July 2015

Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy

Lisa Jane McGuire

BANKING ON BIOMETRICS: YOUR BANK'S NEW HIGH-TECH METHOD OF IDENTIFICATION MAY MEAN GIVING UP YOUR PRIVACY

Beverly Dennis, hoping to receive free samples in the mail, completed a marketing survey.[1] To her surprise, she not only received those free samples; she also received the attentions of a convicted rapist.[2] What the Ohio grandmother did not know when she filled out her questionnaire was that her answers were sent to a Texas prison, where inmates would later process her personal information.[3] Ms. Dennis is not alone. Many privacy horror stories appear in the news on a regular basis.[4]

Now imagine this – your insurance company obtains a detailed list of your shopping habits,[5] finding that you regularly purchase high-fat foods, red

---

[1] Ms. Dennis completed a questionnaire for Metromail Corp., a direct marketing firm, revealing information such as her address, date of birth, marital status and level of income. James Rule & Lawrence Hunter, *Privacy Wrongs: Corporations Have More Right to Your Data Than You Do*, WASHINGTON MONTHLY, Nov. 1996, at 17.

[2] *Id*. Hal Parfait, a Texas inmate convicted of breaking into his neighbor's house and raping her, sent Ms. Dennis a twelve-page sexually explicit letter. *ABC Primetime Live: Inmates, Inc.* (ABC television broadcast, Feb. 18, 1998). Parfait bought Ms. Dennis' information from a fellow inmate working for Metromail Corp. *Id*. What is most troubling is that he purchased her information for a mere twenty-five cents. *See id.*

[3] *See id*. Prison labor is used for a variety of purposes by both private companies and governmental agencies. *See id*. Some companies hire prisoners for telemarketing purposes and taking airline ticket reservations. *Id*. In 1998, inmates in thirty-three states processed personal information. *Id*. Ms. Dennis sued Metromail and the prison system, and Metromail no longer uses prison labor. Mike Ward, *Ex-prison Official Indicted Over '93 Data-entry Deal; Related Suit*, AUSTIN AMERICAN-STATESMAN, Sept. 26, 1998, at B3. In 1995, Texas barred prisons from accepting work from private companies. *Id*.

[4] For example, Mallory Hughes of Florida received a letter from televangelist Oral Roberts, suggesting that, for a donation, Roberts would intercede with God on Hughes' behalf, to help Hughes with a debt problem. Sandra Byrd Petersen, Note, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED. COMM. L.J. 163, 166 (1995). When Margaret Davis of California discovered she was pregnant, she ordered a maternity catalog. She received catalogs and offers for free samples from other companies. Unfortunately, Ms. Davis miscarried. The offers still came, even after the Davis' contacted the companies to tell them to remove their name from mailing lists. Some companies even sent birthday cards around the time her baby was to be born, and Ms. Davis received telephone calls congratulating her on the new addition to her family. It finally got to the point where Davis' husband had to screen the phone calls and open all the mail. *Id*. at 167

[5] More than half of all grocery stores in the United States offer discounts and incentives to their shoppers if the shoppers participate in the frequent shopper, or loyalty card, programs. Robert O'Harrow, Jr., *Bargains at a Price: Shopper's Privacy; Cards Let Supermarkets*

meat, alcohol, and tobacco products.[6] Worse yet, your insurance company learns that you may suffer from diabetes, high blood pressure, or any number of other disorders.[7] Without warning, you are considered to be a high risk and your rates increase. The problem is that the insurance company did not obtain this information from your medical insurance claim form. Instead, your insurance company found out from examining data gathered from your bank's newest method of customer identification.[8]

As scary as the previous scenarios sound, they are not only possible, but also very likely if action is not taken soon. The abundance of computers, both at the office and at home, has made it much easier and more profitable for companies to gather and disseminate information that most Americans would

---

Collect Data, WASHINGTON POST, Dec. 31, 1998, at A01 ("Six of ten supermarket companies electronically collect customer data or plan to soon, about twice the proportion at the beginning of the decade, according to the Food Marketing Institute."). The customer trades information about herself in order to obtain these discounts, as the stores track sales through a magnetic stripe card. *Id*. The stores can then target their coupons to specific customers, based on the customers' buying habits. *Id*. Some stores claim that the program fosters customer loyalty. *Id*. Others claim that they can better serve customers by monitoring particular sales. *See* R.J. Ignelzi, *It's in the Cards; Frequent-shopper Discounts Sometimes Net a Loss of Privacy*, SAN DIEGO UNION-TRIB., Apr. 7, 1998, at E-1. Tracking a customer's sales reaps benefits for government agencies as well. One store acknowledged that, pursuant to subpoenas issued by the Drug Enforcement Administration (DEA), the store released information on customers' purchases. *Id*. The DEA was interested in whether a suspected drug dealer purchased a large supply of plastic sandwich bags, which are often used to package drugs. *Id*.

