THUMBS UP FOR BIOMETRIC AUTHENTICATION!

By
Gwen "Wendy" Kennedy
Associate Professor of Law
Western State University School of Law

INTRODUCTION

For years, biometric authentication devices, such as palm print devices, retinal scanners and facial recognition technology, were things only seen in science fiction movies. But, in recent years, fiction and reality have been on a collision course. Government laboratories and defense installations have utilized these biometric authentication devices for decades, but commercial applications did not exist until more recently. This delay was caused in part by the high cost of these devices and the legal uncertainty surrounding their use in the commercial realm. However, these concerns have vanished and due to the growing instances of identity theft, the timing for this technology has never been better.

The only remaining impediment to the large-scale deployment of biometric authentication devices is the perceived threat to privacy. While existing law provides a modicum of privacy protection for consumers, more protection will be necessary to ease consumer concerns about identity theft. This article proposes the introduction of a federal regulatory regime based in large part on the Code of Fair Information Practices. As an added incentive for vendors and financial institutions to adopt these practices, this article also proposes the grant of favorable legal presumptions to those who abide by these practices.

I. THE NEED FOR GREATER SECURITY IN CONSUMER TRANSACTIONS

Identity theft is one of the fastest growing problems facing the American consumer.[1] Identity theft has become a problem of such widespread concern that an on-site shredding and recycling company started a campaign in 2002 to designate October as "Security Month." (cite) The purpose of the campaign is to inform consumers about the potential risks of disposing of important documents such as bills, credit cards and bank statements in non-secure places like garbage bags, trashcans and dumpsters. In September 2003, the Federal Trade Commission ("FTC") released a survey showing that 27.3 million Americans had been victims of identity theft from 1998 to 2003.[2] Alarmingly, the problem only seems to be growing. For instance, according to the survey, almost ten million Americans have discovered that they have been victims of some form of identity theft within the last year.[3] Furthermore, since November 1, 1999 when the FTC began collecting complaints from consumers, the number of complaints has doubled each year.[4]

---

[1] *See* Sandra Block, *States Pass Laws to Protect Identity*, USA TODAY, July 12, 2003, at B1 ("State lawmakers, alarmed by high-profile identity-theft scams, are adopting measures that could become models for a federal law protecting victims from the nation's fastest-growing crime."); Bruce Bigelow, *San Diego Startup Makes a Name for Itself in the Identity-Theft Wars*, SAN DIEGO UNION TRIBUNE, June 10, 2003, at C1 ("Today, identity theft is one of the fastest-growing crimes in America."); *New Law Forces Companies to Warn Consumers of Computer Security Holes*, HOUSTON CHRONICLE, June 23, 2003 ("…many technology executives and legal experts applaud the bold attempt to crack down on identity theft, one of the fastest growing crimes."); Susan Schrock, *Police Offer Some Simple Steps to Prevent Identity Theft*, FORT WORTH STAR-TELEGRAM, August 23, 2003, at 8.

[2] Synovate, *Federal Trade Commission – Identity Theft Research Report* at 12 (September 2003), *available at* http://www.ftc.gov/os/2003/09/synovatereport.pdf (last visited March 29, 2004). The survey was commissioned by the FTC and conducted by Synovate, a Virginia research firm through interviews with 4,037 randomly selected consumers.

[3] *Id* at 18.

[4] *Federal Trade Commission Overview of the Identity Theft Program, October 1998-September 2003* at 1 (September 2003), *available at* http://www.ftc.gov/os/2003/09/timelinereport.pdf (last visited March 29, 2004).

Identity theft carries massive costs for consumers. The FTC survey estimates that identity theft cost consumers $5 billion in out-of-pocket expenses from 1998 through 2003.[5] But the costs to business were far greater. Consumer fraud cost businesses and financial institutions nearly $48 billion during this period.[6] Consequently, businesses and financial institutions have a special incentive to create ways to prevent consumer fraud, particularly in the context of retail transactions. As businesses process more consumer transactions with checks and credit cards, the risk for fraud continues to increase.[7]

The primary problem in non-cash transactions is authentication. Traditionally, the consumer's identity has been authenticated using two authenticators: (1) something the consumer possesses (instrument authentication) and (2) something the consumer knows (knowledge authentication). In some cases, a merchant or financial institution will rely solely on instrument authentication. For example, when a consumer pays a merchant by bank draft, the merchant requires the consumer to provide instruments, such as a bank check and a form of identification, to demonstrate that the consumer is an authorized payer on the account. In other cases, a merchant or financial institution will rely solely on knowledge authentication. For instance, when a consumer applies for a credit card through the mail, the financial institution requires the consumer to provide identifying information (e.g., name, address, date of birth, social security number). Likewise, most web-based transactions verify identity by using knowledge authentication. The user

---

[5] *Federal Trade Commission—Identity Theft Research Report*, *supra* note 2, at 6.

[6] *Id*. at 7.

[7] On November 14, 2001, the Federal Reserve Board released data showing American consumers use checks and electronic payments to conduct 80 billion transactions annually. In 1979, the number of non-cash payments was only 37 billion. Federal Reserve Board, *Press Release*, *available at* http://www.federalreserve.gov/boarddocs/press/general/2001/20011114/default.htm (last visited March 29, 2004).

enters a credit card number, account number and/or some other identifying information and the transaction proceeds. Finally, a merchant or financial institution may rely on a combination of instrument and knowledge authentication. An example of this is a consumer making a purchase with a debit card: the merchant requires the consumer to present a valid debit card (instrument authentication) and enter a valid personal identification number ("PIN") (knowledge authentication).

Unfortunately, instrument and knowledge authentication can be extremely unreliable. Accordingly, it is possible, utilizing modern advanced computer technology, to defraud by forging bank drafts, identification documents, and other instruments. Likewise, if a third party obtains key identifying information about a consumer, he can open bank accounts and charge accounts in the consumer's name.[8]

For this reason, merchants and financial institutions have begun to focus more attention on a third form of authentication: biometric authentication. Instead of authenticating the consumer based on instruments or knowledge, biometric authentication bases authentication on who the consumer is. Biometric authentication identifies the consumer based on physiological and behavioral characteristics. Thus, biometric authentication is much more reliable because it does not allow for misappropriation by third parties. After all, it is a simple matter for a thief to steal a consumer's credit card or

---

[8] Consumer information seems especially susceptible to misappropriation. The FTC's website lists the following methods by which identity theft can occur: stealing records from an employer; bribing an individual who has access to the records; conning information out of a consumer or organization; hacking into a consumer's or organization's computers; rummaging through a consumer's or organization's trash (known as "dumpster diving"); posing as a landlord, employer or someone else who may have a legitimate need for, and a legal right to, the information; stealing credit and debit card account numbers as the card is processed by using a special information storage device (known as "skimming"); stealing wallets and purses containing identification and credit and bank cards; stealing mail; and completing a "change of address form" to divert mail to another location. FEDERAL TRADE COMMISSION, UNDERSTANDING IDENTITY THEFT, *available at* http://www.consumer.gov/idtheft/understanding_idt.html#1 (last visited March 29, 2004).

social security number, but it is a different matter to steal the consumer's fingerprints or retinal patterns.

Of course, biometric authentication is not a new technology. Introduced more than a century ago, fingerprint technology is perhaps the most common biometric authentication technique.[9] For decades, our criminal justice system has used a number of biometric techniques, including fingerprint analysis, blood tests, hair follicle analysis and, more recently, DNA matching, to authenticate the identity of persons. Yet, businesses have been slow to employ this technology in commercial transactions.

