Static Measurements and Moving Targets: Privacy, Biometrics and the Consumer-Bank Relationship

By Dan Fingerman
January 2003

I. Introduction

It has become cliché to fret over the erosion of privacy in modern life. However, while high-tech peeping toms and businesses selling personal information engender a vague fear in many people, few can articulate precisely the nature of their discomfort.[1] Two basic philosophical approaches underlie modern notions of privacy: "personal" privacy or "intrusion upon seclusion" (the peeping tom) and "public" or "informational" privacy (information selling). One modern technology — biometrics — threatens privacy from both perspectives, which makes the nature of privacy discomfort difficult to articulate. Biometrics refers to the measurement of bodily features for the purpose of identifying individuals. For many people, the intimate measurement required for biometrics evokes the same visceral "yuck factor" as a peeping tom.[2] At the same time, the specter of strangers misusing biometric data imperils the sphere of personal information which we feel entitled to control. Some may feel betrayed simply because such technologies are being widely deployed without their knowledge. These objections to biometrics seem to emerge from Americans' checkered history in addressing the moral and ethical implications of emerging technologies. Although most of the biological knowledge underlying biometrics has existed for over a century, only the recent advent of secondary, enabling technologies has made biometric programs practical.[3] Small and fast computer processors, high-capacity storage media, and robust communications facilities have made biometric applications a practical option for many businesses and governments. The relatively sudden rise of biometric programs has caught most people off guard.

---

[1] *See e.g.*, Bill Zalud, *Security Privacy Tug-o-War*, 38 Security 10 (1 Oct. 2001) ("Zalud"); Marianne Costantinou, *Identity Politics*, San Francisco Chron. Mag. page 8 (2 March 2002) ("Constantinou"); Robyn Moo-Young, "Eyeing" the Future: Surviving the Criticisms of Biometric Authentication, 5 N.C. Banking Inst. 421 (2001) ("Moo-Young")

[2] *Biometrics: Arthur C. Clarke, Where Are You?* Future Banker, 14 (1 June 2001)

[3] Simon Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (2000), 40 ("Garfinkel")

The public and private sectors have embraced biometrics with equal enthusiasm. In the public sector, all levels of government feel biometrics' lure. Even agencies charged with such mundane tasks as administering public welfare rolls are using biometrics.[4] While the potential benefits of biometrics in law enforcement and national security are obvious, the benefits in welfare administration are much less so. John Woodward explains:

> For government agencies in the United States constantly encouraged to 'do more with less,' biometric applications can save tax dollars and make programs operate more efficiently. Government agencies are reporting impressive biometric success stories. For example, the Los Angeles County Department of Public Social Services reported that finger imaging of welfare recipients in a pilot program reduced fraud by over $14 million and resulted in the termination of over 3,000 previously-approved entitlement cases over a three year period. The savings more than paid for the $9.6 million cost of implementing biometric technology. Recognizing this and similar positive applications, the U.S. Secret Service and the [federal] General Accounting Office (GAO) gave biometrics a qualified endorsement as a viable means to deter fraud in government entitlements distributed electronically, known as electronic benefits transfer.[5]

In the private sector, the banking industry has been most receptive to biometrics and conducted some of the earliest feasibility tests.[6] In Japan, consumer banks have employed biometrics in their automated teller machine (ATM) networks since 1996.[7] In the United States, several major banks have biometric programs in various stages of development and testing. Citicorp, Bank of America, Mellon Bank, Bankers Trust, and Chevy Chase Savings and Loan

---

[4] Dana Milbank, Measuring and Cataloguing Body Parts May Help to Weed Out Welfare Cheats, Wall St. J., Dec. 4, 1995, at B1 ("Milbank")

[5] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns — Drafting the Biometric Blueprint*, 59 U. Pitt. L. Rev. 97, 97 (1997) ("Woodward") (citing United States General Accounting Office, Electronic Benefits Transfer: Use of Biometrics to Deter Fraud in the Nationwide EBT Program, GAO/OSI-95-20, Sept. 1995, at 6-7)

[6] *See e.g.*, Christine Barry, *Financial Institutions Give Biometrics A Thumbs Up*, BiometriTech (20 May 2002) (available at <http://www.biometritech.com/features/celent.htm>) ("Barry") and International Biometric Group, *White Paper on Retail, ATM, Point-of-Sale* <http://www.ibgweb.com/reports/public/reports/retail.html> (2002) ("IBG White Paper").

[7] Rajiv Chandrasekaran, *Brave New Whorl: ID Systems Using the Human Body are Here, but Privacy issues Persist*, Washington Post H01 (30 Mar. 1997) ("Chandrasekaran"); Nicholson

Association have all experimented with finger scanning.[8] Chase Manhattan Bank conducted tests of voice recognition and fingerprint scanning and found "that 95% of consumers would [consent to] voice recognition and 80% would use fingerprinting."[9] Bank United has field-tested iris scanners in its ATMs and received positive feedback from its customers.[10] At least one employee credit union has gone beyond mere testing and deployed finger scanners in its ATM network.[11] Even consumers without bank accounts are using biometric equipment in "rapid pay" machines, which permit people without checking accounts to cash checks.[12]

Some biometric technologies are familiar, while others remain exotic. Police have used fingerprints for over a century, but *Mission Impossible* thrilled moviegoers in 1996 when Ethan Hunt, played by Tom Cruise, gained access to a secure vault by forging a retinal scan. "Although for many years biometrics has been widely featured in movies and high-end government and corporate applications, it is only in the past year that the technology has caught up to the hype."[13] Anticipating an imminent explosion of demand for biometrics among governments, banks, and others, a growing cadre of technology companies is jockeying for position to sell biometric hardware and software. Their marketing literature emphasizes the low cost and versatility of biometric programs relative to traditional security measures.[14] As

---

[8] Moo-Young, 5 N.C. Banking Inst. at 423
[9] *Id.*
[10] Leslie J. Nicholson, *Iris-scanning ATMs Coming Online Today*, Dallas Morning News, 10 D (May 13, 1999) ("Nicholson")
[11] *Banks' Future Security Could Be Built on Biometrics House Banking Panel Told*, BNA Banking Daily, 21 May 1998 (describing the Perdue University employee credit union)
[12] Helen Stock, *Firm Uses Biometrics to Serve the Unbanked*, American Banker, 12 (1 Oct. 1999)
[13] Vance C. Bjorn, *An Introduction to Privacy and Security Considerations of Biometrics Technology*, 701 PLI/ Pat 105, 108 (June 2002) ("Bjorn")
[14] *See e.g.*, Sarnoff Corp., *Sensar IrisIdent® Personal Identification*, <http://www.sarnoff.com/government_professional/vision_technology/products/sensar_irisdent.asp> (accessed 1 Sept. 2002); Eye Ticket Corp., *EyeTicket Advises ICAO of Open Licensing To Industry for Iris Recognition Products* <http://www.eyeticket.com/en/releases2002.php?date=09162002b.htm> (16 Sept. 2002) (accessed 24 Nov. 2002); Identix, Inc., *Live Scan Desktop Units: FingerPrinter CMS®* <http://www.identix.com/products/pro_livescan_desktop_cms.html> (2002) (accessed 24 Nov. 2002)

competition drives down the cost of biometric equipment — consumer-grade fingerprint sensors now retail for less than $70 per unit[15] — biometric programs will only expand.

These entities are pressing biometrics without due consideration to the moral and ethical implications of the technology — let alone a general public consensus as to biometrics' usage and, if necessary, regulation. This paper addresses issues created by this void. Part II introduces several specific biometric technologies and explains how they work. Part III outlines the historical perspective through which we should view biometrics. Part IV summarizes the law of privacy with a particular emphasis on the law applying to banks that serve consumers. Finally, part V analyzes the intersection of consumer banking, biometrics, and privacy and offers suggestions for regulating the use of biometrics.

II. Biometric Technology

Part II of this paper describes biometric technology insofar as the technology is relevant to privacy policy.[16] First, it describes the four most commonly used biometric indicia and explains the advantages and shortcomings of each. Second, it introduces the two major biometric applications and gives examples of programs in each category. Third, it describes the capture, storage, and use of biometric data and introduces several specific privacy problems.

---

[15] Bjorn, 701 PLI/Pat at 108

[16] The intended audience for this paper is the legal and policymaking communities, so it does not reach all the technical detail of biometrics. For a more technical approach to biometrics, see the references cited herein and references collected in the web sites of the Biometric Consortium, <http://www.biometrics.org/>, and the International Biometric Group, <http://www.ibgweb.com/>.

A. Biometric Indicia

The International Biometric Group defines biometrics as "the automated use of physiological or behavioral characteristics to determine or verify identity."[17] Biometrics entails measurement of a bodily characteristic but not the removal of tissue.[18] While we can identify individuals from substances present in tissues and secretions, such as deoxyribonucleic acid (DNA), these are not biometric identifiers because they require collection of tissue and cannot yield results in realtime.[19] The two major classes of biometric identifiers are primary (physiological) and secondary (behavioral) indicia.[20] Primary identifiers are physical traits not separable from the body — such as fingerprints, handprints, faceprints, irises, retinas.[21] Several primary identifiers comprise non-unique elements that become unique to an individual only when considered in combination with other elements.[22] Non-unique traits serve as a reliable primary identifiers if they yield unique patterns in combination.

Secondary identifiers are nonphysiological traits such as voice, gait, and handwriting.[23] Behavioral traits are less reliable than primary identifiers for two reasons. First, individuals can consciously modify behavioral traits without the substantial deterrent of surgery or trauma required to alter primary identifiers. Second, measurement of any primary identifier requires the

---

[17] International Biometric Group, *How is 'Biometrics' Defined?* <http://www.ibgweb.com/reports/public/reports/biometric_definition.html> (accessed 25 Oct. 2002) ("IBG, *How is Biometrics Defined?*"). The International Biometric Group describes itself as a "consulting and technology services firm [which] has provided technology-neutral and vendor-independent biometric services and solutions to financial institutions, government agencies, systems integrators, and high-tech firms since 1996." International Biometric Group Home Page <http://www.ibgweb.com/> (accessed 15 Sept 2002).

[18] International Biometric Group, *Is DNA a Biometric?* <http://www.ibgweb.com/reports/public/reports/dna.html> (accessed 25 Oct. 2002)

[19] *Id.*

[20] IBG, *How is Biometrics Defined?*

[21] *Id.*

[22] The two most important examples are faceprints and retinas. I explain the details in section C.

[23] IBG, *How is Biometrics Defined?*. Handwriting as a biometric identifier includes the use of signatures. *See* Part V, *infra*, page 37 at note 196and accompanying, text for further discussion of signature matching as a biometric identifier.

physical presence of the individual, whereas some secondary identifiers may be recorded long before measurement.[24] Several companies have developed equipment that can distinguish between an actual live scan of a primary identifier and a scan from a photograph or video.[25] Good anti-circumvention protections do not yet exist for secondary identifiers — distinguishing a live voice from a pre-recorded voice is simply a harder problem.

The following physical features are the major primary identifiers being used in or considered for biometric applications in banking.

1. Fingerprints

Fingerprints are the most widely used biometric identifier; police forces have used them for decades.[26] Before proceeding, the reader should beware of the confusing terminology in this area. As used in this paper, "fingerprint" (as a single word) refers to the unique patterns that exist on the underside of every human finger. Although unique patterns exist along the entire length of the finger and extend onto the palm of the hand, the portion of the fingerprint most commonly used in biometrics is that on the pad of the finger — the area on the underside of the finger below the distal joint, opposite the fingernail. "Finger printing" (two words) refers to an impression or image of a fingerprint — usually impressed on paper with ink when created intentionally or in oil or dirt on a rigid any rigid surface when created unintentionally. "Finger scanning" is the process of capturing an image of a fingerprint with a digital sensor for use as a biometric identifier.