[6] *See* Petersen, *supra* note 4, at 168-69 (noting that insurance companies could monitor your shopping habits to see if you regularly purchased items that would indicate an unhealthy lifestyle). The California legislature responded to the proliferation of supermarket loyalty cards and possible detrimental effects on privacy by enacting the Supermarket Club Card Disclosure Act of 1999. *See* S.B. 926, 1999-00 Cal. Leg., Reg. Sess. (1999) (to be codified at CAL. CIV. CODE § 1749.60 – 1749.65). Effective July 1, 2000, the Act prohibits stores from selling and sharing personal information except under certain specified circumstances. *See id*.

[7] Certain medical information may be inadvertently obtained from different methods of biometric identification. *See infra* note 184. Biometrics refers to the method of verifying the identity of an individual based on a particular trait such as a fingerprint, voice pattern, or other physical or behavioral characteristic. *See infra* notes 18-22 and accompanying text.

[8] New methods of identification in the banking industry include the use of biometric identifiers. *See infra* notes 71-82 and accompanying text. The recently-enacted Gramm-Leach-Bliley Financial Modernization Act removes previous restrictions on the financial service industry, now allowing banks, brokerage firms, and insurance companies to affiliate into one institution. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999). *See infra* notes 141-148 and accompanying text.

consider private.[9] The ease with which companies buy and sell a consumer's private information, most often without the consumer's knowledge,[10] must be restricted. Americans need some way to protect themselves from threats to their privacy.[11]

I. INTRODUCTION

The vast amount of information stored in databases is increasingly subject to computer hackers and other unauthorized users. Some concerns over the storage and dissemination of this information, other than those previously mentioned, are the potential for identity theft and fraud.[12] In order to reduce the fears of fraud and misuse of personal information, government agencies and private corporations are turning to the high-tech world of biometrics to be sure that you are who you say you are.[13] But what is the

---

[9] *See* William J. Fenrich, Note, *Common Law Protection of Individuals' Rights in Personal Information*, 65 FORDHAM L. REV. 951, 951 (1996) (noting that we leave an information trail through birth, death, and marriage records, by using a credit card or supermarket loyalty card, and by writing a check). *See also* Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1395 (1987) (noting the ease with which companies gather and release information due to the use computerized databases).

[10] There is currently a profitable $1.5 billion market in personal information – information that is "largely hidden from public view." Joel Reidenberg, *Restoring Americans' Privacy in Electronic Commerce*, 14 BERKELEY TECH. L.J. 771, 776 (1999) (noting the privacy problems specific to electronic commerce).

[11] This article concerns privacy as "information privacy," generally defined as "the right to control how information about oneself is used by those to whom it is disclosed." Petersen, *supra* note 4, at 166. (calling for a Congressionally created right to information privacy). Informational privacy is also described as "freedom from unwanted disclosure of personal data." Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on the Mechanisms For Privacy Protection*, 4 WM. & MARY BILL OF RTS. J. 455, 458 (1995).

[12] *See generally* Kristen S. Provenza, Notes & Comments, *V. Privacy: Identity Theft: Prevention and Liability*, 3 N.C. BANKING INST. 319, 319 (1999). Provenza details a rather scary story of a man who purchased vehicles, incurred debt, and broke various laws – all using someone else's identity. *See id.* Almost everyone knows someone who has had a similar experience. The author of this comment was contacted a few years ago from her county's Department of Human Services when someone (other than this author) attempted to obtain state entitlement benefits using her social security number.

[13] *See, e.g., Check Fraud: Check Fraud Losses Rising Rapidly Despite Banks' Growing Use of Technology*, BNA BANKING DAILY, May 2, 1997, at D2. Financial institutions in California, using a fingerprinting program, noted an eight-five percent decrease in losses from check fraud. *See* Phil Britt, *High-tech Identification Systems Come of Age; Biometrics in Banks; Includes Related Article on Privacy*, AMERICAN'S COMMUNITY BANKER, June 1998, at 22. In

gathering of this very personal information doing to the privacy rights of American citizens? This comment attempts to answer that question and then presents possible safeguards to ensure the safety of our own biometric identities.

