fourth Amendment was first violated.[39] It held it was not violated unless there was an official search and seizure of a person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house or curtilage for the purpose of making a seizure.[40] In Brandeis' famous dissent in this case, he declared that the Founding Fathers "conferred, as against the Government, the right to be let alone-the most comprehensive of rights and the right most valued by civilized men."[41] These and other past events in our country's history have shaped our current modern privacy interests under the Constitution.

Privacy Protections Under the United States Constitution and Current Applications

In our current legal system, the concept of privacy was really tested in the latter part of the twentieth century by cases such as *Griswold v. Connecticut,* 381 U.S. 479 (1965). In this case, the United States Supreme Court held that the guarantees in the Bill of Rights create "zones of privacy."[42] The Court reasoned that the specific guarantees in the

Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance, thus creating zones of privacy.[43] Since this case, the Court has extended privacy protection to other areas such as reproductive choices.[44] Also, the federal government has enacted statutes designed to protect a citizen's privacy.

The Fair Credit Reporting Act was created by the federal government to regulate disclosures of consumer credit information.[45] The purpose of this act was to prevent the abusive, deceptive, and unfair practices in debt collection, often resulting in invasion of privacy. [46] Other federal statutes that have been enacted due to the interpretation of privacy are the Privacy Act of 1974 and the Tax Reform Act of 1976. The Privacy Act of 1974 required governmental executive agencies to follow certain procedures in the collection and disclosure of personal information that these agencies collect.[47] Also, the Tax Reform Act of 1976 provided the IRS the same restrictions under the Privacy Act in order to limit the disclosure of an individual's tax information.[48]

Constitutional Issues with the Biometric Authentication System

The implementation of a biometric system in our society must conform with concepts of due process law applicable to both the state and federal governments. The Fifth and Fourteenth Amendments do not allow the government to intentionally deny "a person his life, liberty or happiness without due process of law."[49] This means that a person may not lose his life, freedom of action, a freedom provided by the Constitution or an entitlement granted under state or federal law without a fair process, usually a notice of the deprivation and a subsequent hearing on the matter.[50]

Another issue that affects the implementation of the biometrics system is whether the demand by the government for either a physical characteristic of a person or the biometric device, in which it is incorporated, violates the Fourth Amendment principles. The Fourth Amendment of the U.S. Constitution states "the right of the people to be secure in their persons against unreasonable searches and seizures" unless a warrant is issued based upon probable cause.[51]

Application of the Constitutional Issues to the Biometric System

In order to tackle the Constitutional issues brought to light by the implementation of the biometrics system, the government has to determine that the system does not violate its citizens' privacy rights as mentioned in the above Amendments. The Constitutional issues must be applied to the problems presented above to determine whether the biometrics system passes the Constitutional test.

Applying the Biometrics System to the Due Process of Law

As stated earlier, a biometric identification system must conform to the concepts of due process law applicable to both the state and federal governments. The Fourteenth Amended states:

> No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.[52]

What this means is that a person may not lose his enumerated rights in the Constitution without proper notice of the depraved right and a subsequent hearing on that matter.[53]

For instance, Charles has reached the age of retirement and is entitled under the state and federal government to obtain his social security benefits. The government intends to distribute his benefits with the aid of a biometric identification system (i.e. Charles will have to scan his fingerprints on a scanner to verify authenticity). He will receive his social security benefits as long as his fingerprints match those already stored in the biometric database that corresponds to his physical characteristic. What if Charles fingerprints do not match those in the database? If Charles is denied his social security benefits, his due process law under the Fourteenth Amendment has been violated, unless the government properly demonstrates that he is not entitled to the benefits.

The government would have to demonstrate its reasons, along with a hearing between the person obtaining the benefits and the government entity. During the hearing, the government entity would have to demonstrate that: (1)

the person requesting the government benefit did not match the biometric identifier used as proof of identity; and (2) the biometric process is a scientifically accurate method on which to rely as a demonstration of identity.[54] The first part of the test is easily met, when a person's fingerprints do not match with the fingerprints stored in the database.[55]

The second part of the test examines the accuracy of the biometric process, which is a bit more difficult to prove. Even though administrative hearings do not incorporate to the rule of evidence, it would be prudent to apply Federal Rules 702[56] of evidence during a hearing of such sort. Under this rule, the acceptance of the biometric process depends heavily on scientific studies, which measure its accuracy rate of identification.[57] In other words, a court's finding that the biometric process is accurate is determined by demonstrating that it is a legally acceptable evidence of identity and that the government's denial of the benefit appears fair.[58] The other legal issue is to determine whether the biometric system violates the Fourth Amendment.