For centuries, the primary biometric authenticator used in the commercial context was the manuscript signature, which is still prevalent today. For instance, the payer must endorse all checks and a signature must accompany most face-to-face credit card transactions. Yet in these contexts, the manuscript signature biometric is of little value as an authenticator. In most cases, the person who reviews the signature does not have access to the "real" signature for purposes of comparison. So, when a consumer writes a check at a store, the cashier cannot verify that the signature is legitimate. In most cases, only the bank has the consumer's signature on file, and banks rarely review signatures on checks against signature cards.[10] Furthermore, even if the bank reviews a signature, only

---

[9] Ironically, it appears that the first fingerprint imprint was used in a commercial transaction. According to Chandak Sengoopta, fingerprinting can be traced to an obscure village in Bengal in 1858. Sir William James Herschel, then a member of the Indian civil service, had reached an agreement with a local businessman for supplies. Concerned that the local businessman may later attempt to renege on their agreement by repudiating his signature, Herschel required the contractor to stamp the document with a print of his left hand. CHANDAK SENGOOPTA, IMPRINT OF THE RAJ: HOW FINGERPRINTING WAS BORN IN COLONIAL INDIA (2003).

[10] "[M]any customers and law enforcement and judicial system officials are unaware of the processing changes related to signature verification that have taken place over the last decade. Some do not realize that no large banks and few, if any, small banks verify all signatures. They may also be unaware of the trend among the largest banks away from verification of random signature to a check review, which includes signature verification, of only items identified as risky." American Bankers Association,

an expert in handwriting analysis or a computer-aided analysis can discern a real signature from a passable forgery.

In the past, the high price of reliable biometric devices was the main barrier to their commercial application. However, over the last decade, the price of these devices has dropped dramatically.[11] As a result, biometric authentication will take a greater role in commercial transactions and will aid businesses and consumers in the fight against identity theft in the coming years.

II. Biometric Authentication Technologies

Recently, a number of biometric authentication technologies have emerged. Some of these technologies are too invasive for widespread commercial use: very few consumers would be willing to provide a blood sample in order to withdraw $20 from an automated teller machine ("ATM"). Nevertheless, there are other non-invasive technologies available to merchants and financial institutions.

A. Finger, thumb and palm prints

Finger and thumb print devices analyze the ridges, furrows and minutiae points on the tip of the surface of the finger or thumb. Finger and thumb print analysis is particularly reliable because each person has a unique set of ridges, furrows and minutiae points. Historically, people made fingerprints and thumbprints by applying ink and then pressing or rolling the digit across paper to create the impression. Currently, a computer can scan a person's print into memory by laser technology without ink. Several

---

Signature Verification Evolution to Exception Check Review 2 (April 2000), *available at* http://www.aba.com/NR/rdonlyres/34AE858F-09B6-11D5-AB75-00508B95258D/30733/SigVerWhitePaper.pdf (last viewed, March 29, 2004).

[11] *See* Bill Orr, *Time to Start Planning for Biometrics*, ABA BANKING J. (2000) ("Between 1993 and 1999, the average price per access point fell by more than 90%, from $6,000 to $500….").

companies have begun producing palm readers, which operate in a similar fashion to finger and thumb print devices.

Fingerprint identification is the most widely applied form of biometric authentication and has been utilized in law enforcement and security applications for decades. In the commercial realm, companies have used fingerprint authentication for transactions at the ATM, over the Internet and even in the grocery checkout line.[12] As a result of this widespread use, there is a greater variety of devices available for this kind of biometric than for any other.[13] Furthermore, increased competition in the market for these devices has caused prices to fall rapidly. A company called AuthenTec, Inc., a designer and manufacturer of biometric devices headquartered in Melbourne, Florida, has created a fingerprint sensor that costs only six dollars per unit.[14]

Not only is the price of biometric devices falling, but the social stigma of having a fingerprint taken is also decreasing. In a 1997 survey of 1,000 adults, 75% responded that they would be more comfortable submitting fingerprints for identification purposes than submitting to any other biometric authenticator.[15] The fact that over half of those surveyed had their fingerprints taken at some point in their lives underscores this growing

---

[12] *See* Jennifer Masselli, *Speeding Up the Checkout Line with Biometrics*, INFORMATIONWEEK (March 13, 2002), *available at* http://www.informationweek.com/story/IWK20020313S0060 (last visited on March 27, 2004) ("Customers at the Thrift Way supermarket in Seattle next month can speed through the checkout, using personal ID numbers and their fingerprints to authorize payment for groceries.").

[13] *See* Orr, *supra* note 11. (As of the writing of Orr's article, there were 80 firms producing fingerprint devices as opposed to just 32 firms producing voice recognition devices, 16 firms producing signature verification devices, 12 firms producing facial recognition devices, and just a handful of firms producing the other various devices).

[14] *See* John Moore, *Biometrics Get Cheaper, Smaller*, FED. COMPUTER WK., June 23, 2003.

[15] *See People Patterns: Fingerprints? No Problem*, WALL ST. J., Jan. 31, 1997.

acceptance factor. In fact, only 20% of the respondents thought that fingerprinting stigmatizes a person as a criminal.[16]

B. Hand Geometry

Hand geometry biometric devices measure the size, shape and translucence of the consumer's hand. Hand measurements are unique for each individual, but they are not as distinctive as fingerprints. A few people in every 1,000 have similar-sized hands.[17] Nevertheless, scientists have developed this technology because individuals can easily damage their fingerprints. For instance, individuals can inadvertently alter the ridges and furrows of their fingertips by dipping them in corrosive chemicals, some of which exist in common household cleaning solutions. In addition, registering fingerprints for people with chronically dry skin can be difficult.

For these reasons, hand geometry readings may be better suited to some applications since the size, shape and translucence of an adult's hand are less likely to change over time. The major limitation of hand geometry is that people cannot use hand geometry as a sole authenticator. Still, hand geometry is useful in many situations as a secondary or tertiary authenticator. Currently, organizations use hand geometry devices primarily in closed-end applications, such as permitting access within an organization to facilities or data.

---

[16] *Id*.

[17] *See* James L. Wayman, *Fundamentals of Biometric Authentication Technologies*, INT'L J. OF IMAGE AND GRAPHICS, Vol. 1, No. 1 (2002) at 93, 95.

In a related development, some companies have produced devices that measure the vein pattern on the back of a person's hand.[18] Although some believe this vein pattern to be unique to each person, there are problems in measurement. For instance, veins dilate and contract over time due to aging and temperature changes.

C. Retina and Iris Scans

Retina scan technology maps the capillary pattern of the retina, a thin (1/50th inch) nerve on the back of the eye. A retina scan measures patterns at over 400 points, compared to just 30-40 distinctive minutiae points measured in a fingerprint scan. Consequently, a retina scan is one of the most accurate forms of biometric authentication.

Unfortunately, a retina scan is also the most intrusive biometric authentication method. To enroll, subjects must submit to a series of five retinal scans. Subjects must keep their head and eye motionless within one half inch (½") of the device, focusing on a small rotating point of green light. The entire process takes 45 seconds, and understandably, many people are uncomfortable with placing their eye in close contact with the device for such a long period. Furthermore, due to their complexity, retina scanning devices are at the high end of the cost spectrum. Therefore, organizations use retina scans primarily for authentication in high-end security applications to control access, for example, in government buildings, military operations or other restricted quarters, to authorized personnel only.

Despite their high costs, retina scanning devices do have a commercial use. In fact, Japanese banks have been using retina scans to authorize ATM transactions since

---

[18] Bob Carter, *The Present and Future Sate of Biometric Technology*, Address at CardTech/SecurTech '94 (April 11, 1994).

the mid 1990s.[19] While the introduction of these devices in U.S. consumer transactions has been slow, a related technology is showing promise: iris recognition technology.

The unique pattern and characteristics in the human iris form at six months of age and remain unchanged throughout one's lifetime. Some believe that no two persons in the world share the same iris pattern. Iris scanners analyze the patterns of color and texture of the iris using a conventional camera that requires no close contact with the user's eye. As a result, iris scanning is far less intrusive than retina scanning. However, iris recognition technology is relatively new and correspondingly expensive. Currently, its most common uses are, like the retina scan, in high-end security applications. Yet like retina scanning devices, iris recognition devices have also made their way into bank ATMs.