---

[24] Brian Dye, Jeff Gerttula, Jonathan Kerner, and Brian O'Hara, *An Introduction to Biometrics* (2001) (available at <http://www.stanford.edu/~bjohara/>) ("Dye et al.")
[25] *Id.*
[26] *Biometrics: Arthur C. Clarke, Where Are You?*, Future Banker, 14 (1 June 2001)

The "ridge patterns" of a fingerprint, including arches, loops, and whorls, form "three-dimensional contours and microscopic blemishes that are unique to each person."[27] As explained in detail in the next section of this paper, a fingerprint template does not comprise an image of the entire fingerprints; it comprises only a binary data set that describes the unique aspects of the print — the location, size, and contours of various unique elements. Fixed before birth, these features do not change during a person's life under normal conditions.[28] Unique fingerprint features will even grow back after trauma with sufficient identicality to permit identification with a high degree of confidence. The gangster John Dillinger famously paid a surgeon $5,000 to "burn off his fingerprints with acid."[29] Unfortunately for Dillinger, his fingerprints grew back into the same pattern they had before; and he was later caught, due in part to fingerprint impressions he inadvertently left at the scene of a crime.[30]

Four methods can capture finger prints for biometric use. First, law enforcement agencies have used ink and paper systems for decades.[31] Ink and paper impressions have several disadvantages: messiness, bulkiness of paper cards for long term storage, and imperfections in scanning for digital comparison with live data. Second, optical sensors can capture visual images of the fingerprint; these generally use charged coupling devices (CCD) similar to those in familiar desktop scanners. Third, capacitance sensors use semiconductors to measure variations in electrical capacitance across the finger, from which they infer the fingerprint's features.[32] The durability of silicon and other semiconducting materials relative to the glass used in optical

---

[27] Rosenberg; *see* International Biometric Group, *Fingerprint Feature Extraction* <http://www.ibgweb.com/reports/public/reports/finger-scan_extraction.html> (accessed 9 Oct. 2002)
[28] *Id.*
[29] The Crime Library, *Fingerprints and Other Impressions* <http://www.crimelibrary.com/forensics/fingerprints/3.htm> (accessed 9 Oct. 2002)
[30] *Id.*
[31] *See* International Biometric Group, *Fingerprint vs. Fingerprint* <http://www.ibgweb.com/reports/public/reports/fingerprint_finger-scan.html> (accessed 9 Oct. 2002) ("IBG, *Fingerprint vs. Fingerprint*")
[32] Rosenberg

sensors makes capacitance an appealing option in programs with many inexperienced users, such as in ATM authentication.[33] Fourth, ultrasound sensors are the newest and most promising technology.[34] These sensors measure tiny differences in the transmission of sound waves through the finger and the reflection of sound waves off the fingerprint.[35] Ultrasound technology alleviates the common problem of dirt, oil, and other foreign substances obscuring sensor.[36] Finally, composite sensors combine two or more of these techniques.[37]

2. Faceprints

While biometric identification in public areas remains limited, faceprints are the most common identifier used in such programs.[38] Photographs or video frames captured at significant distances from the subject can yield a usable faceprint template — in contrast to most other biometric identifiers, which require close proximity or physical contact for an adequate measurement. Trauma, disease, deliberate medical alteration, and even changing facial expressions can change the appearance of facial features enough to fool a faceprint system. Features especially susceptible to alteration include lip size and shape, skin color, nose shape, and tooth alignment. Therefore, biometric systems use the features least susceptible to alteration: the "outlines of the eye sockets, the areas surrounding one's cheekbones, and the sides of the mouth."[39]

No facial feature can uniquely identify an individual, but using several in combination can provide a highly unique identifier; the face contains about 80 "nodal points" that biometric

---

[33] Intl. Biometric Group, *Finger Scanning Options* <http://www.ibgweb.com/reports/public/reports/finger-scan_optsilult.html> (2002)
[34] Rosenberg
[35] *Id.*
[36] *Id.*
[37] *Id.*
[38] Rosenberg
[39] Dye et al.

systems combine.[40] Combination techniques include measuring the distances between features or the ratio of their circumferences. Software measures these features in photographs or video frames and creates a binary template from those measurements.[41] Researchers at MIT invented the current state of the art — the "Eigenface technique" — for creating faceprint templates in 2000.[42] This technique involves combining many two dimensional grayscale images to form a single three dimensional data set that describes the entire face.[43] While the technique requires such detailed information to create the most accurate template, a single "mug shot" can suffice.[44]

As for live data, "a straight-ahead video image from a distance of three feet [yields] the most accurate" identification, but clear images collected from any distance can suffice.[45] A matching technique called "feature analysis" can accommodate images of the face captured at "angles up to approximately 25° in the horizontal plane, and approximately 15° in the vertical plane."[46] This technique compares the relationships between many different facial features and accommodates the widest range of facial expressions, hairstyles, and other factors that would otherwise frustrate matching.[47]

Facial scanning works faster but less accurately than most other methods of biometric identification.[48] Consequently, it is usually a "first line of defense" whose results merely limit the number of candidate templates that slower but more accurate techniques will consider.

---

[40] *Id.*
[41] *Id.*
[42] Rosenberg; U.P. No. 6,044,0168 (issued 28 Mar. 2000) ("Eigenface patent"). Texas Instruments now controls this patent.
[43] *Id.*
[44] Dye et al.
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] *Id.*

Current speed limits stem from the scarcity of computational power.[49] Practical constraints limit the size of the template database to several hundred thousand faces.[50] This may suffice for security applications that seek only specified individuals (such as known terrorists at an airport security checkpoint) but it is inadequate for banks with millions of customers. For such commercial applications, template storage on a wallet card may be the most practical option.

3. Eyes

Two parts of the eye, the retina and iris, are the two most uniquely identifying biometric indicia in the human body.[51] Retinas contain twenty times the number of unique identifying points as fingerprints, and irises contain as many as ten times that number.[52] Ironically, however, eye scanning also presents more privacy concerns than any other biometric indicia. The following discussion of the physiology of the eye and the mechanics of data capture for eye scanning highlights these problems.

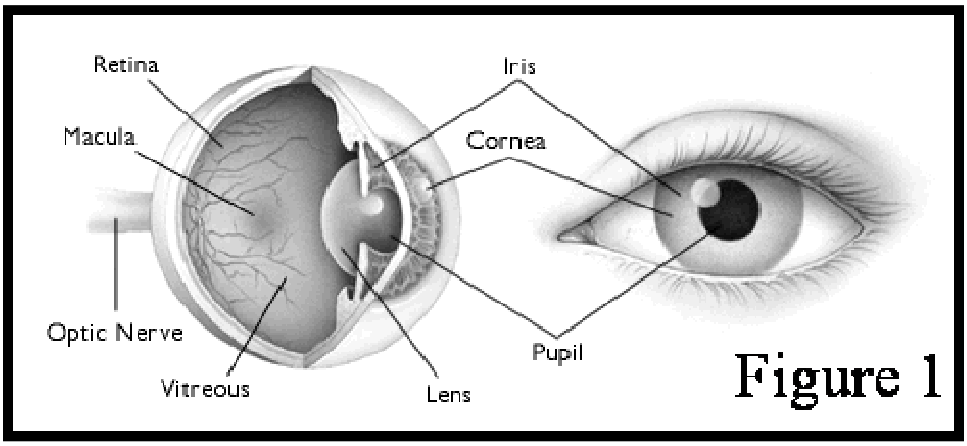

Figure 1

a. Retinas

The retina is "the sensory membrane that lines the eye, … composed of several layers including one containing the rods and cones, and [it] functions as the immediate instrument of

[49] *Id.*
[50] *Id.*
[51] *Id.*
[52] *Id.*

vision by receiving the image formed by the lens and converting it into chemical and nervous signals which reach the brain by way of the optic nerve."[53] "The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain — the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers."[54] The branching network of the blood vessels embedded in the retina make up its biometrically useful characteristics; no individual point is unique, but the vessels' turning points and end points make up a highly unique identifier in combination.[55] Overall, the retina provides the highest number of unique identifying points of any primary biometric identifier.[56] Counterintuitively, retina templates are among the smallest in terms of the number of bits required to uniquely describe an individual retina.[57]

Data capture for retinal biometrics requires placing the eye within three inches of a camera for approximately one minute.[58] Already, this close proximity of a foreign object to one of the body's most sensitive organs for such a long time can induce some discomfort. A light source behind the camera shines into the eye, and green light to reflects off the retina, back toward the camera.[59] The bright intensity of this light can cause additional discomfort during the procedure, especially considering the duration that the user must keep his eyes open. The blood vessels constituting the biometric lie just beneath surface of the retina, producing variations in its

---

[53] Mirriam-Webster's Collegiate Dictionary (available at <http://www.webster.com/cgi-bin/dictionary?retina>); *see* figure 1, *supra*, p 10. Source: International Biometric Group, *Retina Scan Technology* <http://www.retina-scan.com/retina_scan_technology.htm> (accessed 15 Sept. 2002) ("IBG, *Retina Scan Technology*")
[54] IBG, *Retina Scan Technology*
[55] Dye et al.
[56] *Id.*
[57] Rosenberg
[58] *Id.*
[59] *Id.*

albedo from areas without blood vessels.[60] The camera records the variations in the intensity of light reflected back to it from the retina, and computer software infers a "map" of blood vessels from these data. The software then translates this "map" into the binary data of the biometric template describing the unique combinations of points in the retina's blood vessels.

The biology of the eye presents three special privacy problems for retina scanning. First, as already mentioned, the discomfort caused by the proximity of the camera to the eye, the unnaturally bright light shining directly into the eye, and the duration of the data capture procedure all imply a violation of personal privacy. Informed consent may solve the formal privacy problem, but it cannot assuage the underlying discomfort. Second, the retina's pattern of blood vessels can change over time, introducing a complication not present in most other biometric indicia.[61] Certain diseases and traumas to the eye or head can alter their layout.[62] However, the risk of deliberate alteration is generally considered small because few people would want to risk losing eyesight.[63] Moreover, retinal blood vessels grow until the end of adolescence, rendering retina scanning useless for children. Third, some diseases and traumas can cause changes in other parts of the eye that block measurement of the retina.[64] Thus, a disease or trauma may render the retina useless for biometric identification even without affecting the retina. The scanning equipment necessarily can detect some of these medical conditions — either through deliberate misuse or by unintentional deduction from aberrant scanning results. The user may never know if the program operator discovers medically relevant information, let alone what the operator does with that information — whether he stores it,

---

[60] *Id.*
[61] Rosenberg
[62] IBG, *Retina Scan Technology*
[63] Rosenberg. Note especially the low risk of an individual deliberately altering the layout of his retinal blood vessels vis-à-vis the risk of deliberate alteration of the rest of the face. Plastic surgery on the face is increasingly common, especially among affluent Americans, but eye surgery remains relatively rare.
[64] IBG, *Retina Scan Technology*

discloses it to others, or alerts the user to the problem. This potential for medical diagnosis might conceivably render biometric program operators subject to the Health Insurance Portability and Accountability Act of 1996 (HIPPA),[65] which, *inter alia*, establishes privacy protections for patients vis-à-vis healthcare service providers. However, the statute and the regulations promulgated thereunder limit its applicability to "covered entities" — health plans, health care clearinghouses, and "health care provider[s] who transmit[] any health information in electronic form in connection with a transaction covered" by the regulations.[66] Congress intended HIPPA to cover entities whose primary business is healthcare, and its enforcement thus far has been consistent with this intent.[67] Therefore, the accidental discovery of medical information by a biometric program operator would not likely bring it within HIPPA. Deliberate misuse of biometric equipment, however, would make a court far less sympathetic to the program operator.