Does the Biometric System Violate Fourth Amendment Principles?

The Fourth Amendment states: "The right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated…"[59] To determine if the biometric system violates the Fourth Amendment: (1) the government will have to be involved, (2) the use of biometrics will have to be considered a search, and (3) the search considered must be unreasonable.[60]

The first prong of this test is easily met by determining if it is a government agency that is involved in the search. In the example mentioned before, the government agency determining your entitlement for social security benefits would meet the first prong. The second and third prongs are more difficult to determine.

In *Skinner v. Railway Labor Executive's Association*, 489 U.S. 602 (1989), the Supreme Court of the United States held that the collection and subsequent analysis of the requisite biological samples must be deemed a Fourth Amendment search when: (1) the Government seeks physical evidence from a person; (2) where the gathering of the evidence involves an intrusion into the person's body; and (3) the evidence has the potential of revealing a person's medical facts.[61] In this case, Railway Labor Executive's Association filed suit to enjoin the enforcement of regulations promulgated by the Federal Railroad Administration.[62] The regulations that were part of the suit demanded tests of blood, urine, and breath tests of railroad workers who violated safety rules or were involved in accidents.[63] The main issue with this mandate by the Railroad Labor Executive's Association was a Fourth Amendment violation.

Ultimately, the Supreme Court stated that it had long recognized that a compelled intrusion into the body for blood must be deemed a Fourth Amendment search.[64] Also, where an individual's skin is penetrated in order to obtain a blood sample, it is obvious that this physical intrusion infringes an expectation of privacy that society is prepared to recognize as reasonable.[65] Lastly, the Court held that the analysis of urine, like that of blood, can reveal a host of private medical facts about an individual, including whether he or she is epileptic, pregnant, or diabetic.[66]

Extrapolating the reasoning of Skinner into the biometrics issue, one can deduce that the use of biometrics should be deemed a search if gathering the biometric information intrudes into a person's body, while revealing private issues such as medical facts.[67] Therefore it must be established whether or not biometric measures are considered searches under the Fourth Amendment.

As stated earlier, the use of fingerprinting to identify a person has been the oldest and most used biometric measure. In *Davis v. Mississippi,* 394 U.S. 721 (1969), the defendant was detained by police and required to provide a fingerprint sample.[68] The defendant protested that the fingerprinting evidence was inadmissible as evidence because it was obtained during an illegal detention.[69] Even though the Court determined that the fingerprinting was inadmissible due to the illegal detention, the Court held that "fingerprinting involves none of the probing into an individual's life and thoughts that marks an interrogation or search."[70] Also, a person's fingerprints are exposed to the public.

The phrase "exposed to the public" was defined in *United States v. Dionisio,* 410 U.S. 1 (1973). In this case, the Court held:

> The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his

> voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.[71]

Although the Court has determined that fingerprints do not constitute a search, it has not determined if the use of fingerprints to uncovered private information, such as medical information constitutes a search. However, there is case law that may determine the use of biometrics measures, such as fingerprinting or retina scans, which can constitute a search due to the personal information that is revealed.

In *Kyllo v. United States*, 533 U.S. 27 (2001), the Supreme Court held that the use of thermal imaging technology to detect the amount of heat radiating from a house was a search even though the device could not penetrate the walls of the house.[72] Comparing the thermal imaging technology to a retinal scan, the reality is that no physical penetration is involved. However, the retinal scan can determine a person's medical state by the vessel pattern in a person's retina (i.e. diabetes). The second prong of the test is met by a biometric system if it appears to involve the requisite level of physical intrusion or the ability to reveal private medical facts, in order to constitute a Fourth Amendment search.