D. Facial Recognition

The primary benefit to using facial recognition as a biometric authenticator is that people are accustomed to presenting their faces for identification. People are "authenticated" in this manner every time they are asked to present a photo ID when making a credit card purchase or writing a check. The clerk authenticates people's identity by comparing their faces to the picture on the ID card. The clerk could use a facial recognition device for the same purpose, yet the clerk would not require the consumer to present a picture ID because the authenticating device would have access to a pre-existing photo of the consumer's face.

Another advantage of facial recognition as a biometric authenticator is that it is non-invasive. Organizations can operate facial recognition devices from a considerable

[19] *See* Orla O'Sullivan, *Biometrics Comes to Life*, A.B.A. BANKING J., January 1997 at 31.

distance from the subject. Far enough, in fact, that the subject is not required to present himself willingly for identification. For these reasons, this technology has become popular with law enforcement. In June 2001, Tampa, Florida became the first city to employ Visionics Corp.'s FaceIt™ facial recognition technology to photograph pedestrians in an attempt to identify and capture wanted criminals.[20] Additionally, airports in Boston, Dallas and West Palm Beach began using this technology to conduct surveillance on everyone at the airport in the aftermath of September 11, 2001.[21] Security officials employed the technology to scan the crowds in attendance at the Superbowl in New Orleans in January 2002.[22] Despite several early setbacks,[23] the technology still holds promise for the future.

The biggest hurdle in developing facial recognition algorithms is that the human face changes dramatically because of the aging process. Additionally, people can alter their faces in the short-term. A woman can drastically alter her appearance with makeup,

---

[20] *See* Dibya Sarkar, *Can a Picture Catch a Thousand Criminals?*, FED. COMPUTER WK., August 6, 2001, *available at* http://www.fcw.com/civic/articles/2001/aug/civ-comm1-08-01.asp (last visited March 29, 2004). In the Tampa program, police monitored a 16-square-block area using 36 cameras to scan and evaluate the images of passersby. Images captured on camera were matched against a database containing 30,000 images of sexual offenders, people with outstanding felony warrants, and runaway children and teens.

[21] *See* Ken Bell, *At DFW, the Eyes of Texas are Upon You*, THE AUSTIN REV., February 22, 2002, *available at* http://www.austinreview.com/articles/2002_02/dfw.htm (last visited March 29, 2004).

[22] *Id*.

[23] *See* Richard Willing, *Airport Anti-terror Systems Flub Tests*, USA TODAY, September 1, 2003, *available at* http://www.usatoday.com/tech/news/technicalinnovations/2003-09-02-faces-anti-terror_x.htm (last visited March 29, 2004). After a two-year test, police in Tampa shut down their face-recognition cameras because the cameras had not made any matches during the two-year test period. Similarly, Virginia Beach did not report a single match in a year of using a similar system. Furthermore, two separate face-recognition systems at Boston's Logan Airport failed many times to detect potential terrorists, played by volunteers, as they passed security checkpoints. The systems, however, correctly identified them 153 times.

colored contact lenses, and a different hairstyle. A man can use these same techniques, but a man can also grow facial hair to obscure his appearance. For this reason, facial recognition algorithms generally concentrate on measuring the relative position of ears, noses, eyes and other facial features. Of course, even these features can be altered through plastic surgery. Nevertheless, facial recognition technology holds great promise for the future of biometric authentication.

E. Voice Verification

Voice verification is one of the least intrusive of all biometric methods because few things in life are more natural than talking. Furthermore, voice verification is easy to use and does not require a great deal of user education. To enroll, the user speaks a given pass phrase into a microphone or telephone handset. The system then creates a template based on numerous characteristics, including cadence, pitch, tone, and shape of larynx. Typically, the enrollment process takes less than a minute for the user to complete.

Unfortunately, a number of technological and biological difficulties beset voice verification authentication. For one, voice verification programs perform poorly if the transmission quality is poor or there is ambient noise. Furthermore, the human voice changes with age and sometimes changes for a short while: if the speaker is suffering from a cold, the voice sounds different. Finally, voice recognition programs can be easily tricked by skillful impersonators or by someone who makes a prior recording of the subject's voice.

Nevertheless, voice verification has found a place in the mix of biometric authentication techniques. This is particularly true for telephone-based commercial

applications. In addition, as many computers have built-in microphones, the possibilities exist for authenticating web-based transactions using voice verifications.

F. Signature Recognition and Keyboard Dynamics

As discussed earlier, one of the most common, yet flawed, biometric authenticators is the manuscript signature. New devices that measure the biometric signature process in a non-obvious way are boosting the reliability of this form of authentication. When the user signs his name on an electronic pad, rather than merely comparing signatures, the device instead compares the direction, speed and pressure of the writing instrument as it moves across the pad.

Interestingly, the same biometric process is being used to measure the timing and rhythm of a person's typing on a keyboard. The concept is that each person's typing has a distinctive pattern. The user enrolls by typing the same word or words a number of times. Then, to authenticate their identity, the authenticator asks the user to type this particular word or words and the comparison is made. This technology holds promise for companies attempting to authenticate identities over the Internet.

G. Alternative Techniques

Recently, researchers have begun to consider additional biometric measures for authentication, such as a person's gait, sweat pores and even body odor.[24] It seems that so long as the biometric information is unique to each person measurable and reliable, technology can be developed to use it as an authenticator.

III. Enforceability of Biometric "Signatures"

[24] *See* John Moore, *Scents and Sensibility*, FED. COMPUTER WK., June 23, 2003, *available at* http://fcw.com/fcw/articles/2003/0623/cov-side1-06-23-03.asp (last visited March 29, 2004).

Biometric authentication is not a new idea. For decades, people have envisioned the benefits that would accrue from employing secure biometric authenticators. However, businesses and financial institutions have been slow to adopt these devices in consumer transactions, in part, because of the unpredictable legal environment governing these transactions. There has been some question as to whether contracts entered into by a biometric authentication device are enforceable in a court of law.

Historically, the manuscript signature was the only legally-enforceable biometric authenticator. Many transactions were unenforceable unless one or both parties manually signed a written document.[25] Moreover, even for those transactions not subject to the writing requirement, a written document was often the best way for the parties to demonstrate the terms of the agreement in court. If the document affixed a manual signature, then courts presumed that the signing party agreed to the terms specified in the document. Absent any other factors that would invalidate the contract, such as fraud, forgery, unconscionability, or public policy considerations, the contract would be enforceable against the signor.

Based on reasons stated above, the manuscript signature is a relatively unreliable authenticating form. People can forge signatures and, in most cases, the signature is not authenticated until long after the transaction's completion. In fact, signature authentication usually only occurs after a claim of fraud. By then, it is usually too late. The dishonest third-party has already fraudulently obtained goods, services, or money from the vendor or financial institution.

---

[25] For instance, the Statute of Frauds requires that a contract for the sale of real estate is invalid unless signed by both parties. Likewise, the statute requires that a personal guaranty must be signed by the guarantor to be enforceable. In addition, there are literally thousands of federal, state and local laws requiring that certain transactions be documented in writing and signed by one or more parties.

However, in order for businesses to switch to more reliable biometric authenticators, they first needed assurance that these biometric "signatures" would be afforded the same legal weight as a manuscript signature.[26] This assurance started in the legal arena in 1999,[27] when the National Conference of Commissioners on Uniform State Laws ("NCCUSL") adopted the Uniform Electronic Transactions Act ("UETA"). In 2000, Congress passed the federal equivalent of UETA: the Electronic Signatures in Global and National Commerce Act ("E-SIGN").[28] As of this writing, 43 states have adopted the UETA.[29]

Around the same time, Europe enacted similar legislation. In 1999, the European Union ("EU") adopted the Electronic Signatures Directive.[30] The following year, the EU

---

[26] Of course, in many contexts, it would be possible to retain the manuscript signature and simply add a second biometric authenticator to the process. This would satisfy the legal requirement for manuscript signatures and address the business' need for a more secure authenticator. However, the increasing popularity of electronic commerce made this solution unworkable in many contexts. As a result, the need arose for a more robust solution to the enforceability problem.