b. Irises

The iris is "the opaque contractile diaphragm perforated by the pupil and forming the colored portion of the eye."[68] "[L]ocated behind the cornea and the aqueous humour, but in front of the lens[, the iris] is the only internal organ of the body that is normally visible externally."[69] The iris's distinctive characteristics lie in the trabecular meshwork — a web fibrous tissue that fixes permanently by the eight month of gestation and remains stable throughout a person's life.[70] This meshwork "gives the appearance of dividing the iris in a radial fashion. Other visible

---

[65] Pub.L. 104-191, Aug. 21, 1996, 110 Stat. 1936
[66] 45 C.F.R. § 160.102(a) (2002)
[67] Telephone interview with Daria Niewenhous, Special Counsel, Mintz Levin Cohn Ferris Glovsky and Popeo PC (26 Nov. 2002)
[68] Mirriam-Webster's Collegiate Dictionary (available at <http://www.webster.com/cgi-bin/dictionary?iris>)
[69] John Daugman, *Anatomy and Physiology of the Iris* <http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html> (accessed 9 Oct. 2002); *see* figure 1, *supra*, page 10.
[70] International Biometric Group, *Iris-Scan: How it Works* <http://www.ibgweb.com/reports/public/reports/iris-scan_tech.html> (2002) (accessed 1 Oct. 2002) ("IBG, *Iris-Scan*")

characteristics include rings, furrows, freckles, and the corona."[71] In contrast to the retina, which develops naturally for years after birth and may change later still due to disease or trauma, the iris never changes.[72] "There is a popular belief that the iris systematically reflects one's health or personality, and even that its detailed features reveal the state of individual organs ('iridology'), but such claims have been discredited as medical fraud."[73]

Although the retina has more individual points for identification than the iris, retinal identification requires analysis of the configuration of many points in combination, and the retina yields fewer identifying combinations than the number of individually unique points in the iris. The retina's potential to change over time further diminishes its usefulness, so the iris is the most uniquely identifying tissue now known in the human body.[74] "In the entire human population, no two irises are alike in their mathematical detail — an individual's right and left irises are different; even identical twins have different irises. The probability that two irises could produce the same IrisCode® is about 1 in 10^{48} (the population of the earth is only 10^{10})."[75] Although genetics determine an iris's distinctive color and overall appearance, the trabecular meshwork of every iris forms a highly unique pattern.[76] The minutia "of genetically identical eyes…are as uncorrelated as they are among unrelated eyes."[77] This holds true both for identical twins and the two eyes of a single individual.[78]

---

[71] *Id.*
[72] John Daugman and Cathryn Downing, Epigenetic randomness, complexity, and singularity of human iris patterns, Proceedings of the Royal Society, 268 Biological Sciences 1737, 1740 (2001) (available at <http://www.cl.cam.ac.uk/users/jgd1000/roysoc.pdf>) ("Daugman and Downing")
[73] *Id.* (citing L. Berggren, Iridology: A Critical Review, 63 Acta Ophthalmology 1, 1-8 (1985))
[74] This excludes DNA because, as explained above, DNA is not a biometric identifier.
[75] Ellen Chang, *Iris Scanning* <http://www.stanford.edu/~ellenc/cs147/IrisScanning.htm> (accessed 29 Nov. 2002) ("Chang"). IrisCode® is a proprietary iris template format patented by Dr. John Daugman of Cambridge University and subject to trademark rights. Iridan Technologies, *Science Behind the Technology* <http://www.iridiantech.com/basics.php?page=5> (accessed 9 Oct. 2002).
[76] Daugman and Downing, 268 Biological Sciences 1737, 1739
[77] *Id.*
[78] *Id.*

Iris scanning technology avoids implicating some, but not all, of the privacy issues that hinder retina scanning. For example, the iris' natural exposure to the outside world permits a camera to capture images of it from a distance, obviating the need for the close proximity of a retinal camera.[79] A camera can detect the trabecular meshwork of an iris from three feet away.[80] Moreover, this additional distance from the eye reduces the intensity of the light received by the eye, further reducing the discomfort inherent in the data capture procedure. However, iris scanning has an ambiguous effect on the risk of stealth collection of medical data by the program operator. On one hand, the iris resides near the front of the eye, so fewer tissues lie between the camera and the subject of the scan, thereby reducing the risk of incidental detection of the medical state of the surrounding tissues. On the other hand, iris scanning works best with visible and near-infrared light — the same wavelengths of light recommended by the American Academy of Ophthalmology for the diagnosis and study of conditions such as macular cysts.[81] The use wavelengths commonly used in medical procedures can only increase the potential for illicit diagnosis.

B. Biometric Applications: Identification and Authentication

The two major biometric applications are "identification" and "authentication." A biometric "program" refers to a particular system or process that seeks to identify or authenticate individuals by comparing a "live" scan of their biometric indicia against existing "biometric templates" — data derived from previous biometric scans.[82] Identification, or "one-to-many," programs seek to identify specified individuals within a larger population by comparing each

---

[79] IBG, *Iris-Scan*
[80] *Id.*
[81] *Id.*
[82] A detailed discussion of the capture, storage, and use of biometric templates must wait until the next section. *See* part II.C., *infra*, page 17.

person's biometric indicia to templates stored in a database.[83] For example, airport security personnel might compare the faceprint of each traveler to faceprint templates in a database of known terrorists. At the 2001 Super Bowl, law enforcement agencies used a facial recognition system, purportedly to identify terrorists and felons in the audience.[84] A biometric-enabled automated teller machine (ATM) might identify customers by comparing live biometric scans to templates of the bank's customers. If it finds a match, the ATM would permit access to that customer's account; otherwise, it would deny access to any accounts.

Authentication programs, also called "one-to-one" or "verification" programs, seek to verify or refute that an individual is who he claims.[85] Such programs compare live data to only one template, not to an entire database.[86] For example, a biometric-enabled ATM might first ask a customer to identify himself, then compare his live biometric scan only to that customer's own template; the program need not test the live scan against any other templates. Controlling access to joint accounts present a hybrid scenario, where the user claims to be one of two or more authorized users of a particular account.[87] Counterintuitively, authentication programs do not require a database of templates: the person seeking authentication may supply the template against which to compare his body. While a biometric-enabled ATM could retrieve each template from a central database via the same electronic communication lines through which it retrieves account information, it could equally read a biometric template encoded on a magnetic strip or bar code on the customer's ATM card. The bank would simply encode the template on the card when the customer enrolls in the biometric program.

---

[83] Jenn Rosenberg, *Biometrics* <http://www.colby.edu/~jbrosenb/STS%20Project/web/> (accessed 21 Sept. 2002) ("Rosenberg")
[84] *See* Zalud and Constantinou
[85] Rosenberg
[86] *Id.*
[87] In this case, the program is still an authentication program if it first asks the user to identify himself to narrow the field of templates against which it will compare his live scan.

C. Data Capture, Storage and Use

To participate in a biometric program, a user must first enroll, "a process where multiple measurements of the particular biometric indicia are made, in order to establish a baseline for future comparison."[88] Computer software creates a set of binary data called a "template" that describes the unique aspects of the biometric identifier.[89] At the time of authentication or identification, an input device will capture a "live" image of the identifier, create a new set of binary data describing its unique aspects, and compare this "live" data to the stored template.[90]

Contrary to popular misconception, biometric systems do not directly compare images of biometric indicia, and they rarely store raw images for longer than required to generate a template. Despite the difficulty of converting images into templates,[91] this conversion has three compelling advantages over using and storing "raw" image data. First, electronic computers process information in binary code, so the creation of a binary template during enrollment removes the need to extract the appropriate information from the raw image during matching, when speed matters most.[92] Second, a template includes only the information useful for identification and disregards the extraneous information in the image.[93] This permits the template to occupy a smaller binary "size" than the original image — reducing the cost of storage media, bandwidth required for transmission, and the time required for matching.[94] One frame of high quality video, for example, occupies approximately 300 kilobytes, but a faceprint template

---

[88] R.R. Jueneman and R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 Jurimetrics J. 427, 448 (1998)
[89] Rosenberg
[90] Dye et al.
[91] Converting visible characteristics such as the trabecular meshwork of the iris or the precise positioning and shape of facial nodes into binary data "requires a degree in advanced mathematics" and the aid of a powerful computer. IBG, *Iris-Scan*.
[92] Rosenberg
[93] *Id.*
[94] *See* Dye et al.

derived from many such frames will occupy only 1.3 kilobytes.[95] Finally, the destruction of the raw image after generation of the template reduces the likelihood of abuse of the biometric data. The difficulty of reverse engineering an original image from a template affords some protection to users in the event of illicit access to the data.[96] Abuse of human-readable images presents a greater loss of privacy than illicit access to data strings that only specialized software can interpret — especially when the database would associate each image with additional private information like addresses, Social Security numbers, and account numbers.

A biometric template, like any data set, can reside in many types of storage media. Common template storage media include magnetic or optical computer disks, such as hard drives or compact discs, and magnetic strips or bar codes on wallet-size cards.[97] A few applications compel a particular storage medium, but most permit some flexibility. One-to-many programs generally require a central database of templates,[98] for no computer can compare templates from many disparate sources in realtime. Accordingly, most identification programs store templates on computer disks, where comparison software can access them quickly. Authentication programs allow greater flexibility with respect to the storage medium. Users of authentication systems usually consent to and cooperate with them, obviating the need for realtime results: bank customers, for example, already tolerate delays of several seconds at ATMs during authentication based in personal identification numbers (PINs). Moreover, ATM users already carry wallet cards equipped with magnetic strips that identify they to the machine, so encoding a biometric template on such cards would entail minimal retooling of the card manufacture and

---

[95] *Id.*
[96] The erasure of nonessential data and the proprietary algorithms applied to the images combine to make reverse engineering difficult — and some would argue impossible. *See* Dye et al. and Rosenberg.
[97] The space efficiency of a bar code for storing data surprises many people. The most common two-dimensional bar code symbology can store over one kilobyte (1,048 bits of information) in an area about the size of a postage stamp. Azalea Software, *The Barcode FAQ* (1999) <http://www.azalea.com/faq/> (accessed 4 Jan. 2003).
[98] Rosenberg

issuance processes. The implications of a bank's choice between central template storage and storage on wallet cards is discussed further in part V.

Once the input device captures a "live" image of a biometric identifier, computer software extracts the uniquely identifying information from that image and converts it to binary data.[99] Comparison software weighs the live data against the template and returns a single value as a result — positive or negative, indicating a match or not.[100] The comparison software sends the result to a second software routine which performs whatever action the program operator specifies.[101] Thus, the actions taken following a positive or negative result remain independent from the comparison and can be reprogrammed without altering the comparison software.

This division between the comparison and action routines permits standardization in the comparison routines across programs and diversity in the actions taken after acceptance or rejection of a match. In a surveillance program, the action software might play an audible alarm message after a positive result while simply ignoring negative results. In a secure access program, the action software might unlock a door following a positive result but do nothing — so the door remains locked — after a negative result. In an ATM program, the action software might display account balances or a list of commands following a positive result and prompt the user to rescan his biometric indicia upon receiving a negative result. In addition to any actions taken in response to the result of any individual scan, the action software might take separation action based on the aggregate rate of positive or negative results. For example, an ATM program might trigger an audible alarm following a string of negative results in rapid succession.