This Comment investigates privacy implications stemming specifically from the use of biometrics in the banking industry. Part II of this comment defines biometrics.[14] The various types of, and uses for, this technology are presented in this section. Part III investigates the right to privacy.[15] The history of the right of an individual to protect her privacy is then presented, and the sources of this fundamental right are identified. Part IV details the modern trend of the use of biometrics in the banking industry.[16] An analysis is then made concerning the implications of privacy protection of this information. This comment concludes in Part V with suggestions for potential legislation necessary to protect biometric information gathered for identification and verification purposes in the banking industry.[17]

II. BIOMETRICS

"Biometrics" refers to the techniques and methods used to identify individuals based on a physical characteristic or particular trait unique to that individual.[18] While the name may sound like something out a popular science-fiction movie,[19] the idea behind using biometrics for identification and

---

Charlotte, North Carolina, First Union reported a forty percent decrease during the first year of its fingerprinting program. *See Id*.

[14] *See infra* notes 18-31 and accompanying text.

[15] *See infra* notes 84-114 and accompanying text.

[16] *See infra* notes 183-193 and accompanying text.

[17] *See infra* notes 207-231 and accompanying text.

[18] *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium). The Biometric Consortium serves as "a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification/authentication technology." Joseph P. Campbell, Jr., *et al*., *Government Applications and Operations*, in CTST GOVERNMENT CONFERENCE PROCEEDINGS (1996), available at <http://www.biometrics.org/REPORTS/CTSTG96> (visited Oct. 23, 1999). *See also* John D. Woodward, Article, *Biometric Scanning, Law & Policy: Identifying the Concerns – Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 99 (1997).

[19] The use of biometrics has fascinated moviegoers for many years. Mission: Impossible, Demolition Man, True Lies, and the many James Bond movies have depicted various forms of biometric identification. *See, e.g*., Richard Des Ruisseaux, *High Tech ID: Prepare to Have Your Body Parts Scanned*, COURIER-JOURNAL (Louisville, KY), July 13, 1998, at 01C.

verification certainly is not new.[20] The procedure in different systems varies, but generally consists of four steps.[21] Upon enrollment, the physical characteristic or trait is scanned, and the unique features are converted into a digital code.[22] The code is then stored, either in a database, on a smart-card, or in a barcode format.[23] When the individual seeks access to the system, she is scanned again and compared to the digital code that has previously been stored.[24]

Biometrics can be used for identification, in comparing one person to the complete database of information.[25] Biometrics is also used to verify that the user is who he claims to be.[26] The reliability and suitability for a particular purpose depends on the type of biometric identifier used. The biometric

---

[20] For instance, fingerprinting as a means of identification has been used in the criminal law arena since the early 1900's. *See* Vincent J. Gnoffo, Article, *Requiring a Thumbprint for Notarized Transactions: The Battle Against Document Fraud*, 31 J. MARSHALL L. REV. 803, 803-804 (1998) (providing a brief history of fingerprinting in the criminal law setting and analyzing California's requirement of a thumbprint for all notary services). *See also* Frederick M. Avolio, *Buyer's Guide: Biometrically Speaking*, NETWORK COMPUTING, Aug. 23, 1999. Even retinal scanning is not new. The technology behind scanning the retina as a means of identification has been available since 1976. Sharon Latka-Davis, *IrisIdent ATM Security System Catches Eye of Bankers*, TELEGRAM & GAZETTE (Worcester, MA), July 22, 1996, at C1.

[21] Bill Siuru, *Iris Recognition Systems*, ELECTRONICS NOW, Feb. 1999, at 41.

[22] *Id*.

[23] *Id*.

[24] *Id*.

[25] *See* Campbell, *et al*., *supra* note 18 ("Biometric recognition can be used in *identification* mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match.") (emphasis in original). This is also called "one-to-many matching." *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium). *See also* Woodward, *supra* note 18, at 100 ("Identification is defined as the ability to identify a person from among all those enrolled, i.e. all those whose biometric measurements have been collected in the database. Identification seeks to answer the question: 'Do I know who you are?'").