[27] Of course, consumers were conducting electronic transactions long before 1999. Nevertheless, these transactions were usually backed by manually signed documents. For instance, well prior to 1999, a consumer could pay for an airline ticket over the telephone without the need to sign a receipt. This type of transaction was enforceable because the consumer had previously signed a contract with the credit card issuer providing for such transactions. In a later dispute between the issuer and the consumer over the charges, the issuer would be able to produce a signed agreement. However, prior to 1999, it was questionable whether a credit card issuer could issue a credit card via the Internet and enforce its rights against the consumer under an electronic agreement that the consumer had never manually signed.

[28] Pub. L No. 106-229, 114 Stat. 464 (2000) (codified as 15 U.S.C. §§ 7001-7006, 7021, 7031) (enacted S. 761). For a full text of the final bill, see the Congressional web site: http://thomas.loc.gov/home/thomas.html and search for S. 761.

[29] *See E-Transaction Law Resources Legislation, Regulation and Policies—By U.S. State*, *available at* http:// www.bakernet.com/ecommerce/legis-t.htm (last visited on March 29, 2004).

[30] Official Journal of the European Communities, Directive 1999/93/EC of 13 December 1999 on a Community Framework for Electronic Signatures, *available at* http://europa.eu.int/information_society/topics/ebusiness/ecommerce/8epolicy_elaw/law_ecommerce/legal/documents/1999_93/1999_93_en.pdf (last visited on April 13, 2004).

adopted the Electronic Commerce Directive.[31] Both of these directives allow for electronic signature enforceability throughout Europe. In 1996, the United Nations Commission on International Trade Law ("UNCITRAL") Working Group on Electronic Commerce developed its Model Law on Electronic Commerce.[32] Five years later, in 2001, it finalized and approved its Model Law on Electronic Signatures.[33] This Model Law forms the basis for the enforceability of electronic signatures in several countries.[34]

In the United States, the UETA and E-SIGN have paved the way for biometric authentication enforceability by giving electronic records and electronic signatures the same force and effect as the manuscript signature in most business transactions.[35] However, the unique relationship between UETA and E-SIGN is complicated. Even

---

[31] Official Journal of the European Communities, Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 (Directive on electronic commerce), *available at* http://europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf (last visited on April 13, 2004).

[32] *See* UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE WITH GUIDE TO ENACTMENT (1996), *available at* http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm (last visited on March 29, 2004).

[33] *See* UNCITRAL MODEL LAW ON ELECTRONIC SIGNATURES WITH GUIDE TO ENACTMENT (1996), *available at* http://www.uncitral.org/english/texts/electcom/ml-elecsig-e.pdf (last visited on March 29, 2004).

[34] *See* Thomas J. Smedinghoff, *The Legal Requirements for Creating Secure and Enforceable Electronic Transactions* at 5, *available at* http://www.imf.org/external/np/leg/sem/2002/cdmfl/eng/smedin.pdf (last visited on March 29, 2004)

[35] Interestingly, rather than stating this proposition in the affirmative, each act states instead that a transaction cannot be denied enforceability simply because it is in electronic form. For instance, UETA states, "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form." UETA § 7(a), *available at* http://www.law.upenn.edu/bll/ulc/uecicta/uetast84.htm (last visited March 29, 2004). Likewise, E-SIGN states, "a signature, contract or other record relating to [a] transaction … may not be denied legal effect, validity, or enforceability solely because it is in electronic form." E-SIGN, 15 U.S.C. § 7001(a).

though the laws are significantly similar, they do differ in a few key respects. Since E-SIGN is federal law, one might expect that E-SIGN preempts any inconsistent provision in a state UETA. However, E-SIGN specifically allows for state law to "modify, limit or supercede" portions of E-SIGN in certain circumstances.[36] Therefore, for purposes of this article, it is necessary to discuss the requirements of both UETA and E-SIGN.

Under both laws, there are a number of basic requirements necessary to ensure enforceability of electronic transactions, regardless of whether any form of biometric authentication is used. First, all parties must agree to conduct the transaction electronically.[37] Secondly, all parties must have access to an electronic record of the transaction and must also have the ability to store or print a copy of that record.[38] Thirdly, all records must be retained in such a way as to protect their accuracy.[39] Finally, to be enforceable against one of the parties, the electronic agreement must be electronically "signed" by that party.

Under both E-SIGN and UETA, an "electronic signature" is defined as any sound, symbol or process made with the intent to sign the electronic record.[40] For instance, typing your name at the end of an e-mail message can qualify as an electronic signature.

---

[36] For a complete discussion of the differences between E-SIGN and UETA and the preemption issue arising therefrom, s*ee* Gail Hillebrand and Margot Saunders, *E-Sign and UETA: What Should States Do Now?, available at* http://www.consumersunion.org/finance/e_sign.htm#_ftn1.

[37] UETA § 5(b).

[38] UETA § 8; 15 U.S.C. § 7001(e).

[39] 15 U.S.C. § 7001(d)(3) (providing that if records are stored in such a way that they (i) accurately reflect the information set forth in the record and (ii) remain accessible for later reference, then these records will satisfy any rule of evidence that requires the record to be retained in its "original" form).

Likewise, pressing the "#" key when prompted by a telephone message may also qualify as an electronic signature. Furthermore, supplying a password, a PIN or a "digital signature" created through the use of public key cryptography may qualify as an electronic signature.

Significantly, while not explicitly stated in the statutes, under both E-SIGN and UETA, supplying a biometric-identifier, such as a voiceprint, thumbprint, or retinal scan, can qualify as an electronic signature.[41] Additionally, under the European Union Electronic Signature Directive, biometric identifiers qualify as electronic signatures. Therefore, in domestic and international transactions, biometric identifiers have the same legal force and effect as the traditional manuscript signature.[42] Because of the high reliability of biometric-identifiers, it is arguable that they have greater legal force and effect.

Furthermore, it is important to understand that an agreement (whether signed manually or electronically) is only enforceable against a party to the extent that the party knowingly entered into the agreement. Thus, if the agreement was forged by a third party, then the agreement would be invalid. For this very reason, despite the fact that electronic signatures can be created in a number of ways, not all electronic signatures are created equal.

For instance, some forms of electronic signatures are more reliable in identifying the true "signor." An electronic signature obtained by requiring the consumer to click on an "I Accept" button on a web page does little to lend authenticity to the transaction. By

---

[40] UETA § 2(8); 15 U.S.C. § 7006(5).

[41] *See* Smedinghoff, *supra* note 34, at 23.

[42] *Id.*

fulfilling these limited requirements, the user has not necessarily proven that he or she is who they claim to be, rather they have simply proven an ability to "point and click." Understandably, this is not a particularly unique identifier among people. A merchant or financial institution depending solely upon this form of electronic signature would find it very difficult to enforce an electronic agreement against the consumer.

On the other hand, electronic signatures obtained by requiring the user to input a password or PIN are more reliable than having the user, for example, press "#" on a telephone key pad. Even so, passwords and PINs are not the most reliable electronic signatures. After all, there is no realistic way for the merchant or financial institution to determine whether the transaction is being authorized by the true consumer or by an imposter in possession of the consumer's password or PIN.

It is for this very reason that biometric authentication holds so much promise for vendors and financial institutions. While a third party can click "I Accept" or even steal a consumer's password, it is nearly impossible for a third party to steal the consumer's thumbprint or retinal patterns. Thus, biometric authentication provides for the greatest presumption of the validity of the transaction. And given that the legal hurdle of enforceability has been removed from these transactions, merchants and financial institutions will likely rush to obtain secure electronic signatures, even where the consumer is available to provide the traditional manuscript signature.