---

[99] *Id.* This process essentially creates a new template that could be stored for future use.
[100] Dye et al.
[101] *Id.*

The data capture and comparison processes described above implicate several privacy concerns. Users rarely or never have direct control over the program operator's use of the live data; the program operator could retain or otherwise misuse the live data or raw images without users' consent. Even if users have consented to centralized template storage under the program operator's control, the program operator might violate that consent by storing raw live images. He would certainly violate the consent of any users who consented to a biometric program that stores templates on media in the users' direct control, such as wallet cards. Identification programs can implicate particularly acute privacy concerns because individuals may be wholly unaware of the data capture, and they will have no opportunity to grant or deny consent. For example, law enforcement agencies already record video images of travelers in every airport, and they might convert those images into faceprint templates for future use. The customary check-in at the terminal or gate provides an easy opportunity to identify the name and destination of each person captured on tape. Such a practice would present obvious privacy problems: a person's bodily traits would enter a long-lived database without his having manifested consent in any form.

Even voluntary programs suffer from problems relating to the storage and use of live data. By definition, users consent to voluntary programs, so they may have an opportunity to review the operator's policy regarding the use and storage of live data. Informed consent can go a long way toward resolving privacy issues, but the users typically must rely on the operator's honesty in adhering to the scope of the users' consent. Additionally, the operator of a voluntary program must establish a policy for dealing with data captured from at least two types of unauthorized users — people who have not enrolled, and therefore have not consented, to the program. First, some unauthorized people will inadvertently enter areas monitored by a data

capture devices, especially where cameras monitor a public space or a wide area within a private building. Second, some unauthorized individuals will deliberately trigger the system for the purpose of gaining unauthorized access to whatever the system guards. While this behavior may constitute a crime (such as attempted fraud), criminals have rights — including the right to privacy.

Even restricting our focus to people who consent to a biometric program does not eliminate the problems. Particular bodily features make good biometric identifiers because they never (or rarely) change, but the software that compares live scans to templates must permit some variation between scans to account for numerous intervening variables. Those variables include different lighting conditions, background noise, new hairstyles, eyeglasses and contact lenses, movement by the user during the scan, and foreign substances on the data capture devices. Even a single biometric program may require different levels of permissiveness in different locations. An outdoor ATM, for example, must contend with greater variations in lighting, temperature, and background noise than one residing indoors. Once the program operator identifies the most likely sources of interference, he can tweak the comparison software to permit an appropriate level of variation — bearing in mind the fundamental trade-off between permissive matching and false positives.[102] The operator of a biometric program must optimize the level of permissiveness to suit the requirements of his program and the demands of users.

A given level of permissiveness in biometric comparison software can have drastically different implications in different biometric programs. Consider these two examples: program A seeks to identify terrorists at an airport security checkpoint, and program B authenticates bank customers at an ATM. In program A, a high level of permissiveness implies high levels of both

[102] IBG, *Retina Scan Technology* ("Of course, there are many measures of accuracy in biometrics, and with 0.0001% [False Acceptance Rate], there will be an increased number of False Rejections.")

security aggravation among travelers because the permissive software will identify most real terrorists while wrongly flagging many innocent travelers as terrorists. Reducing permissiveness in program A's software would reduce both security and aggravation by allowing at some terrorists to pass undetected while wrongly flagging fewer innocent travelers. In program B, permissiveness in the comparison software has the opposite correlation with security and user aggravation. Highly permissive software aggravates few ATM customers because it will produce few false negatives that would prevent legitimate customers from accessing their own accounts, but it also permits many unauthorized people to access accounts illegitimately. Low permissiveness in program B implies high security because it will prevent most illicit attempts to access accounts, but it will simultaneously aggravate more customers with false negatives.

III. Historical Perspective on Biometrics

Biometric technology has generated warnings of hubris, fire, and brimstone but little frank discussion of the problems it presents. Proponents invoke popular bogeymen like terrorism and identify theft, and they portray biometrics as a magic bullet. "Today," writes Identix Corp., "banks and brokerage houses find themselves vulnerable to theft, from both internal and external sources, a fast-growing, alarming number of identity fraud cases and a whole host of other security risks as well as privacy issues posed by providing services over the internet."[103] Fortunately, Identix and its brethren offer a product for every bugbear at low prices, of course, and requiring minimal disruption of business as usual.[104] Governments and private companies launch new biometric programs at an ever-increasing rate — and not just in such obvious fields as law enforcement and ATM security. Even welfare administration has gotten fifteen minutes

---

[103] Identix Corp., *Securing Critical Information*, <http://www.identix.com/solutions/sol_financial.html> (accessed 9 Oct. 2002)
[104] *See e.g.*, Identix Corp., *Product Listing* <http://www.identix.com/products/pro_all.html> (accessed 9 Oct. 2002)

of biometrics' fame.[105] Before long, the public's pervasive exposure of biometrics will diminish the technology's novelty, and our society will have lost its only opportunity for frank discussion of the technology's moral and ethical problems. This fate has plagued many technologies that lean as heavily on information as biometrics. Once any technology gains economic importance before it gains general public awareness, the public stands little chance of stopping its adoption, moral and ethical problems notwithstanding. The telegraph — the foundational modern information technology — provides the clearest example of this phenomenon.

In 1840, the United States Patent & Trademark Office (PTO) granted Samuel Finley Breese Morse a patent for the first practical telegraphy machine.[106] Morse lacked sufficient personal wealth to finance a dramatic exhibition of his device, so he sought private and public funds to demonstrate it. The private sector met early versions of the telegraph "with an immediate and overwhelming lack of interest."[107] Congress likewise hesitated to appropriate funds for the telegraph.[108] Three years later, when Morse proposed a bill to allocate $30,000 for a public demonstration, several Congressmen openly ridiculed it, "and they proposed many amendments to the bill to show their scorn."[109] These facetious amendments would have diverted half the money toward research of mesmerism, animal magnetism, and other mystical arts that were equally considered nonsense.[110] They ignorantly "explained" that Morse claimed to communicate via lightning, the only source of electricity they understood.[111] However, Congress did finally give Morse his money.

---

[105] *See supra*, page 4, notes 4 and 5 and accompanying text.
[106] U.P. No. 1,647 (issued 20 June 1840) ("Telegraph patent")
[107] Kenneth W. Dobyns, *History of the United States Patent Office*, 118 (Sergeant Kirkland's Press 1994) ("Dobyns")
[108] *Id.* at 118-19
[109] *Id.* 119
[110] *Id.*
[111] *Id.* at 118

Meanwhile, religious leaders "proved" the telegraph would never work by citing the Bible, where god chastised Job for hubris. God asked Job, "Canst thou send lightnings, that they may go, and say unto thee, Here we are?"[112] To them, the telegraph represented an arrogant infringement on god's lightning. As a painter and professor of literature,[113] Morse was acutely aware of the implications of his electrical telegraph for the humanities, and he planned his publicly funded demonstration with these concerns in mind. In 1844, Morse strung a telegraph wire along the fifty miles of railroad track from Baltimore, where the Democratic party would soon hold its Presidential nominating convention, to Washington, D.C., where he would report the party's nomination long before conventional messages arrived. Despite the public controversy and ridicule, only 16 people gathered on the appointed day in the Supreme Court chamber of the Capitol, where the inventor had erected his apparatus.[114] Morse gave the honor of transmitting the first signal to Annie Goodrich Ellsworth, the daughter of the Commissioner of Patents, whose family had supported Morse for years.[115] In a slight dig at her friend's detractors, Ellsworth began her ceremonial first signal with a Bible verse, "What hath god wrought!"[116] From the Mount Clare depot in Baltimore, Morse's friend Alfred Vail then informed the group in the Capitol that the Democrats had nominated James K. Polk five minutes earlier.[117] Messengers relying on the previous state of the art — horses and paper — verified the result nearly a full day later.

---

[112] King James Bible, Job 38:35
[113] Dobyns, 119
[114] *Id.* at 120
[115] *Id.*
[116] King James Bible, Numbers 23:23
[117] Dobyns, 120; *see also* Tom Standage, *The Victorian Internet* (Walker & Co. 1998)

Despite the public feud between the moralists, theologians, and the inventor, only one newspaper covered Morse's demonstration; and the public barely noticed it.[118] This indifference would not last long, however, as the technology's economic value soon overwhelmed any moral misgivings.[119] The business community recognized the telegraph's potential almost as instantly as the device's transmission of information. One contemporary observer wrote about the fading voice of moral fears in *Scientific American*, "The steed called Lightning (say the Fates) / Was tamed in the United States / 'Twas Franklin's hand that caught the horse / 'Twas harnessed by Professor Morse."[120] By 1850, a new communications industry had strung more than 12,000 miles of telegraph wire;[121] five years later, networks of telegraph cables crisscrossed the nation;[122] and the first transatlantic cable began service in 1865.[123] During this period, the acute military need for instant communication during the Mexican and Civil Wars made the U.S. government the largest consumer of telegraph services.[124] In the two decades following Morse's demonstration, society stopped asking *whether* it should use the telegraph and began to ask *how soon* telegraph networks could expand to meet its needs.

Today, the cutting edge of information technology is biometrics, and the recent wave of adoption bears striking resemblance to the telegraph's early years. A few people today speak out against biometrics as those early Congressmen and clergymen did against Morse's telegraph in 1843. Pat Robertson, founder of the Christian Coalition, warns that biometrics implies the mark of the beast. "The Bible says the time is going to come when you cannot buy or sell except

---

[118] Dobyns at 120
[119] *See History of the Telegraph: Difficulties and Success of an Inventor*, Scientific American, 19 (29 Sept. 1855) ("Scientific American")
[120] *Id.*
[121] *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-Line Pioneers*, Mappa Mundi Magazine, available at <http://mappa.mundi.net/reviews/victorian/> (2000) (accessed 21 Sept. 2002)
[122] Scientific American
[123] *Id.*
[124] Standage

when a mark is placed on your hand or forehead."[125] William Abernathy and Lee Tien of the Electronic Frontier Foundation (EFF) write specifically about civil liberties, "Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging."[126] While paying lip service to their concerns, the biometrics industry has never invited such groups as the Christian Coalition and the EFF for frank discussion of their products' implications. Just as in Morse's day, the public has begun to consume a new technology before the requisite dialog on its morality.