The next prong that needs to be determined to find out if a violation of the Fourth Amendment has taken place is to examine if the biometric search is reasonable. In order to determine if a particular search meets the reasonableness test standard, it is judged by balancing the intrusion on the individual's Fourth Amendment interest against its promotion of legitimate government interests.[73] A search is not unreasonable if a person voluntarily consents to the search or the search is being done for administrative purposes. Administrative searches are defined as a general regulatory scheme conducted for administrative purposes, rather than as part of a criminal investigation to secure evidence of a crime.[74]

The legality of administrative searches was upheld in *United States v. $124,570 U.S. Currency*, 873 F.2d at 1243. The Ninth Court of Appeals stated that:

> Americans submit to metal detectors and x-ray devices without a second thought. The intrusion into our privacy—and an intrusion it surely is—is accepted by most travelers with equanimity. The unavoidable consequence of [security checks] is that security personnel will become aware of many personal items that do not pose a danger to air safety…When packages are opened, or when pockets are emptied, [airport security] agents will see many items that are considered private.[75]

Thus, the government has a strong interest in promoting the use of biometrics as a means of protecting its citizens, as well as preventing any harm. Even if the use of biometrics is reasonable, it is necessary that such use "serve a narrow but compelling administrative objective and that the intrusion be as limited as is consistent with satisfaction of the administrative need that justifies it."[76] Therefore, the biometric system must be carefully implemented so that no Fourth Amendment violation is committed.

Applying the Biometrics Issue to Privacy Laws

A third issue that confronts the implementation of a biometric system is the right to privacy. Even though the right to privacy is not expressly stated in the Constitution, it has been recognized by a number of Supreme Court cases. As stated earlier, *Griswold v. Connecticut,* which involved the dissemination of birth control, was one of the first cases to discuss the right to privacy.[77] Justice Douglas, who gave the majority opinion, reasoned that:

> A State could not impede the distribution of birth control information because a constitutional right to privacy located in the "penumbras" emanating from the First Amendment's right of Association, the Third Amendment's prohibition against the quartering of soldiers in any home in time of peace, the Fourth Amendment's right of the people to be free from unreasonable search seizures, the Fifth Amendment's right against self-incrimination, and the Ninth Amendment's reservation of right to the people.[78]

Even though not everyone agreed with Justice Douglas' opinion, it became the foundation for other right to privacy cases. Therefore, privacy protections are at the heart of any possible debate about the implementation of a biometric authentication system.

Opponents to the implementation of a biometric identification system fear that a biometrics system will chip away at citizens' privacy rights under American Law.[79] Opponents also fear that criminals, the government or industry will access the databases and obtain personal information concerning a person's buying habits, private financial transactions, and so forth.[80] A trepidation also exists that an outside source could obtain the biometric data during its transmission through the Internet. This fear is stemmed from the U.S. Supreme Court's decision in the *Whalen* case.

In *Whalen v. Roe,* 429 U.S. 589, the constitutional question was whether the State of New York could record, in a centralized computer database, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs.[81] The facts showed that the New York state legislature established a commission to evaluate the state's drug control laws. To correct perceived deficiencies in this state law, the commission, after study, drafted legislation, as part of the New York Public Health Law, which required prescriptions for Schedule II drugs to be prepared by the physician on an official state-provided form.[82] Various parties consisting of patients, doctors and physician's associations challenged this statute in the federal courts. The Court held that neither the immediate nor the threatened impact of the patient-identification requirements, on either the reputation or the independence of patients, was sufficient to constitute an invasion of any right or liberty protected by the Fourteenth Amendment.[83] The Court basically held that the government's centralized, computerized database containing massive amounts of sensitive medical information passed constitutional muster.

Determining whether a biometric identification system violates a person's right to privacy really depends on the program the government decides to use. A program that is all encompassing might have a difficult time getting past the privacy issues. Also, the biometric system has to be used for its intended purpose and not expanded to other things. For instance, the social security number in the United States was originally intended for use by employers and employees.[84] In later years, the government expanded the system to all federal employees and in 1961, the IRS used the number to identify people for taxing purposes. Currently, the social security number is used for many more applications.[85] In order for the biometric identification system to work, it will have to withstand the restrictions by some of the privacy laws used in our country.

The Electronic Communications Privacy Act (ECPA) codifies warrant requirements for the interception of electronic communications and also create privacy protections for stored electronic messages.[86] Title I of the ECPA makes it a crime and a statutory tort[87] for any person to: (1) intercept any wire, oral or electronic communications; (2) to disclose such intercepted communications; and, (3) to use a device to intercept oral communications.[88] Title II of the ECPA protects stored wire and electronic communications and transactional records, which means it could protect the transmission and storage of biometric patterns only if they fall under one of the protected categories.[89]

The biometric system works by storing a person's physical characteristics, such as fingerprints, as encrypted electronic data. If you compare the biometric system to the codified language in the ECPA, one can conclude that the transmission of a fingerprint pattern from a stored database to other private or government entities as a method of identification might be protected. However, there are two exceptions to the ECPA. It allows private-sector employers unlimited ability to monitor employees' email communications through two exceptions: (1) prior consent, and (2) business use. An employee can sign a written policy, which gives the employer consent to monitor electronic communications.[90] Also, the provider of the electronic communication system has the right to intercept messages, including e-mail and voice mail, within the ordinary course of the employer's business.[91] These two exceptions would have to be removed for a biometric system to work properly. An Act like the ECPA would have to be tailored specifically for biometrics and not allow private-sector employers unlimited ability to access your biometric patterns.