IV. The Privacy Hurdle

While the legal enforceability of biometric authentication is well established, there are still significant privacy concerns posed by this technology. For some Americans, the thought of providing a retinal scan or thumbprint to purchase groceries

conjures up dystopian images of George Orwell's *1984*. Furthermore, many consumers are concerned about the dissemination of their personal information. In fact, in a January 2000 Wall Street Journal/NBC poll, Americans ranked the loss of privacy as their primary concern about the 21st century.[43]

As a result, federal and state governments have passed laws to address these privacy concerns. In 1999, Congress passed the Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act ("GLB").[44] This sweeping piece of legislation removed many of the restrictions on banks and other financial institutions, allowing them to merge with insurance companies and to enter the securities market. Nevertheless, most people identify GLB with its consumer privacy provisions. The stated purpose of these provisions is to ensure that financial institutions respect the privacy of their customers and protect the security and confidentiality of nonpublic personal information[45] collected when an individual obtains a financial product or service.[46] For purposes of this Act, this protected information includes even publicly available information if the grouping of that information discloses nonpublic personal information.[47] For instance, a list of names, addresses and phone numbers of a credit card company's cardholders is nonpublic information even if one can find in the local telephone directory a list of all of the names, addresses and phone numbers can. The

---

[43] *Your Best Defense Against Big Brother: You*, WALL ST. J., Jan. 24, 2000, at A27.

[44] Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq.*

[45] 15 U.S.C § 6809(4)(A) (2003) (defining nonpublic personal information).

[46] § 6801(a).

[47] 15 U.S.C. § 6809 (4)(c).

rationale is that the credit card company is telling the recipient something nonpublic about the consumer; namely that the person has a credit card with the issuer.

For purposes of GLB, the definition of a "financial institution" encompasses more than just traditional institutions such as banks, thrifts, savings and loans, mortgage lenders, credit card issuers, brokerage houses and insurance companies. In fact, a financial institution is any entity engaged in financial activities as described in Section 4(k) of the Bank Holding Company Act of 1956.[48] However, due to the wide range of activities defined as "financial in nature" under Section 4(k), the definition of financial institution includes a broad spectrum of businesses.[49] Some commentators have suggested GLB covers any of the following entities: personal property appraisers, real estate appraisers, career counselors for employees in financial occupations, courier services, real estate settlement service providers, and manufacturers of computer software and hardware.[50] In particular, retail sellers of goods are treated as "financial institutions" if they extend credit or assist customers in obtaining credit.[51]

Under the GLB, financial institutions must:

1) Notify consumers of the institution's privacy policies;[52]

2) Give the consumer an opportunity to "opt-out" of certain information sharing by the institution;[53]

---

[48] *See* 12 U.S.C. § 1843 (k) (2003).

[49] *See id*.

[50] *See, generally*, Jeff Arouh, *Gramm-Leach-Bliley Has Long Reach*, NAT'L RELOCATION & REAL ESTATE MAGAZINE (June 18, 2002).

[51] 15 U.S.C. § 6809(3) (2003).

[52] § 6803.

3) Refrain from sharing account access information with third parties for marketing purposes;[54] and

4) Provide safeguards to protect a consumer's personal information.[55]

Upon entering into a customer relationship, the financial institution is required to provide the consumer with a written or electronic notice of its privacy policy.[56] In this notice, the financial institution must disclose how it: (1) shares the nonpublic personal information of its current and former customers with affiliates and nonaffiliated third parties and (2) protects such customer information.[57] For financial institutions engaged in long-term relationships with their customers (e.g., mortgage lenders, brokerage firms, insurers, etc.), this notice must be given on an annual basis.[58]

For financial institutions that share customer information with third parties for marketing purposes, institutions must give the customer an opportunity to opt-out of this information sharing.[59] However, the customer does not have the right to opt-out of all information sharing. For instance, the financial institution may share the customer's information with third parties engaged in necessary processing or customer service

---

[53] § 6802(b).

[54] § 6802(d).

[55] § 6801(d).

[56] § 6803.

[57] § 6803(a).

[58] *Id*.

[59] § 6802(b)(1).

functions.[60] Likewise, institutions may disclose the information if it is required to prevent fraud, report transactions to a credit-reporting agency, or comply with the law.[61] Finally, even if the consumer opts out of information sharing for marketing purposes, the financial institution may still share this information with affiliated parties in an effort to cross-sell services because the opt-out provisions of the Act only apply to financial institutions who share information with "nonaffiliated third parties."[62] The Act defines a "nonaffiliated third party" as "any entity that is not an affiliate of, or related by common ownership or affiliated by corporate control with, the financial institution, but does not include a joint employee of such institution."[63] Thus, the credit card arm of a financial services conglomerate could transfer data to the home mortgage arm of the conglomerate to solicit credit card customers to consolidate their debt into their home mortgage obligation.

Furthermore, a financial institution may share the customer's personal information with a third party for marketing purposes, in direct defiance of the customer's election to opt-out of such sharing, if the financial institution has entered into a joint marketing agreement with a third party.[64] The institution must disclose this agreement in the privacy notice.[65] The privacy notice need not specifically name the

---

[60] §§ 6802(e)(1)(A)-(B).

[61] §§ 6802(e)(3), (6), (8).

[62] § 6802(b)(1).

[63] § 6809(5).

[64] § 6802(b)(2).

[65] *Id*.

third parties that have entered into joint marketing agreements with the financial institution.[66] It is enough for the institution to make a blanket statement that the institution potentially might share the customer's personal information with third parties pursuant to joint marketing agreements. Furthermore, in the agreement, the third party must agree to use the shared information solely for purposes of joint marketing.[67]

Another requirement imposed by GLB is that financial institutions may not share account access information with non-affiliated third parties for marketing purposes.[68] This is true even if the third party is subject to a joint marketing agreement. Account access information includes account numbers, access codes, etc.[69]

Finally, GLB requires all financial institutions to employ administrative, technical, and physical safeguards to:

(1) Insure the security and confidentiality of customer records and information;

(2) Protect against any anticipated threats or hazards to the security or integrity of such records; and

---

[66] *Id*.

[67] *Id.*

[68] § 6802(d).

[69] *Id*. (stating that "[a] financial institution shall not disclose, other than to a consumer reporting agency, an account number or similar form of access number or access code for a credit card account, deposit account, or transaction account of a consumer to any nonaffiliated third party for use in telemarketing, direct mail marketing, or other marketing through electronic mail to the consumer.").

(3) Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[70]

This requirement appears to be an open invitation for the use of biometric authentication in consumer transactions. After all, the most secure method of controlling unauthorized access to records of personal information is to authenticate the identity of the recipient based on whom the person is, as opposed to authentication based on what the person possesses or knows.

Nevertheless, despite the progress for consumer privacy represented by GLB, many privacy advocates are disappointed in the Act.[71] This disappointment stems from two sources. First, GLB requires consumers to make the effort to opt-out of information sharing. Some believe that, instead, consumers should have to make an affirmative choice to have their information shared with third-party marketers ("opt-in").[72] Second, the joint marketing agreement exception to information sharing allows financial institutions to perform an "end run" around the restrictions on information sharing. So long as the financial institution has entered into a joint marketing agreement, it can share nonpublic personal information with third parties.

---

[70] § 6801(b).

[71] *E.g.*, Electronic Privacy Information Center, *The Gramm-Leach-Bliley Act*, *available at* http://www.epic.org/privacy/glba/ (last visited March 29, 2004).