The telegraph grew entrenched before the 19th century public could fully grasp it, and the current explosion of biometric products has caught the 20th century public similarly off guard. The first modern biometric programs appeared the 1980s, when minicomputers became widely available. By 2000, dozens of companies and governments had enrolled tens of thousands of people in biometric programs.[127] The war on terrorism declared after September 11, 2001 has accelerated the growth of biometrics in the same way that the Mexican and Civil Wars spurred the growth of the telegraph. This growth of biometrics also piggybacks on the rise of computing technology. Although the science and mathematics underlying most biometrics have existed for over 70 years,[128] exploitation of that knowledge had to wait for the electronic computer.[129]

Alphonse Bertillion, the son of an anthropologist and chief of the Paris police, compiled the first government database of criminals' physical characteristics in the 1880s.[130] Bertillion measured body height, finger length, head circumference, distance between the eyes, and other

---

[125] Chandrasekaran
[126] William Abernathy and Lee Tien, *Biometrics: Who's Watching You?* (available at <http://www.eff.org/Privacy/Surveillance/biometrics.html>) (accessed 1 Dec. 2002) (Abernathy and Tien)
[127] *See supra*, pp 2-3, notes 6-12 and accompanying text.
[128] *See e.g.*, Garfinkel; IBG, *Retina Scan Technology*
[129] The major exception is fingerprint technology, which has been used for law enforcement purposes for over a century.
[130] Garfinkel; Patricia Caristo, *Early Pioneers in the Field of Investigation* (available at <http://www.nia-nm.com/TheInvestigatorsClassroom.html>) (accessed 28 Nov. 2002)

non-unique features of convicted criminals and used these data in combination to identify repeat offenders.[131] This remained the state of the art until the early 20th century, when fingerprinting became widespread.[132] By the 1930s, research suggested the identifying properties of the retina.[133] However, the discoverers of these properties could not compare a biometric feature to a template fast enough to make the technology practical in most situations.[134]

Biometrics faced almost no resistance during this era, before computers enabled widespread use.[135] The recent coupling of biometrics and computers has created possibilities beyond Alphonse Bertillion's wildest dreams — while reducing the economic cost of biometrics to the point where most of our society can realistically afford to participate. Bertillion probably never envisioned identifying ordinary people with fingerprints for such routine transactions as buying food at a grocery store or withdrawing cash from a bank. The fast rise of computers has enabled biometric programs that we have scarcely begun to contemplate. Theologians, civil libertarians, and others have just begun to explore the moral and ethical implications of biometrics. Biometrics' benefits resemble those of the telegraph: efficiency, speed, and convenience, to name a few. Today we have the benefit of hindsight that clearly shows the telegraph's opponents drowning in its economic wake after the Civil War. Biometrics has grown with similar speed and shows signs of an impending growth spurt. Soon, it may seem as difficult to remove biometrics from the routine of daily life as it seems to us to remove the telegraph and its successors like the telephone and the Internet. If we do not address the privacy issues inherent in biometrics very soon, we will lose the opportunity forever.

---

[131] Garfinkel
[132] *Id.*
[133] IBG, *Retina Scan Technology*
[134] The important exception is fingerprinting for law enforcement purposes, where officers could compare fingerprints left at a crime scene to templates in a database at their leisure, over the course of an investigation.
[135] It is noteworthy that early biometric programs were limited to law enforcement. I suspect that these incurred no widespread opposition because convicted criminals have never had effective advocates in high places.

IV. Privacy Law and Consumer Banking

In 1890, Louis Brandeis and Samuel Warren wrote the foundational paper on privacy in America.[136] At that time, no federal statute specifically addressed privacy, so the authors argued that the common law and the Constitution must recognize a right to privacy. Although history credits them with characterizing privacy as the "right to be let alone,"[137] Thomas Cooley had coined this phrase two years earlier in his treatise.[138] Today, several statutes specifically address privacy, but no privacy law specifically addresses biometrics.[139] However, we can take a lesson from Brandeis and Warren and reason by analogy from existing statutes and caselaw to deduce how modern privacy law will regard biometrics. As the scope of this paper is limited to consumer banking, this discussion of privacy law will be limited to the common law, statutes, and regulations that apply to commercial banks that serve consumers.

A. Privacy at Common Law

The lay conception of privacy comes from the causes of action recognized at common law. The common law has traditionally recognized "the right to be free from the unwarranted appropriation or exploitation of one's personality, the publicizing of one's private affairs with which the public has no legitimate concern, or the wrongful intrusion into one's private activities, in such manner as to outrage or cause mental suffering, shame, or humiliation to a person of ordinary sensibilities."[140] Different courts have characterized the right of privacy in different ways, but they all share certain core elements, which William Prosser summarizes "as the right to be let alone, to be free from unwarranted publicity, to live a life of seclusion, and to live without

---

[136] *The Right To Privacy*, 4 Harv. L. Rev. 193 (1890) ("Brandeis and Warren")
[137] *Id.* at 195
[138] Lisa Jane McGuire, *Banking on Biometrics*, 33 Akron L. Rev. 441, 469 (note 157) (2000) ("McGuire") (citing Thomas Cooley, *The Law of Torts*, at 29 (2d ed. 1888))
[139] *See* McGuire at 456-73
[140] Leonard I. Reiser, *Privacy*, 62A Am. Jur. 2d § 1 (2002) ("Reiser")

unwarranted interference by the public in matters with which the public is not necessarily concerned."[141] Professor Prosser lists the fundamental privacy torts as "Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs; Public disclosure of embarrassing private facts about the plaintiff; Publicity which places the plaintiff in a false light on the public eye; [and] Appropriation, for the defendant's advantage of the plaintiff's name or likeness."[142]

B. Constitutional Foundations of Privacy

Some scholars have argued and some Supreme Court Justices have held that the United States Constitution establishes a right to privacy.[143] The Constitution does not expressly enumerate a right to privacy, but it has long been considered a corollary to core constitutional liberties.[144] A majority of the Supreme Court first recognized a constitutional basis for the right to privacy in 1965, when Justice Douglas wrote in *Griswold v. Connecticut* [145] that privacy is an unenumerated constitutional right. The "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance," and one penumbra "create[s] zones of privacy" guaranteed by the Constitution.[146] This penumbra emanates from the specific guarantees of the First, Third, Fourth, Fifth, and Ninth

---

[141] William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 389 (1960) ("Prosser")
[142] *Id.*
[143] *See e.g.*, *Griswold v. Connecticut*, 381 U.S. 479 (1965) ("*Griswold*"); *Roe v. Wade*, 410 U.S. 113 (1973); W. Page Keeton et al., *Prosser and Keeton on the Law of Torts* (5th ed. 1984); Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 Harv. J.L. & Tech. 319 (Spring 2002) ("Sobel")
[144] *See Olmstead v. U.S.*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("The makers of our Constitution… sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men."); *Griswold*, 381 U.S. at 494 (Goldberg, J., concurring) ("[T]he right of privacy is a fundamental personal right, emanating 'from the totality of the constitutional scheme under which we live."' (quoting *Poe v. Ullman*, 367 U.S. 497, 521 (1961) (Douglas, J., dissenting)))
[145] 381 U.S. 479 (1965)
[146] *Id.* at 484

Amendments.[147] However, the U.S. Constitution protects individual privacy rights only against unreasonable intrusions by the government, not against intrusions by private entities.[148]

The Supreme Court implied the existence of "a right to information privacy"[149] in *Whalen v. Roe* [150] — even while it sustained the constitutionality of a state statute requiring the collection of the names of all persons taking certain prescription drugs. The Court noted the potential "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[151] However, the Court applied the lowest level of constitutional scrutiny, the so-called "rational basis test," and upheld the law as rationally related to the legitimate governmental interest in preventing illegal distribution of drugs.[152]

Finally, some state constitutions establish a right of privacy for those states' citizens.[153] However, just as with the federal Constitution, most of these state provisions protect citizens only against governmental intrusion upon their privacy.[154] Only Hawaii's constitution protects citizens' privacy against intrusion by private entities.[155]

---

[147] *Id.*
[148] *See e.g.*, *Bowers v. Hardwick*, 478 U.S. 186 (1986); *Burton v. Wilmington Parking Authority*, 365 U.S. 715 (1961); *Roe v. Wade*, 410 U.S. 113 (1973); *Jackson v. Metropolitan Edison Co.*, 419 U.S. 345 (1974); *Stanley v. Georgia*, 394 U.S. 557 (1969); McGuire at 460
[149] McGuire at 460
[150] 429 U.S. 589 (1977)
[151] *Id.* at 605
[152] *Id.* at 597-98
[153] *See* Alaska Const. Art. I § 22; Ariz. Const. Art. II § 8; Cal. Const. Art. I § I; Fla. Const. Art. I, § 23; Haw. Const. Art. I § 6; Ill. Const. Art. I § 6; Mont. Const. Art. II § 10; S.C. Const. Art. I § 10; Wash. Const. Art. I § 7.
[154] Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier For Individual Rights?*, 44 Fed. Comm. L.J. 195, 208 (March 1992) ("Reidenberg"); *see Luedtke v. Nabors Alaska Drilling, Inc.*, 768 P.2d 1123 (Alaska 1989); *State v. Murphy*, 570 P.2d 1070 (Ariz.1977); *Hart v. Seven Resorts Inc.*, 947 P.2d 846 (Ariz. Ct. App. 1997); *Perkey v. Dept. of Motor Vehicles*, 721 P.2d 50 (Cal.1986); *Barr v. Kelso-Burnett Co.*, 478 N.E.2d 1354 (Ill.1985).
[155] Haw. Const. art. I, § 6; *McCloskey v. Honolulu Police Dept.*, 799 P.2d 953, 956 ("Privacy as used in this sense concerns the possible abuses in the use of highly personal and intimate information in the hands of government *or private parties*" (emphasis added)); *see also* McGuire at 465

C. Banking-Specific Privacy Laws

1. Background Federal Statutes

Several federal statutes and many state statutes deal specifically with privacy. "Because federal legislative jurisdiction for commercial information processing activities is drawn principally from the [Commerce Clause], federal law tends to be adopted on a narrow sectoral basis."[156] In keeping with the scope of this paper, I will limit my discussion to the statutes applicable to commercial banks that serve consumers. Even in this narrow slice of the economy, where Congress acts frequently, there is no comprehensive system of privacy applicable to banks.[157] Instead, Congress tends to enact *ad hoc* legislation in this area, addressing specific privacy problems as they arise.[158] The "financial services sector has perhaps the greatest variety of applicable legislation that does not systematically address privacy concerns."[159] Consequently, privacy regulation in consumer banking resembles a patchwork quilt.

The bank/consumer relationship was traditionally that of a debtor and creditor,[160] but it "now more closely resembles an agency model."[161] In general, a bank is liable for damages resulting from a breach of its duty not to disclose information about its customers.[162] "Inviolate secrecy is one of the inherent and fundamental precepts of the relationship of the bank to its depositors."[163] The roots of this duty of secrecy stem ultimately from the Fourth Amendment's guarantee that "persons, houses, *papers*, and effects…shall not be violated."[164] While Fourth Amendment rights are formally enforceable only against the government, the Framers of the

---

[156] Reidenberg at 208
[157] *Id.* at 210
[158] *Id.*
[159] *Id.*
[160] *Davison v. Allen*, 47 Idaho 405, 276 P. 43 (1929); 7 Am.Jur., Banks, § 444
[161] Donald A. Doheny and Graydon John Forrer, *Electronic Access to Account Information and Financial Privacy*, 109 Banking L.J. 436, 438 (1992) ("Doheny and Forrer")
[162] Doheny Forrer at 439
[163] *Peterson v. Idaho First National Bank*, 367 P.2d 284, 289 (Idaho 1961) ("*Peterson*")
[164] *Id.* (emphasis added)

constitution evinced an intent to protect personal material from unreasonable intrusion by anyone.[165] They reasoned that "[o]f all the rights of the citizen, few are of greater importance or more essential to his peace and happiness than the right of personal security, and that involves, not merely protection of his person from assault, but exemption of his private affairs, books, and papers from the inspection and scrutiny of others. Without the enjoyment of this right, all other rights would lose half their value."[166]