The Privacy Act of 1974[92] was created to forbid the disclosure of federal agency records without the written consent of an individual to whom the record pertains unless the disclosure is for the purpose for which the data was collected.[93] The records mentioned in the statute are basically any record used by any agency, which contains a particu-

lar identifying characteristic of a person.[94] The Privacy Act mandates employees of a federal agency not to disclose any financial, education, criminal, employment and medical data to any not entitled person.[95] However, a person's private information can be transferred between agencies or to state criminal law enforcement entities, as long as the specific information is requested and its specific purpose is stated.[96]

A person's financial records can identify, among other things, a person's associates, political allies, and religious and social affiliations. Financial institutions, such as credit card companies or mortgage companies possess a plethora of financial information, which is routinely disseminated. The Fair Credit Reporting Act (FCRA) limits the persons to whom consumer-reporting agencies can disclose data.[97] Also, the Federal Right to Financial Privacy Act of 1978[98] limits the ability of financial institutions to disclose customer information to federal agencies. Since many US corporations contain many people's financial records, the privacy of biometrics characteristics will have to be closely guarded to prevent the dissemination of this information.

Conclusion

The constitutionality of a biometric identification system will be difficult to determine, since there is no true consensus. On one side, there are cases like *Whalen v. Roe*, which state that there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[99] On the other hand, a case like *Katz v. United State*s, 389 U.S. 254 (1970), which held that the Fourth Amendment protects people and not places, and where a person has a reasonable expectation of privacy, the person is entitled to be free from unreasonable government intrusion.[100] However in the Katz case, the determination of whether or not the taking of the biometric sample violated the Fourth Amendment relied on: (1) whether a search under the Fourth Amendment had occurred; and, (2) whether the search was "unreasonable." Therefore, the implementation of a biometric identification system will have to walk the tight rope of constitutionally protected rights.

The biometric identification system will have to withstand legal and policy challenges. The government will have to create a biometric identification system type of act that will make certain that the databases used will be secure and that all reasonable measures will be taken to prevent any unauthorized disclosures. If history is an indicator, technology always seems to outpace laws. While it is unclear whether the government will fully implement a biometric identification system, the government should be proactive in fleshing out the details for a technology that will eventually be used globally. Therefore, Larry can still enjoy X-men® and fantasize about a world where technology is not hindered by laws.

Endnotes

1 X-MEN (Fox Pictures 2000). A movie based on the screen adaptation of the classic comic book about a band of unique power-possessing mutants who live in a world where their kind is hated and persecuted by humans and under the guidance of their leader, Professor Charles Xavier, the X-men strive for a world where humans and mutants can peacefully co-exist.

2 US Patriot Act §. 403(c), (it requires the federal government to develop and certify a technology standard that can be used to verify the identity of persons).

3 Biometrics, *available at* http://en.wikipedia.org/wiki/Biometrics.

4 *Id.*

5 Joseph P. Campbell, Jr. et al., Biometric Security: Government Applications and Operations, at 1, in CTST '96 Government Conference Proceedings (1996), *available at* http://www.biometrics.org/REPORTS/CTSTG961.

6 *Id.*

7 Bill Siuru, Iris Recognition Systems, ELECTRONICS NOW, Feb. 1999, at 41.

8 Donald R Richards, Rules of Thumb for Biometric Systems, Security Mgmt., Oct. 1, 1995, at 67.

9 *Id.*

10 701 PLI/Pat 105.

11 *Id.*

12 *Id.*

13 *Id.*

14 *Id.*

15 *Id.*

16 See, supra note 3.

17 (Bankrate.com, "Banks not yet banking on biometrics" by Laura Bruce [accessed on Apr. 6, 2006).

18 http://www.eff.org.