[72] *Id.*

For these reasons, many states have enacted their own privacy measures.[73] These laws are permissible under GLB, which does not preempt any state law granting greater privacy protections, so long as the law is consistent with GLB.[74] In June 2002, North Dakota residents passed a referendum requiring that consumers in the state must opt-in to information sharing. In Vermont, the state's Department of Banking, Insurance, Securities, and Health Care Administration adopted opt-in provisions for information sharing.[75] Moreover, state legislators have passed laws requiring some form of opt-in consent in Alaska,[76] Connecticut,[77] Illinois,[78] and Maryland.[79]

Perhaps the most interesting state battleground for privacy advocates has been in California. In 2001 and 2002, the state legislature failed in its efforts to pass "opt-in" privacy legislation.[80] Nevertheless, San Mateo County, Contra Costa County, Alameda County and Daly City each passed a local ordinance requiring "opt-in" for information

---

[73] California has enacted 40 new privacy initiatives since 1999. *See* Financial Services Privacy Collection website, *at* http://www.caprivacyprotection.org/laws_californialaws.html (last visited on March 29, 2004).

[74] 15 U.S.C. § 6807 (2003).

[75] *See* Patrick Thibodeau, *New Vermont 'Opt-in' Privacy Law Faces Legal Challenge*, Computerworld, *at* http://www.computerworld.com/databasetopics/data/story/0,10801,68104,00.html (last visited March 27, 2004).

[76] *See* ALASKA STAT. § 06.05.175 (Michie 2003).

[77] *See* CONN. GEN. STAT. §§ 36a-42 (2003).

[78] *See* 205 ILL. COMP. STAT. ANN. 5/48.1 (West 2003).

[79] *See* MD. CODE ANN. § 1-301 (2003).

[80] Ann Marimow, *Data Legislation Sputters*, *available at* http://www.siliconvalley.com/mld/siliconvalley/news/3521921.htm (last visited March 29, 2004).

sharing. In addition, some state legislatures are considering bills that deal specifically with the sharing of biometric information. For instance, legislators have introduced bills in California,[81] Massachusetts,[82] and New Jersey[83] to regulate the collection and distribution of biometric information. These bills would have prevented merchants and financial institutions from collecting biometric information without the consent of the consumer. They would have also prevented the recipient from disclosing the information to third parties other than law enforcement and other rightful parties, or using the information for any purpose other than identification. While legislatures failed ultimately to pass any of these bills, the trends suggest that it is likely that legislators will introduce similar state bills in the near future with success.

On the other hand, the European Union has taken a slightly different approach to the issue of consumer privacy. On October 25, 1998, the European Union Data Protection Directive (the "EU Directive")[84] took effect. The key provisions of the EU Directive are:

(1) Limitations on the collection, use and storage of personal information;[85]

---

[81] S.B. 71, 1999-00 Leg., Reg. Sess. (Cal. 1999) (the bill failed in the Judiciary Committee).

[82] H.B. 4483, 181st Gen. Ct., 1999 Reg. Sess. (Mass. 1999) (the bill passed just one house).

[83] The Biometric Identifier Privacy Act, AB 2448, Leg., 210th Sess. (passed in the Assembly, September 23, 200, received in the Senate, and referred to the Senate Judiciary Committee, September 26, 2002).

[84] Data Protection Directive, Council Directive, 95/46/EC, 1998.

[85] Under the EU Directive, data must be collected for specified, legitimate purposes and kept no longer than necessary to fulfill the stated purpose. Council Directive, 95/46/EC, Art. 3.

(2) Transfer restrictions;[86]

(3) Special protections for sensitive data;[87]

(4) The creation of an independent public authority to oversee personal data protection in each EU member state;[88]

(5) The appointment of a registered "data controller" within each business organization;[89] and

(6) Remedies for consumers.[90]

The EU Directive is more demanding for financial institutions than GLB. Moreover, the EU Directive restricts international transfers of personal information into countries that do not place adequate safeguards on the collection and use of personal data.[91] Due to the relative weakness of GLB, many transnational businesses were concerned that the European Directive would prevent the transfer of personal data into the U.S. However, on March 17, 2000, EU-US negotiators approved an agreement

---

[86] Authorized users of personal information may only transfer personal information to third parties with the permission of the individual providing the data or the data subject. In the case of international data transfers, the EU Directive prohibits transfers outright to any country lacking an "adequate level of protection" for personal information, as determined by the EU. Council Directive, 95/46/EC, Art. 25.

[87] The collection and processing of information identifying "racial or ethnic origin, political options, religious or philosophical beliefs … [or] concerning health or sex life" is generally forbidden and subject to special government scrutiny. Council Directive, 95/46/EC, Art. 8.

[88] Council Directive, 95/46/EC, Art. 28.

[89] Council Directive, 95/46/EC, Art. 10.

[90] Council Directive, 95/46/EC, Art 22; *see also* Council Directive, 95/46/EC, Art. 7. Under the EU Directive, a data subject has the right to: (1) access information about himself; (2) correct inaccuracies; and (3) object to the organization's use of the information.

[91] Council Directive, 95/46/EC, Art. 25.

featuring "safe harbor" principles by which U.S. organizations can receive such international data transfers.[92] Under this safe harbor, so long as the U.S. business provides data subjects with notice as to the purpose of the data collection, allows data subjects to opt-out of information sharing and permits information access to data subjects, European companies can transfer personal information to U.S. businesses.[93]

Of course, the main thrust of GLB, its state law equivalents and the European Directive is to protect the consumer from the unauthorized disclosure of the consumer's personal information to third parties. In the context of biometric information, the provisions of GLB (and the European Directive, to the extent it applies) are sufficient to protect consumers. For one, GLB prevents financial institutions from disclosing account access information to third parties under all circumstances. Therefore, if the institution collects biometric identifiers for account access purposes, then GLB protects the consumer from any dissemination of this information.[94] Second, at present, there is not a great demand by marketers for biometric information. For instance, there should be little concern that financial institutions and others will start selling their customer's thumbprint images to say, glove manufacturers.[95] The main use for biometric information is account

---

[92] U.S Department of Commerce Export Portal, *Safe Harbor Principles* (July 21, 2000*), available at* http://www.export.gov/safeharbor/ENFORCEMENTOVERVIEWFINAL.htm (last visited March 29, 2004).

[93] *Id.*

[94] Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(d) (2003).

[95] Ironically, one of the most disturbing privacy concerns is not addressed by GLB or its state alternatives – the government's use of a citizen's financial information to track her movements or whereabouts. In fact, GLB and most state laws specifically allow for the financial institution to make disclosures to the government. See 15 U.S.C. § 6802 (e)8. Furthermore, in the wake of 9/11, Congress has passed the Patriot Act and other legislation giving law enforcement enhanced surveillance powers. *See* Patriot Act, 6 U.S.C. § 122(b)1-2 (2003).

access. Existing law and business sense should prevent businesses from disclosing this information to third parties.

Furthermore, the use of biometric authentication can serve as an important tool in protecting other consumer information. In fact, a survey released in January 2003 shows that Americans favor the security benefits of biometric authentication despite its privacy risks.[96] For instance, 85% of the respondents said companies should use biometrics to verify the identity of anyone making credit card purchases.[97] Likewise, 78% of the respondents said ATMs should use biometrics when an individual is withdrawing funds from the machines.[98]

While privacy concerns have diminished in some respects the wider deployment of biometric authentication devices in consumer transactions, the participants in the survey said they would be more comfortable with the use of biometrics if certain basic privacy safeguards existed.[99] Almost 90% of the respondents wanted companies to disclose if companies were collecting and storing their biometric information, and 85% of the respondents wanted some mechanism to access and verify their information.[100]

V. REGULATORY MODELS

Given the rapidly falling prices of biometric devices, the legal enforceability of agreements entered into on this basis, and the improved perception of the technology, the

---

[96] *See* Sharon Gaudin, *Poll: Biometrics Gaining Acceptance*, eSecurityPlanet.com, *at* http://www.esecurityplanet.com/trends/article.php/1566401 (January 8, 2003). This survey of more than 1,000 U.S. adults was funded by the U.S. Bureau of Justice Statistics and conducted by the Privacy & American Business newsletter.

[97] *Id*.

[98] *Id*.