Most banking-specific privacy laws expressly apply to only "financial" information, but; at least since the 1960s, many courts have interpreted banks' duty to maintain the customer's privacy quite broadly,[167] often covering even the fact that the customer is a customer.[168] Today, "a bank depositor…has a right to expect that a bank will, to the extent permitted by law, treat as confidential, all information regarding his account and any transaction relating thereto. Accordingly, … absent compulsion by law, a bank may not make any disclosures concerning a depositor's account without the express or implied consent of depositor."[169] In addition, the common law of contracts has developed a privacy component in light of modern privacy statutes and regulations.[170] Many jurisdictions today consider it "an implied term of the contract between a banker and his customer that the banker will not divulge to third persons without consent of the customer, express or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his

---

[165] *Id.*
[166] *In re Pacific Ry. Commission*, 32 F. 241 (C.C.Cal. 1887)
[167] *See e.g.*, *Peterson*, 367 P.2d 284; *Milohnich v. First Nat. Bank of Miami Springs*, 224 S.2d 759 (Fla. App. 1969)
[168] Interview with Jay Spencer Dunham, Chief Executive Officer of Liberty Bank & Trust Co. (July 2001) ("Dunham")
[169] *Suburban Trust v. Waller*, 408 A.2d 758, 764 (Md. App. 1979)
[170] *See* 10 Am. Jur. 2d Banks and Financial Institutions § 332

account, unless the banker is compelled to do so by order of the court [or] the circumstances give rise to a public duty of disclosure."[171]

Most federal statutes that establish privacy rights control only the government's collection and use of personal information and say nothing about such actions by private entities.[172] Several major exceptions to this generalization cover the banking and financial sector — most notably the Fair Credit Reporting Act and the Gramm-Leach-Bliley Financial Modernization Act of 1999.[173] "Congress enacted most of these [privacy] statutes *reactively*, rather than *proactively*," usually reacting to some event in the national headlines.[174] Congress enacted the Right to Financial Privacy Act of 1978,[175] as a response to *U.S. v. Miller*,[176] where the Supreme Court held that bank customers had no Fourth Amendment expectation of privacy in their financial records while those records were held by a third party such as a bank.[177] Although Congress limited this Act to criminal investigations and certain types of documents,[178] its swift response to the Supreme Court decision it shows its attentiveness and sensitivity to the issue of privacy in the banking context.

Another 1978 statute, the Electronic Funds Transfer Privacy Act[179] ("EFTA"), required disclosure of information-sharing practices in wire transfer transactions. The most notable feature of the EFTA is its innovative mechanism for preempting state law: it expressly preempts state law to the extent that state law was less protective of the consumer but left state law intact

---

[171] *Id.*
[172] *See* McGuire at 461-65 (citing the Privacy Act of 1974 (5 U.S.C. § 552A), the Tax Reform Act of 1976 (Pub. L. 94-455 (10/4/76)), and the Driver's Privacy Protection Act (18 U.S.C. § 2721))
[173] *Id.* at 464-66
[174] *Id.* (emphasis added)
[175] 12 U.S.C. §§ 3401-3422 (2001)
[176] 425 U.S. 435 (1976)
[177] Doheny and Forrer at 446
[178] *Id.*
[179] 15 U.S.C. §§ 1693-1693r (2001)

to the extent that it gives consumers more protection.[180] Congress later modeled other federal statutes' preemption clauses on this one.[181]

2. Current Statutory Regime: The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 is Congress's most recent major enactment relating to consumer banking, and Title V of the Act[182] deals specifically with privacy. Title V prohibits disclosure of "nonpublic personal information to a nonaffiliated third party" except in certain defined circumstances.[183] Two chief sets of circumstances are excepted from this general rule. First, a bank may share certain customer information according to its "privacy policy regarding the sharing of non-public personal information with both affiliates and third parties," provided that it has made a "clear disclosure" of this policy to its customers and gives them "an opportunity to 'opt-out' of sharing of non-public personal information with nonaffiliated third parties."[184] Second, a bank may make certain disclosures when necessary "to comply with Federal, State, or local laws, rules, and other applicable legal requirements…or to respond to judicial process or government regulatory authorities having jurisdiction over the financial institution for examination, compliance, or other purposes as authorized by law."[185] Remedies include both civil and criminal penalties, including fines and imprisonment, and "aggravated" offenses may incur stiffer penalties.[186]

Several sources of potential future confusion appear immediately from the Act's text. First, Congress vested rulemaking authority under the Gramm-Leach-Bliley Act in many

---

[180] Doheny and Forrer at 449
[181] *Id.*
[182] 15 U.S.C. § 6801 *et seq*. (2001) ("Gramm-Leach-Bliley"). The trade literature cites sections of this Act according to the Act's own section numbering, not the numbering imposed when it was integrated into Title 15 of the United States Code. This paper follows that convention.
[183] Gramm-Leach-Bliley § 502
[184] United States Senate Committee on Banking, Housing, and Urban Affairs, *Gramm-Leach-Bliley: Summary of Provisions* (1999) (available at <http://www.senate.gov/~banking/conf/grmleach.htm>)
[185] Gramm-Leach-Bliley § 502 (e)(8)
[186] Gramm-Leach-Bliley § 523

different entities: the "Federal banking agencies, the National Credit Union Administration, the Secretary of the Treasury, the Securities and Exchange Commission, and the Federal Trade Commission."[187] Each agency may grant exceptions to the Act's privacy provisions so long as the exceptions are consistent with the policy underlying the Act.[188] However, Congress provided neither guidelines for determining whether a proposed exception meets this test nor a clear division of rulemaking authority into different spheres of jurisdiction. Second, Congress assigned "authority for enforcing [Title V's] provisions to the Federal Trade Commission and the Federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, according to their respective jurisdictions, and provides for enforcement of the subtitle by the States."[189] Again, Congress failed to provide a clear division of authority. Third, the Act's preemption provision follows the EFTA model, preempting only state laws that protect personal privacy to a lesser extent than the federal law.[190] The extent of protection of any state law — and therefore its validity — shall be "determined by the Federal Trade Commission, after consultation with the agency or authority with jurisdiction" over the complaint at issue.[191] However, Congress provided no guidelines for determining whether a state law is more or less protective than Title V.

The Gramm-Leach-Bliley Act's privacy provisions expressly apply to consumers but not to banks' commercial customers. The Act defines a consumer as "an individual who obtains, from a financial institution, financial products or services which are to be used primarily for personal, family, or household purposes, and also means the legal representative of such an

---

[187] Gramm-Leach-Bliley § 504(a)(1)
[188] Gramm-Leach-Bliley § 504(b)
[189] *Id.*
[190] Gramm-Leach-Bliley § 507
[191] Gramm-Leach-Bliley § 507(b)

individual."[192] Additionally, its express language protects only "personally identifiable financial information," which it defines as information "provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."[193] The Act exempts from this definition any "publicly available information" but leaves this term to be defined later, by administrative rules.[194] This exception is limited so as not to disqualify from being "personally identifiable financial information" "any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information."[195] In sum, the Gramm-Leach-Bliley Act protects "personally identifiable financial information" that a consumer provides to a bank pursuant to the customer-bank relationship but not information that is not so provided to the bank — e.g., information that the bank has discovered from other sources.

V. Intersection: Consumer Banking, Biometrics, and Privacy

A. Why Now?

The banking industry has an obvious and compelling need for accurate identification of customers — not just when they enter the branch but also to authenticate transactions conducted outside the bank. If there were ever a time when local bankers had a personal relationship with each customer, that time has long passed. Modern bankers need a reliable alternative to personal knowledge for identifying hundreds or thousands of unfamiliar people — let alone the needs of conglomerates like Fleet and Bank of America. For many years, the industry has relied on two chief methods of identification: signature matching and customer-memorized personal

[192] Gramm-Leach-Bliley § 509(9)
[193] Gramm-Leach-Bliley § 509(4)(A)
[194] Gramm-Leach-Bliley § 509(4)(B)
[195] Gramm-Leach-Bliley § 509(4)(C)

identification numbers (PINs). Although handwriting is technically a biometric identifier,[196] the use of signatures to authenticate transactions has rarely, if ever, been analyzed in biometric terms.[197] In light of this, one might ask why biometrics deserve close scrutiny now, if so many people have already grown accustomed to it without noticing significant erosion of their privacy.

The answer is two-fold: one part descriptive and one part normative. First, descriptively, biometric programs have historically required laborious, manual comparison of live data and templates. The advent of fast, small, and cheap electronic computers has only recently removed the practical barriers to ubiquitous biometrics. They have also increased the number of indicia available for biometric programs, including several that are orders of magnitude more accurate than "traditional" biometric identifiers like handwriting.[198] These secondary, enabling technologies — small computer processors, cheap digital communications, and reliable sensors — arose long after the adoption of fingerprint and handwriting programs. They have simultaneously decreased the cost of all biometric programs while increasing the number of places where biometric programs can reach. They have also introduced novel possibilities for sharing biometric information instantly and cheaply. This new diversification and expansion of biometrics will facilitate the weaving of the technology into the fabric of everyday life in ways that we can scarcely imagine today. We are now at the cusp of fast nationwide — perhaps worldwide — growth in biometrics, so privacy issues are ripe for examination now.

Second, normatively, no technology should be generally adopted without due consideration of its moral and ethical implications. Political and religious leaders expressed deep

---

[196] Recall from Part III, *supra*, page 5 at note 23, that handwriting is a secondary biometric identifier.
[197] My research in the legal and banking-industry literature failed to yield a single paper or article with significant analysis of signature authentication in biometric terms. Papers on biometrics tend to focus on newer technologies and only note in passing that banks have been using a secondary biometric identifier for many years.
[198] *See e.g.*, *supra*, pages 10-15

reservations about the telegraph before Samuel Morse's first public demonstration.[199] Still, industrialists installed hundreds of thousands of miles of telegraph wire and sprouted telegraph offices like mushrooms in every major city. Caught off-guard by new technology, the telegraph's detractors never organized effectively, and the public did not take them seriously after a few years. The business community and government overwhelmed the telegraph's detractors under the twin banners of economic progress and war. The proponents of biometrics appeal to nearly identical concerns today: expansion of commerce[200] and the war on terrorism.[201] We must learn from history and examine the privacy concerns raised by biometric technologies immediately — before we lose the opportunity to do so.