[26] *See* Campbell, *et al*., *supra* note 18 ("A [biometric] system can also be used in *verification* mode, where the biometric system authenticates a person's claimed identity from his/her previously enrolled pattern.") (emphasis in original). This is also referred to as "one-to-one matching." *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium). *See also* Woodward, *supra* note 18, at 100 ("[Verification] involves the authentication of a person's claimed identity from his previously enrolled pattern. Verification seeks to answer the question: ' Are you who you claim to be?'").

system should be user-friendly and accurate,[27] and it must be based on a distinguishable trait.[28] Ideally, the system would also collect data in a non-intrusive manner[29] and operate at a high speed.[30] The technology is becoming more widely used, as prices fall and the systems become more financially viable.[31]

[27] Accuracy in biometrics is described by three terms: (1) the false acceptance rate (defined as the percentage of imposters accepted), (2) the false rejection rate (defined as the percentage of authorized users the system rejects), and (3) the equal-error rate (described as the process of adjusting the decision threshold so that the false acceptance rate equals the false rejection rate). Campbell, *et al*., *supra* note 18. *See also* Woodward, *supra* note 18, at 101. "The better biometric systems have low equal error rates of less than 1%." *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium).

[28] Campbell, *et al*., *supra* note 18.

[29] Woodward, *supra* note 18, at 101. Part of the notion of a system being non-intrusive is the minimal amount of contact between the scanning device and the person being scanned. *See id*.

[30] Woodward, *supra* note 18, at 101.

[31] James Menendez, *Biometrics useful in health care, e-commerce; Technology Information*, COMPUTING CANADA, April 16, 1999, at 25 ("Until recently, the technology was extremely expensive, but falling chip and scanner prices have made biometric solutions feasible for even the smallest applications, including personal desktop PCs."). "The price of biometric devices has plummeted. Five years ago, the smallest fingerprint reader sold by Identicator Technology was the size of a telephone and cost $2,000; today, it's the size of two sugar cubes and sells for $99. In five years, a similar gizmo may cost $15." Pamela Sherrid, *You Can't Forget This Password: Hint: It's Your Face, Iris, or Fingerprint*, U.S. NEWS & WORLD REPORT, May 17, 1999, at 49.

A. Types of Biometric Identifiers

Biometrics ranges from the more common fingerprinting to highly sophisticated retinal scans. On the low end of reliability[32] lie facial imaging or face recognition,[33] hand geometry,[34] voice recognition,[35] and signature recognition.[36] These systems are less reliable partly because changes occur to the physical aspects of the biometric identifier over time.[37]

---

[32] *See* Woodward, *supra* note 18, at 105-107. Woodward categorizes the various biometric identifiers into what he refers to as "high," "lesser," and "esoteric" biometrics. ("The use of the High Biometrics, Lesser Biometric and Esoteric Biometrics categories is done for organizational purposes. . . ; the categorization is not based on any rigorous technical formula.") *Id*. at 102, n.29.

[33] "Face recognition is a noninvasive process where a portion of the subject's face is photographed and the resulting image is reduced to a digital code." Woodward, *supra* note 18, at 106. The system by Visionics uses a camera that can take an acceptable picture from hundreds of feet away. Ashley Dunn, *The Cutting Edge; The Password is Biometrics; High-Tech Identification Systems are Moving Into Corporate and PC Worlds, Offering Log-On Security in the Blink of an Eye or the Tap of a Finger*, L.A. TIMES, Dec. 7, 1998, at C1.

[34] Hand geometry measures the length, width, and height of the hand and fingers. *See* Woodward, *supra* note 18, at 105. One advantage of a hand geometry system is the fact that it requires a small amount of computer storage, as opposed to some of the other methods. *See id*. at 106.

[35] "Voice recognition involves taking the acoustic signal of a person's voice and converting it to a unique digital code which can then be stored in a template." Woodward, *supra* note 18, at 107. Usually, the user repeats a pre-determined phrase for identification. *See id*. Systems measure voice cadence, tone and pitch to determine a match. *See* Britt, *supra* note 13, at 22.

[36] In the arena of biometrics, signature recognition, also referred to as signature dynamics, is not merely the comparison of two signatures. *See* Woodward, *supra* note 18, at 107. Instead, the system compares the shape and speed of the letter strokes, the pressure one puts upon the writing instrument, and the number of times the writing instrument leaves the surface. *Id. See also* Mary Deibel, *Biometrics: The New Wave of Identification*, DESERET NEWS (Salt Lake City, UT), June 2, 1999, at C02.