[99] *Id*.

widespread use of biometric authentication is almost inevitable. It is more of an issue of "when" than "if". As a result, it makes sense to turn our attention now to creating a regulatory framework for the collection, use and dissemination of biometric information. In that regard, we have several options.

A. The Laissez Faire Approach

One possible approach to the regulation of biometric authentication is to let consumers and businesses decide for themselves how to utilize the technology. Each vendor or financial institution would be free to establish its own policy with respect to the collection, use and distribution of biometric data. The consumer could then consider this policy when making purchasing decisions. For instance, consumers who are averse to using biometric authentication could choose to patronize those businesses that depend upon the more traditional forms of authentication such as photo IDs, manuscript signatures, etc. Conversely, consumers who are concerned about identity theft could choose to patronize businesses using voice prints, thumb prints, and other biometric technologies. Moreover, consumers could make choices based upon the particular form of authentication. For example, some consumers may be willing to provide a thumbprint but not a retinal scan and vice versa.

The chief advantage to this approach is that it allows for maximum flexibility in the deployment of this burgeoning technology. As the marketplace would be the ultimate arbiter, each existing technology (and those technologies that scientists will develop in the coming years) would have a fair chance to establish itself in the marketplace. In addition, the laissez faire approach would allow for true choice amongst consumers. Unfortunately, without some form of regulation, this choice may not be particularly

---

[100] *Id*.

meaningful. Under a true laissez faire regime, no authority *requires* businesses to disclose their biometric policies to consumers.[101] Therefore, it would be difficult for customers to weigh meaningfully the alternatives.

For instance, consider the example of the fictional video rental chain, Brickbuster Video. Instead of relying on customers to present a membership card, Brickbuster decides to authenticate customer identities by the use of thumbprint scanners. In this hypothetical situation, the customer would be aware of Brickbuster's collection and use of biometric information[102] but there are no provisions under current law requiring Brickbuster to publish its policies with respect to its use and dissemination of the information.

Furthermore, even assuming that Brickbuster's customers demand to know how Brickbuster is utilizing their information, they will have little power to monitor and enforce Brickbuster's compliance with its own biometric policies. Unless a company's policy explicitly provides for audit rights, customers will not have the right to inspect the books and records of the company for compliance.[103] Perhaps the only opportunity for inspection would come because of the discovery phase of a lawsuit. However, this would

---

[101] As discussed previously, under GLB, financial institutions are required to disclose the types of information they obtain from consumers and the third parties with whom this information is shared. Moreover, financial institutions must provide consumers an opportunity to opt-out of information sharing with third-party marketers. However, even under GLB's broad definition of "financial institution," many businesses are still left unaffected by the law. *See supra* text accompanying notes 53-55.

[102] With most forms of biometric authentication, it is difficult to collect the required biometric information surreptitiously. The only form that can be used surreptitiously is facial recognition technology. However, current concerns about its reliability would likely preclude use of this technology in commercial transactions in the near future. *See supra* note 20.

[103] Under GLB, the various regulatory agencies (e.g., SEC, FDIC, FTC, etc.) are empowered to enforce the provisions of the act and therefore, they may launch their own audits and investigations of businesses under their jurisdiction. *See* Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 *et seq*.

require a consumer to form a reasonable suspicion that the company was misusing its data and, perhaps more importantly, a perception that the consumer would be entitled to significant monetary damages should such misuse be proven at trial. Therefore, while in theory the laissez faire approach would yield great benefits in terms of consumer choice, it is uncertain whether such consumer choice would be meaningful.

B. Self-Regulation

As some form of regulation is likely necessary to protect the privacy rights of consumers, the question becomes which form of regulation is most appropriate for biometric authentication. One possible answer is self-regulation. Instead of state and federal lawmakers passing legislation, industry groups could draft their own codes of consumer privacy practices. In fact, several industry groups, including the Direct Marketing Association and the Information Industry Association, have taken this approach already.[104]

The arguments for self-regulation in this context are powerful. For one, industry groups are much more agile than legislatures and can act more quickly in response to changes in technology and the business environment surrounding biometric authentication. This could be particularly helpful in the case of a relatively new industry and technology, which may change drastically in the coming years. Second, any governmental solution to the problem of consumer privacy will likely be of the "one size fits all" variety. As a result, the legislative approach will not take into account the differences between industries or between technologies. For instance, it may be entirely

[104] *See* UCAN/PRIVACY RIGHTS CLEARINGHOUSE, A REVIEW OF THE FAIR INFORMATION PRINCIPLES: THE FOUNDATION OF PRIVACY PUBLIC POLICY, *available at* http://www.privacyrights.org/ar/fairinfo.htm (last visited March 29, 2004).

appropriate to differentiate between the regulation of biometric authentication in the banking industry and the video rental industry. Moreover, it may be appropriate to establish different regulations for retinal information than for voice print information.

Though it has several advantages, self-regulation entails one major drawback: the lack of enforcement. Self-regulation is most effective in cases where the number of industry participants is relatively small. For instance, the National Association of Securities Dealers ("NASD") regulates brokers, dealers, and to a lesser extent, public companies. These industry participants make up just a tiny portion of the millions of American businesses. As a result, the regulatory activities of the NASD are manageable.[105] However, to be effective, biometric self-regulation would have to apply to any business using the technology, many of which do not belong to any self-regulatory organization. For this reason alone, self-regulation of the collection, use, and dissemination of biometric information is likely to be ineffective.

C. Federal Regulation

Of course, the alternative to self-regulation is binding legislation. Therefore, one approach would be the passage of a federal biometric privacy law. In developing such a law, Congress should be mindful not to "play favorites" concerning certain technologies or certain uses of biometric information. For instance, Congress should not pass a federal law that favors thumbprints over retinal scans or allows for the use of biometric authentication in only banking but not insurance. Any federal law regulating the still emerging technology of biometric authentication should provide only general principles for the collection, use and dissemination of biometric information.

---

[105] Although given the spate of corporate bankruptcies and financial fraud that have occurred in recent years, even this proposition is debatable.

Interestingly, GLB provides a good framework for any such legislation. GLB requires financial institutions to (1) notify customers of the types of information collected from them, (2) allow customers to opt-out from certain information sharing practices; and (3) use reasonable means to protect the confidentiality of customer data.[106] However, as discussed earlier, GLB is weak in regards to allowing the consumer to control the dissemination of her personal information.[107] Moreover, GLB does not provide a mechanism for consumers to access and verify their information.

For these reasons, the congressional enactment of a biometric privacy act should more closely model the Code of Fair Information Practices ("CFIP").[108] The CFIP came into existence in 1973 when a task force of the U.S. Department of Health, Education and Welfare analyzed the impact of computerization on medical records privacy. In its findings, the task force established five principles for the fair collection and use of personal information. These are:

(1) There must be no personal data record-keeping systems whose very existence is secret;

(2) There must be a way for an individual to find out what information is in his or her file and how the information is being used;

(3) There must be a way for an individual to correct information in his or her records;

---

[106] *See supra* text accompanying notes 53-56 & 65.

[107] *See supra* text accompanying notes 60-64.

[108] U.S. DEP'T. OF HEALTH, EDUCATION AND WELFARE, SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS, *available at* http://aspe.os.dhhs.gov/datacncl/1973privacy/tocprefacemembers.htm (last visited March 29, 2004).

(4) Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and

(5) There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.[109]

Despite the fact that these principles were drafted 30 years ago, they seem to echo the sentiment of today's consumer. For instance, in the 2003 survey discussed earlier, 90% of the respondents wanted to be fully informed that their biometric information was being collected and stored (Principle #1). Likewise, 85% of the respondents wanted some mechanism to access and verify their information (Principles #2 and #3).[110] Therefore, CFIP seems a natural starting point for a federal biometric privacy law.