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

23 *Id.*

24 David H. Flaherty, Privacy in Colonial New England 85-88 (1972).

25 *Id.*

26 Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

27 U.S. Const. Amend. I.

28 U.S. Const. Amend. III.

29 U.S. Const. Amend IV.

30 U.S. Const. Amend. V.

31 U.S. Const. Amend. IX.

32 U.S. Const. Amend. X.

33 See, supra note 3.

34 Alan F. Westin, Privacy and Freedom 337 (1967) (citing W. Scott & M. Jarnagin, Treatise Upon the Law of Telegraphs, Appendix, 457-507 (1868).

35 *Id.*

36 Richard F. Hixson, Privacy in a Public Society: Human Rights in Conflict 30 (1987).

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

38 Olmstead v. United States, 277 U.S. 438 (1928).

39 *Id* at 440.

40 *Id.*

41 *Id.*

42 Griswold, supra note 26, at 479.

43 *Id.*

44 See, Roe v. Wade, 410 U.S. 113 (1973).

45 15 U.S.C. § 1681 (1999).

46 See 1692.

47 5 U.S.C. § 552(a) (2006).

48 26 U.S.C. § 6103.

49 U.S. Const. XIV Amend.

50 Goldberg v. Kelly, 397 U.S. 254 (1970).

51 U.S. Const. IV Amend.

52 U.S. Const. XIV Amend.

53 Goldberg, supra 50, at 254.

54 80 J. Pat. & Trademark Off. Soc'y 703, 721.

55 *Id.*

56 (governing the admission of testimony of expert witnesses, obligates a trial judge to act as screener for all scientific evidence)

57 See, Neil v. Biggers, 409 U.S. 188, 198 (1972)

58 80 J. Pat & Trademark Off. Soc'y 703, 722.

59 U.S. Const. IV Amend.

60 20 Temp. Envtl. L. & Tech. J. 251, 257.

61 Skinner v. Ry. Labor Executives' Assoc., 489 U.S. 602 (1989).

62 *Id at* 612.

63 *Id at* 606.

64 *Id. at* 616.

65 *Id.*

66 *Id at* 617.

67 20 Temp. Envtl. L. & Tech. J. 251, 259.

68 Davis v. Mississippi, 394 U.S. 721 (1969).

69 *Id at* 722.

70 *Id. at* 727.

71 United States v. Dionisio, 410 U.S. 1 (1973).

72 Kyllo v. United States, 533 U.S. 27, 34 (2001).

73 Acton, 515 U.S. at 653-54 [citing Skinner v. Ry. Labor Executives' Assoc., 489 U.S. 602, 619 (1989).

74 United States v. $124,570 U.S. Currency, 873 F.2d 1240 (9th Cir. 1989).

75 *Id.* at 1243.

76 *Id. at* 1244.

77 Griswold, supra 26, at 479.

78 *Id at* 484.

79 See, supra note 18.

80 Whalen v. Roe, 429 U.S. 589 (1977).

81 *Id.* at 591.

82 *Id.* at 593.

83 *Id.* at 603.

84 Simon G. Davies, Touching Big Brother. How Biometric Technology Will Fuse Flesh and Machine, Vol. 7 Information Technology & People no. 4 (1994) at 6.

85 *Id.*

86 Henry H. Perritt, Jr., Law and the Information Superhighway, 399 (1996). Electronic Funds transfers made by consumers are regulated by the Electronic Funds Transfer Act. Article 4A of the Uniform Commercial Code regulates wholesale wire transfers except for those covered by Federal Reserve regulations operating circulars of Federal Reserve banks,

87 18 U.S.C. § 2511(1).

88 *Id.*

89 18 U.S.C. §§ 2701 (2006).

90 18 U.S.C. § 2511(2)(d) (2006).

91 18 U.S.C. § 2510(5)(a) (2006).

92 5 U.S.C. § 552a.

93 See 5 U.S.C.§ 552a(b)(3) and § 552a(a)(7).

94 5 U.S.C. § 552a(a)(4) (2006).

95 5 U.S.C. § 552a(b)(7) (2006).

96 *Id.*

97 Consumer reporting agencies are persons who collect or evaluate consumer credit information for third parties. See 15 U.S.C. § 1681a(f) (2006).

98 12 U.S.C. § 3401, et seq.

99 Whalen, supra note 81, at 589.

100 Katz v. United States, 389 U.S. 254 (1970).

State Bar of Michigan
Michael Franck Building
306 Townsend Street
Lansing, MI 48933

**Presorted
First Class Mail
U.S. Postage Paid
Lansing, MI 48933
Permit No. 191**