B. Current and Anticipated Biometric Applications in Consumer Banking

Banks constantly battle fraud perpetrated through their automatic teller machines (ATMs). "The banking industry reports that false acceptances at ATM machines are as high as 30 percent, resulting in worldwide financial fraud of $2.98 billion a year."[202] This is where biometrics' utility is perhaps the most obvious, and the earliest programs initiated by banks were designed to combat these false acceptances.[203] Since their introduction, most ATMs have operated by identifying a customer by the information encoded on a magnetic strip embedded on

---

[199] *See supra*, pages 23-24 at notes 106-112 and accompanying text

[200] *See e.g.*, Guy Gugliotta, *Bar Codes for the Body Make It to the Market; Biometrics May Alter Consumer Landscape*, Washington Post A1 (21 June 1999); Samir Nanavati, *Face-off: Is the use of biometrics an invasion of privacy? The International Biometric Group says no.*, Network World Fusion (8 May 2000) (available at <http://www.nwfusion.com/columnists/2000/0508faceno.html>); Tim Schellberg, *How to Advocate Biometrics Legislation in the Age of Privacy Fears* <http://www.biometricgroup.com/a_bio1/columnists/list_of_columnists.htm> (accessed 10 Sept. 2002) ("Schellberg"); Barry Steinhardt, *Face-off: Is the use of biometrics an invasion of privacy? The American Civil Liberties Union says yes.*, Network World Fusion (8 May 2000) (available at <http://www.nwfusion.com/columnists/2000/0508faceyes.html>) ("Steinhardt")

[201] This has obviously become a more pressing concern since 11 September 2001. *See e.g.*, Simon Liu and Mark Silverman, *A Practical Guide to Biometric Security Technology*, IT Professional (Jan./Feb. 2000) (available at <http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm>); Richard Sobel, *The Demeaning of Identity and Personhood in National Identification Systems*, 15 Harv. J.L. & Tech. 319 (Spring 2002);

[202] Chang

[203] *See supra*, page 2-3 at notes 6-12 and accompanying text

a plastic card, then authenticating him with a personal identification number (PIN) that the customer must memorize and keep secret. Eye or finger scanning can prevent illicit access to funds more reliably than PINs because thieves cannot acquire the customer's eye or finger from a distance with a pair of binoculars. Also, "[u]nlike a password, you can't forget biometrics. You can lose your key or even leave it at home, but you can't lose your finger."[204] Therefore, "[f]rom an economic standpoint, iris scanning could potentially save…billions of dollars annually" by preventing fraud, in dollars not stolen and dollars not spent on investigation and other security measures.[205] "The first [iris scanning] ATM was deployed in 1998 and has since led to similar ATMs appearing in Asia, Europe, and North America."[206] Despite the privacy concerns, the "vast majority of users of these ATMs responded positively, commenting that iris scanning is easier and faster" than using PINs.[207]

In addition to ATM authentication, the banking industry is investigating at least two other applications and could implement either or both of them within a few years. The first is in-branch security and authentication. All bank branches already have an installed base of security cameras trained on teller stations with cables capable of data transmission connecting them to a data center for recording.[208] Adapting this existing system for facial scanning would require little additional capital expense. Software that compares large numbers of faces to a large number of facial templates already exists; recall it received a very public field test at the 2001 Super Bowl in Tampa.[209] In that test, the software processed every face captured in the crowd captured by video cameras, comparing them to the templates stored in the Federal Bureau of

---

[204] Datamax System Solutions, *Biometrics* <http://www.datamaxsys.com/biometrics.html> (accessed 9 Oct. 2002)
[205] Chang
[206] *Id.*
[207] *Id.*
[208] Dunham
[209] Zalud; *see also supra*, page 15, notes 83-84 and accompanying text

Investigations' (FBI) database of known criminals.[210] Processing such a large number of faces so quickly required a significant amount of computer "horsepower."[211] Most banks have fewer total customers than there are criminals in the FBI's comprehensive database, and even the largest bank branch holds many fewer people at once than the smallest football stadium. These less demanding circumstances will require less computing power and correspondingly less money to implement. A few banks are also considering other biometrics for in-branch authentication. "The Chase Manhattan Bank, for example, is now using voiceprint identification for its retail customers within branches in order to expedite customer identification at the teller windows."[212] Chase ultimately wants to use biometrics "for legal signature purposes" but doubts that the law has adapted that far yet.[213]

The second major application that banks are exploring is remote account access, especially via telephone and the Internet. These tools "have made it easier for depositors to gain access to their funds on deposit [but] have also made it easier for nondepositors to gain access to account information and sometimes even to the funds themselves."[214] The banking industry embraced electronic commerce early and translated its ATM security system to this new context in order to get operations online quickly to meet burgeoning consumer demand.[215] Thus, the most prevalent security system pairs account numbers with secret, memorized PINs. Reliable desktop fingerprint scanners would obviate the need for customers to memorize these numbers while reducing the risk of illicit access. However, fingerprint scanners are still too expensive for

---

[210] *Id.*
[211] *Id.*
[212] Richard L. Field, *Digital Signatures: Verifying Internet Business Transactions*, 471 Practising L. Inst. 721, 725 (1997) ("Field 1"); Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Laws Affecting Electronic Banking in the United States*, 46 Am. U.L. Rev. 967, 987 (1997) ("Field 2").
[213] *Id.*
[214] Doheny and Forrer at 436-37
[215] Dunham

banks to distribute to all consumers.[216] In the meantime, some banks have adopted voiceprint systems for the telephone. Chase Manhattan Bank, for example, "hopes to use [its voiceprint] technology in the near future to permit remote telephone transactions."[217]

C. Specific Privacy Concerns and Legal Implications

1. Personal Privacy

All capturing of biometric data requires some infringement of the subject's personal space. Retina and finger scanning requires close proximity of biometric sensors to the body — within three inches of the eye for the retina and actual physical contact for the finger. "Because voiceprints are less intrusive than fingerprints or retina scans…they have been comparatively well received by customers."[218] In one of the few cases where a bank has conducted a detailed poll of consumers' reactions to iris scanning, Bank United in Texas claims that its customers reacted positively.[219] Additionally, few, if any, biometric applications can be forced on a consumer by a bank without at least nominal consent. A customer's granting of consent to be probed negates the initial and most formal privacy concern. However, once biometric systems become pervasive, consumers may lack any realistic exit option, and nonconsent might preclude a consumer from having a bank account. As chilling as this seems, concerns over informational privacy present even bigger problems.

The second major problem of personal privacy remains conveniently undiscussed by proponents of eye scanning technologies. Many authors of trade literature and marketing material warn that the accuracy of retina scanning may decrease over time because the pattern of

---

[216] The least expensive units still cost around $70 apiece. Bjorn, 701 PLI/Pat at 108.
[217] Field 1
[218] Chase
[219] Leslie J. Nicholson, *Iris-scanning ATMs Coming Online Today*, Dallas Morning News, 10 D (May 13, 1999) ("Nicholson")

blood vessels that constitute the biometric identifier may change over an adult's lifetime due to disease or trauma.[220] A few even admit that the wavelengths of light used for eye scanning are the same ones used by ophthalmologists to diagnose disease.[221] However, none discusses the ability of a program operator to collect such medical information about his customers illicitly. Recall that the Gramm-Leach-Bliley Act protects consumers from disclosure of their "personally identifiable financial information," which it defines as information "provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution."[222] Anything discovered during a biometric scan probably falls within the second or third prongs of this definition, so such information is probably safe from disclosure. However, the banker's mere knowledge of that information, even without subsequent disclosure, constitutes an invasion of personal privacy for which there was almost certainly no disclosure and informed consent.

2. Informational Privacy

Many people involved in the banking industry dismiss the informational privacy concerns surrounding biometrics. For example, Raj Nanavati, a partner at the consulting firm International Biometrics Group, "says the privacy spin is hyped…because biometrics don't add any sensitive information to what a bank already knows about its customers' financial affairs. 'If they add fingerprint identification, somebody there knows I have whorls and loops on my finger. So what?'"[223] Mr. Nanavati fails to recognize that, while the financial data already known to banks certainly carry a high degree of sensitivity, that data rarely, if ever, has a one-to-one correspondence to information about the customer held by third parties. Other merchants or

---

[220] *See e.g.*, Chang, Dye et al., and Rosenberg
[221] Predominantly visible light and near infrared. *See e.g.*, Dye et al. and IBG, *Iris-Scan*
[222] Gramm-Leach-Bliley § 509(4)(A)
[223] *Biometrics: Arthur C. Clarke, Where Are You?* Future Banker page 14 (1 June 2001)

government agencies may have records pertaining to that same customer, but no method yet exists that can easily link all these records to one another without time-consuming collusion. However, if each entity has a copy of the individual's biometric template, that template becomes a key that links disparate sources information in separate databases, kept by separate owners. Suddenly, anyone with access to these systems can quickly compile an intimate dossier of a persons life, showing his bank account records, employment information, medical records, and anything else linked to the biometric template. Such a frightening scenario might arise in several ways. Program operators may collude to track the individual; someone may gain unauthorized access to one or more systems and compile the information illicitly; or the government might collect such information, perhaps legitimately at first, as in a criminal investigation. Records compiled by the government have a knack for persisting long after their usefulness expires or appearing in unexpected places. Despite advance assurances by the FBI that the facial recognition system used at the 2001 Super Bowl in Tampa could identify only terrorists, all nineteen positive results flagged by the software "were only of ticket-scalpers and pickpockets, proving to critics that the database was filled with more than just terrorists or even felons."[224] Embarrassed, police made no arrests, despite confirming all nineteen positive matches.[225] All of these scenarios subject the consumer to a far more intimate form of profiling than anyone could perpetrate without biometric link between sources of information.

The Gramm-Leach-Bliley Act is the most obvious source of law protecting against abuses involving collusion between banks and third parties. The Act prohibits banks from sharing some information about consumers without their consent.[226] However, it describes

---

[224] Constantinou
[225] Patty Pensa, *Airport Officials: Face-Scan Security System Not Reliable*, South Florida Sun-Sentinel p. 3B (30 may 2002).
[226] *See supra*, pages 34-36 at notes 182-195 and accompanying text

private information alternatively as "nonpublic personal information"[227] and "personally identifiable financial information"[228] and expressly states that it protects only the latter.[229] Some might argue that biometric data do not fit within the Act's definition of "personally identifiable financial information." Recall that the Act defines this term to mean information "provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution"[230] but exempts any "publicly available information."[231] This exemption applies even if the bank obtains the publicly available information from the consumer at the same time and in the same manner that it obtains private information. Consumers may not know the difference and have no way of knowing what information a bank can find elsewhere. Thus, they cannot know in advance the scope of their privacy vis-à-vis their banks.

Congress charged various administrative agencies with implementing the Gramm-Leach-Bliley Act, which includes the task of defining "publicly available information." None has yet defined this term.[232] Therefore, it could arguably cover information that a bank obtains through collusion with another entity. The Gramm-Leach-Bliley Act applies only to banks, so collusion between a bank and a non-bank entity could circumvent the legislative intent behind the Act. Moreover, liability under the Gramm-Leach-Bliley Act appears to lie against only the bank that betrays a customer's confidence, not to third parties that receive that information and trade it further, to fourth and fifth parties. Analogizing to trade secret law, a consumer might recover damages against the bank that first misappropriates his private information, but the bank's

---

[227] *See* Gramm-Leach-Bliley § 502 and *supra*, page 34, note 183
[228] *See* Gramm-Leach-Bliley § 509(4)(A) and *supra*, page 36, note 193.
[229] *Id.*
[230] Gramm-Leach-Bliley § 509(4)(A)
[231] Gramm-Leach-Bliley § 509(4)(B)
[232] I have been unable to find any administrative agency definition of this term in the regulations implementing the Gramm-Leach-Bliley Act.

partner that received the illicit information might escape liability for further misappropriating that private information.