In particular, any federal law dealing with the collection, use and dissemination of biometric information should incorporate the basic tenets of CFIP:

(1) Notice. The consumer must be given notice of the types of biometric information being collected and the collector's intended uses of that information;

(2) Access. The consumer should have the right to access her information in the database. Specifically, the individual must be able to discover if her biometric information is in the database;

---

[109] *See id.*

[110] *See supra* text accompanying note 97.

(3) Correction Mechanism. The consumer must be able to correct or make changes to any biometric information in the database;[111]

(4) Informed Consent. A collector of biometric information must receive prior consent from the consumer before disclosing such information to third parties (reasonable exceptions should be made for disclosures required by law).[112] By requiring consent, consumers would have to "opt-in" to information sharing[113]; and

(5) Reliability and Safeguarding. The collector must guarantee the reliability of the data and safeguard the information.[114] At its most basic level, appropriate managerial and technical controls must be used to protect the confidentiality and integrity of the data.

D. State Regulation

Alternatively, Congress could leave the protection of consumer privacy to the state legislatures, thereby granting each state the freedom to enact its own form of biometric privacy law. The chief advantage of leaving legislation to the states is that there would not be a generic approach to the protection of consumer liability. States

[111] As one of the advantages of biometrics is that it is based on physical characteristics that rarely change over time, this principle would only come into play when the consumer suspected some mistaken or fraudulent use of his information.

[112] U.S. DEP'T OF HEALTH, *supra* note 109.

[113] Of course, merchants and financial institutions could require the consumer to opt-in as a condition of doing business. However, this approach might prove risky if other competitors did not require opt-ins and used this difference as a marketing advantage.

[114] U.S. DEP'T OF HEALTH, *supra* note 109.

would enact laws, and, over time, the varying laws would be evaluated to determine which laws best protect consumers and which laws best promote innovation. Scholars call this approach the "state laboratory" theory of legislation.[115] However, since failed legislation would only affect the state enacting the legislation, this theory works best in the context of intrastate commerce.[116] In fact, considering the proliferation of interstate banking and transactions over the Internet, state regulation would likely prove unruly and potentially disastrous.

To understand the level of complexity that would result from numerous state laws, consider the following hypothetical situation. Suppose the fictional Bank of the United States begins to allow its customers to conduct banking transactions over the Internet by using voice print devices. Prior to this decision, the state of California outlawed the use of voice print devices for biometric authentication purposes. Based on these facts, Bank of the United States will be unable to offer online banking to its California customers without an alternate device that provides the same services as the voice print device. Alternatively, assume the state of Illinois allows for biometric authentication, but only if the information is encrypted in 32-bit technology. This might not be a problem except that the state of New York requires 64-bit encryption and the state of Maryland requires all biometric records to be stored both electronically and on paper. The difficulty in trying to comply simultaneously with 50 different state regulations would likely prevent Bank of the United States from employing biometric authentication over the Internet.

---

[115] Barry Latzer, *A Critique of Gardner's Failed Discourse*, 24 RUTGERS L.J. 1009, 1018 (1993).

[116] *Id*.

E. A Hybrid Approach

Due to the limitations of self-regulation and state legislative solutions to the problem of consumer privacy in biometric transactions, this article proposes federal regulation. However, federal regulation alone will not suffice. Though the GLB is limited to financial institutions, accusations of weak enforcement have plagued the Act.[117] A new federal law that regulated all businesses in addition to financial institutions would exasperate the problems of enforcement and oversight.

Under GLB, the federal government charges existing regulatory agencies to enforce the law as it applies to the companies under their jurisdiction.[118] For those companies not subject to a specific regulatory authority, the Federal Trade Commission ("FTC") retains oversight and enforcement for the remaining businesses.[119] In essence, the FTC handles all overflows.[120] If Congress passed a biometric privacy bill affecting non-financial institutions (many of which are unregulated by any agency), the FTC likely could not feasibly oversee the activities of a large majority of the vendors who fell under its charge.[121]

---

[117] On May 1, 2002, several privacy advocacy groups, including Electronic Privacy Information Center, Privacy Rights Clearinghouse, Consumer Union and US PIRG, submitted comments for a U.S. Treasury study on the effectiveness of GLB. In their comments, these groups described flaws in the implementation of the GLB. In addition, 37 state Attorneys General submitted comments stating that the "current law does not adequately protect consumers' privacy." Electronic Privacy Information Center, *The Gramm-Leach-Bliley Act*, *available at* http://www.epic.org/privacy/glba/ (last visited March 29, 2004).

[118] Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6804, 6805 (2003).

[119] § 6805(a)(7).

[120] *Id*.

[121] Furthermore, it is unlikely that Congress would establish a new federal agency solely for this purpose.

Therefore, to encourage businesses to adopt fair information practices, Congress may attempt to dangle the "carrot" of legal presumptions. In other words, if a business conducts its operations in accordance with federal law, it will not only avoid fines and penalties, but will receive favorable legal presumptions in a dispute. Conversely, if a business fails to act in accordance with federal law, it will suffer adverse legal presumptions with respect to disputes.

For example, assume that a customer complains that he did not place an order with a vendor via an Internet transaction. The vendor counters that it received a hand geometry scan from the customer at the time of the transaction and the scan matched the vendor's records for the customer. To encourage vendors to employ fair information practices, federal law could grant a legal presumption of validity to the transaction if the vendor complies with federal law governing biometric authentication. Consequently, in this hypothetical case, a compliant vendor would benefit from the legal presumption of validity.[122] This type of legal benefit, in and of itself, may provide enough of an incentive for vendors to abide by the federal law.

In fact, this type of incentive is already in place in several areas of the law to encourage security in commercial transactions. For instance, Uniform Commercial Code section 4A, which regulates electronic transfers, provides that if a bank verifies a payment order by using a commercially reasonable security procedure, then courts will enforce the order even if the customer did not authorize it.[123] In this situation, the only

---

[122] Of course, this is a rebuttable presumption. If the consumer could prove that he did not place the order (e.g., he was in a coma at the time of the transaction), then he could avoid enforcement of the contract.

[123] Uniform Commercial Code § 4A-202(b) (2003).

way for the customer to shift the loss back to the bank is to prove that the person sending the fraudulent order did not receive authorization from the customer or his agents.[124] Proving such an event is extremely difficult in most cases. In contrast, if the bank did not use a commercially reasonable security procedure, then it must cover the loss without regard to how the fraudulent payer received the information necessary to authorize the payment order.[125] As previously discussed, the Illinois Act is a good example of a law that incentivizes the use of "secure electronic signatures."[126] The Illinois Act grants transactions that use secure electronic signatures a rebuttable presumption of legal validity.[127]

CONCLUSION

With the rapidly growing incidents of identify theft and the resulting fraud, both businesses and consumers are anxious for greater security in commercial transactions. This article has shown that a very viable and effective solution to this common concern is biometric authentication. Recently, barriers to the implementation of this technology have fallen. The technology is increasingly reliable and affordable, and the nagging question of the legal enforceability of electronic contracts is settled.

The only remaining issue is how to balance the promise of greater security against the threat to personal privacy. While consumers recognize the benefits of biometric

---

[124] § 4A-203(a)(2).

[125] § 4A-202(b).

[126] 5 ILL. COMP. STAT. § 175/10-110.

[127] *Id*.

authentication, they are reluctant to fully embrace the technology without adequate assurances that companies will keep their biometric information confidential and subject to various safeguards. While existing law provides a limited measure of protection for biometric information, there must be greater protection offered to give consumers enough comfort to accept this new technology.

In evaluating the various options for the regulation of biometric authentication, this article concludes that the most promising solution is to combine a mixture of federal regulation and legal presumptions. The federal government should base legislation on the CFIP, as it provides many of the benefits that consumers are currently seeking. To encourage businesses to adopt such practices, the law should provide favorable legal presumptions to businesses that follow the legislation. This hybrid mix of federal regulation and legal incentives may finally allow businesses and consumers to realize the benefits of biometric authentication.