Some biometric programs will create gray areas where the Gramm-Leach-Bliley Act does not obviously apply. For example, "rapid pay" machines, which look and operate much like ordinary ATMs, cash checks for people without bank accounts.[233] Some of these machines already use iris scanning technology to identify repeat customers.[234] The Gramm-Leach-Bliley Act defines "consumer,"[235] but not what it takes to constitute a consumer-bank relationship. A "rapid pay" transaction does not obviously create such a relationship, so the users of such machines may not have any protection. Additionally, contracts of adhesion likely govern most use of rapid pay machines. Even if a consumer nominally consents to data sharing in a contract of adhesion, a court may decline to enforce the term permitting data sharing.[236] In another example, banks that issue debit cards (which often double as ATM cards) necessarily reveal a limited amount of information to merchants at the point of sale for the purpose of processing transactions initiated by the customer. Generally, customers authenticate a debit card transaction by entering a PIN on a keypad at the point of sale. As banks deploy biometrics in ATMs, PIN use will disappear, so biometrics must also replace PINs at the point of sale.[237] It may vary by contract whether the bank or the merchant bears the cost of authentication, and the bank has an

---

[233] Helen Stock, *Firm Uses Biometrics to Serve the Unbanked*, American Banker, 12 (1 Oct. 1999) ("Stock")
[234] *Id.*
[235] Gramm-Leach-Bliley § 509(9)
[236] Contract law varies by state, but several general principles governing contracts of adhesion are common. Generally, contracts of adhesion are enforceable, and consumers have a duty to read them, but courts generally interpret them narrowly with respect to the drafter of the contract. *See e.g.*, *Henningsen v. Bloomfield Motors*, 161 A.2d 69 (N.J. 1960). Terms that are not of the sort that a consumer would reasonably expect to be in such a contract are not enforceable. *See e.g.*, *Broemmer v. Abortion Services of Phoenix*, 840 P.2d 1013 (Ariz. 1992). A court would have to determine whether a term permitting sharing of the biometric template is reasonably foreseeable in the contract governing the use of rapid pay machines. Given the strictness of the confidentiality rules that traditionally apply to banks, the foreseeability of such a term is far from certain. *See supra*, pages 31-34 at notes 156-181 and accompanying text.
[237] *See Seattle Thriftway Supermarket Deploys Indivos' Pay By Touch Service*, BiometriTech (2 May 2002) (available at <http://www.biometritech.com/enews/050202c.htm>)

incentive to push that cost to the merchant. Thus, the bank's incentive may include providing the biometric template to the merchant for authentication[238] — something the Gramm-Leach-Bliley Act may or may not prohibit. If the customer voluntarily permits a biometric scan by the merchant, the template based on that biometric scan may constitute "publicly available information," which the Gramm-Leach-Bliley Act exempts from its protections. This would relieve the bank of any duty to keep its biometric template secret, and the consumer may never know that his first retail purchase with his new debit card constitutes permission for the bank to disclose of his biometric template to the world. However, until a regulatory agency or court definitively answers this question, banks make this assumption of consent at their own risk.

Illicit access to biometric information presents even more problems. "Security and trust are the lifeblood of a financial institution's existence. As the holders of sensitive and private data, financial institutions are obligated to ensure the highest levels of security. The obvious inadequacy of current systems, especially passwords, is causing the industry to investigate new technologies to enhance current security methods and replace those most susceptible to fraud. Decreasing costs, higher accuracy levels, smaller devices, and changing consumer attitudes have positioned biometric technologies as a very viable option."[239] Unfortunately, investment in securing biometric templates from theft has lagged behind investment in securing funds through biometric scanning. Large databases of biometric templates make an attractive targets for theft. Storing biometric templates on wallet cards that customers carry with them reduces the enticement for thieves to "hack" a biometric system. However, decentralized storage of templates does not obviate the need for transmission of both the biometric data to a computer for processing. Any electric or electromagnetic transmission is susceptible to tapping by third

---

[238] Barry
[239] *Id.*

parties. The Fourth Amendment forbids the government from intercepting such communications without a warrant, and many (perhaps all) states have statutes that prohibit private parties from tapping communications for illicit purposes.[240] Civil and criminal penalties may protect consumers and their banks from such wiretapping.[241] However, the law may protect consumers against the original perpetrator of the wiretap; but, as in the context of deliberate collusion among banks, there may be no secondary liability for those who later trade in the data.

D. Suggestions for Respecting Privacy in Biometrics Programs

Whether the public's currently heightened sensitivity to privacy threats will fade remains to be seen. The year 1995 appears to have been a turning point in the public's conception of privacy, stemming from a perceived breach of trust by corporations.[242] The current "privacy rights explosion" arose after "corporate abuses of information."[243] Developments in the name of national security following September 11, 2001 have simultaneously fueled the proponents and opponents of expanding privacy rights. We must consider any proposals in light of the long-term histories of information technology and privacy. If any proposed regulations would be limited to the banking industry, then the history of the consumer-bank relationship is also paramount. Congress and state legislatures are already subject to intense lobbying for legislation that would substantially curtail privacy rights.[244] Policy makers must bear in mind the ignominy of the telegraph's detractors and refrain from making rash decisions without hearing from proponents of privacy rights.

---

[240] *See e.g.*, 18 U.S.C. § 1343 (2002) (the Federal Wiretap Act), and Mass. Gen. Laws ch. 272 § 99 (2002) (prohibiting "Interception of wire and oral communications" without consent of all parties to the communication)
[241] *See e.g.,* U.S. Const. amend. IV; 42 U.S.C. § 1983 (2002); 18 U.S.C. § 1343 (2002); Mass. Gen. Laws ch. 272 § 99 (2002)
[242] *See California Commerce Bank Utilizes Biometrics*, Biometric Digest, 2-6 (Feb. 2001)
[243] *Id.*; Schellberg at 3
[244] Schellberg at 3

Any regulatory system should encompass all phases of a biometric program (enrollment, template storage, data capture, transmission, or comparison), for it matters little to the customer during which phase his privacy is violated. Even the termination of a biometric program requires regulatory attention; the former operator of a defunct biometric program may still control a database of templates, ripe for abuse. Sale of that database in a bankruptcy might remove all protection that the Gramm-Leach-Bliley Act provided. Blunt groupings of industries by any body of law may produce conflicts among the laws that control any individual industry. Any unified approach to biometric regulation must bend to accommodate conflicting industry-specific regulations and different economic realities across industries. A biometric rule drafted intelligently with respect to banks might be senseless if applied to airports. This danger counsels in favor of an industry-by-industry approach. Unfortunately, this segmented approach would leave entities that operate in two or more fields to comply with potentially conflicting sets of regulations and leave consumers to deal with many different regulatory systems all at once. Abstaining from regulation to give industries a chance for self-regulation would fragment privacy protections even further, leaving consumers unable to determine their rights overall and creating many different vested interests that would make future regulation even more difficult.[245] Therefore, we must begin to regulate biometrics soon and find some compromise on the scope of those regulations.

One approach solves the difficulties outlined above: enactment of a broadly applicable set of default rules for biometric programs that applies to all industries, which permits individual companies and consumers to alter rules by contract. This approach would create a baseline of

---

[245] *See* International Biometric Group, *Best Practices for Privacy-Sympathetic Biometric Deployment* <http://www.bioprivacy.org/best_practices.htm> (accessed 20 Sept. 2002); *Visionics Corp Calls for Legislation to Safeguard Against Misuse of Face Recognition Technology*, Biometric Digest, 1 (Sept. 2001); *International Biometric Group Announces BioPrivacy Impact Framework*, Business Wire (28 Aug. 2001)

privacy for consumers, demand a close examination of privacy rights by all biometric program operators, and permit sufficient flexibility for different contexts. Program operators have many incentives to contract away from the baseline protections toward lower standards of protection but few, if any, incentives bringing them toward stronger protections. Therefore, the baseline of privacy must tightly restrict the ways in which program operators may use and share biometric data. If we identify any specific privacy right as so sacred that no private contract should alter it, we may codify that special exemption from alterability in the law.[246] This approach to biometric regulation would protect unwary consumers from harm, allow informed customers to consent to permissive programs, and permit flexibility for growth.

Two major difficulties confront this approach, but each is answerable. First, Congress is often loath to enact broad legislation, preferring instead to enact laws sector-by-sector.[247] The intensity of lobbying it would face on such a bill would render quick action impossible. Creating a new biometric regulatory agency to handle the minutia through administrative rulemaking may only divert lobbying and may not speed the initial codification process, but such an agency could react faster than Congress to problems that arise in the future. Second, most companies enjoy significant bargaining power over individuals, so those that choose to alter the baseline protections would likely use contracts of adhesion. Few consumers will read these contracts carefully, and the enforceability of their terms will necessarily be uncertain.[248] While these concerns tend to tip the balance of power away from individuals, the law controlling contracts of adhesion will maintain some core protections. Unfortunately, this protection through contract law comes only after costly litigation by individual consumers — and probably long after the

---

[246] The Copyright Act of 1976, 17 U.S.C. § 101 *et seq*, provides a precedent for this. The Copyright Act permits an author to transfer a copyright to a third party, but the author retains a right to terminate that transfer after 35 years. Section 203 of the Act provides that any purported waiver of this right before the 35th year is unenforceable.
[247] Reidenberg at 208; *see also supra*, page 31, note 156 and accompanying text
[248] *See supra*, page 45, notes 233-236 and accompanying text, regarding contracts of adhesion

damage is irreversible. However, protecting one's own privacy in the absence of regulation may prove impossible, so the possibility of protection with some expense is an improvement.

The International Biometric Group's (IBG) BioPrivacy Initiative has published a set of "best practices" that purports to encompass all biometric applications in all industries.[249] While many of its provisions are too vague to be useful, IBG's proposal provides a starting point for a set of regulations. The most useful provisions speak directly to specific concerns about personal or informational privacy.

During the design phase, IBG recommends that the program operator should analyze risks according to the intended uses of the system *and* potential future uses or abuses. Failure to consider the second category of risks would constitute an abdication of the operator's responsibility to maintain the system responsibly. Second, the operator must clearly define program's scope and periodically grant access an independent auditor to assess the operator's compliance with this definition. The operator would, of course, make the auditor's reports available at least to customers and perhaps to the public as well. Third, the operator should plan scenarios for suspending the program and, if necessary, immediate destruction of biometric templates in the event of a security breach or misuse by an insider that puts customers' privacy at risk. Fourth, the operator must offer an alternative to the biometric program to all customers who decline to enroll. The functionality of this alternate system must mimic the functionality of the biometric system as nearly as possible; otherwise, the specter of second-class service would effectively coerce many dissenting customers into the biometric program.

---

[249] International Biometric Group, *Best Practices for Privacy-Sympathetic Biometric Deployment* <http://www.bioprivacy.org/best_practices.htm>. IBG is a consulting firm serving the biometrics industry, which sells biometric products and services to other businesses. The provisions that are summarized following this note all appear on the page cited here and are not individually footnoted.

The IBG proposal also calls for protections of informational privacy. First, the program operator should isolate data storage and transmission equipment used for biometrics from all other systems to prevent accidental mingling — thereby limiting the possible damages from illicit access by outsiders. Second, the operator should restrict access to biometric data to employees responsible for maintaining the biometric system, for no others would have any legitimate reason for accessing biometric data. Third, the operator should handle backup copies of biometric data according to the same security protocols that apply to the primary copy of the data. Fourth, the program should automatically destroy the raw image from any biometric scan immediately after it extracts the data required for comparison to minimize the amount of human-readable information that a thief could want to steal. Finally, the program operator must promptly destroy the biometric data of any customer who leaves the program. Retention of other records regarding that customer may serve legitimate purposes, but no legitimate purpose would justify the retention of biometric data.

VI. Conclusion

We can declare only one thing about biometrics with confidence: neither the "pie in the sky" promises of the biometrics industry nor the "doom and gloom" warnings of privacy activists has yet been realized. If we do nothing, market forces will pull and tug biometrics into an equilibrium somewhere between these two extremes — most likely one that leans away from strong privacy protections. We must address these issues now, before many players' interests grow too vested in the status quo. We must examine them in their proper historical context, realizing that technology advances faster than the law and often faster than politics. Proponents of biometrics may complain that a full societal examination of the implications of their technology will take too long and that strong privacy protections will impose high costs on the

fledgling industry, but we have a moral duty to act before they destroy privacy and extinguish the voices of their opponents. Without immediate democratic deliberation on biometrics, the technology will advance to a point where we feel dependent on it. By then, deliberation will be too late.