[37] Injuries to the hand can affect hand geometry. Rajiv Chandrasekaran, *Brave New Whorl; ID Systems Using the Human Body are Here, But Privacy Issues Persist*, WASHINGTON POST, Mar. 30, 1997, at H01. *See also* Woodward, *supra* note 18, at 106. Similarly, facial hair may affect facial recognition, and identical twins or others who look alike can compromise the system. *Id*. Emotions and illness can affect voice patterns. *Id*. at 107. Background noises can also affect voice recognition systems. Chandrasekaran, *supra* note 37, at H01. Signature recognition faces similar disadvantages, as injuries to the hand affect the way a person signs her name. Dunn, *supra* note 33, at C1.

Biometric identifiers with a high degree of reliability[38] include retinal scanning,[39] iris scanning,[40] and fingerprinting. These biometric identifiers are less likely to change over time, and are unique to the individual.[41] However, these methods have their disadvantages as well.[42]

---

[38] The retina and the iris are more reliable than fingerprints, because they contain more "discriminators," or identification points. John D. Woodward, Comment, *Biometrics Offers Security But Legal Worries, Too*, AMERICAN BANKER, Aug. 23, 1996, at 11. The iris contains more than 400 such discriminators, while the average fingerprint has only 68. Latka-Davis, *supra* note 20, at C1. *But see* Kurt Loft, *Eye on Tomorrow; The Information Obtained From a Simple Scan of Your Eye's Iris Could Replace the Need for ATM Cards and the PINs That Go With Them*, TAMPA TRIBUNE, July 26, 1999, at 4 (noting that fingerprints contain approximately 35 reference points, while the iris has 266).

[39] Retinal scanning is a process that maps the vein pattern of one's retina, the innermost layer of the eye. Woodward, *supra* note 18, at 102-103. A beam of light bounces off the retina, and the pattern of the retina's blood vessel structure is reduced to a digital code. *Id*. at 103.

[40] Similar to retinal scanning, iris scanning maps the variation in the iris, the colored portion of the eye. Woodward, *supra* note 18, at 103. Computers sort through the iris's identifying features of the corona, pits, filaments, crypts, striation, radial furrows and other structures. Loft, *supra* note 38, at 4. A video camera takes a high-resolution image of the iris. Dunn, *supra* note 33, at C1. An accurate image can be captured from three feet away, and a match can be made in two or three seconds. *Id*. Systems can scan the iris through contact lenses and most glasses, except reflective sunglasses. Loft, *supra* note 38, at 4.

[41] However, one reporter suggests that systems based on IriScan and other companies specializing in iris scanning can be compromised by the use of a high-resolution photograph. Dunn, *supra* note 33, at C1. *But see* Siuru, *supra* note 21, at 41 ("Since the technique relies on the physiological response to light and natural pupillary oscillation, it cannot be fooled by a photograph or another substitute for a real human eye."). *See also How the Eyeball Scanner Will Know It's You*, ST. LOUIS POST-DISPATCH, June 5, 1996, at 5C ("The camera shoots the iris several times, verifying in seconds that the pupil moves and thus that it is a real eye rather than a photo."). Dunn also comments that a carefully constructed artificial finger can fool a fingerprint scanner and morbidly suggests that a freshly severed finger can also circumvent the system. Dunn, *supra* note 33, at C1. *Cf.* Joe War, *Ex-Louisvillian Pioneers Access to Computers by Fingerprint*, COURIER-JOURNAL (Louisville, KY), May 30, 1999, at 01E (The technology of finger scanning can differentiate between live fingers and dead fingers, artificial fingers and live fingers, and photographs.).

[42] *See, e.g*. Chandrasekaran, *supra* note 37, at H01. Iris recognition often requires a large amount of computer memory. *Id*. Retinal scanning often requires close physical contact, and many suggest that the method may not receive public approval. *Id*. Fingerprinting or finger imaging is not well suited in some environments, such as manual laborers or construction workers who may not be able to provide an acceptable scan. Ross Snel, *On-Line Banking: Factors Found to Affect Accuracy of Biometric identification Systems*, AMERICAN BANKER, Apr. 1, 1999, at 13. *See also* Chandrasekaran, *supra* note 37, at H01. The system can be set up to compensate for injuries. Joe Ward, *supra* note 41, at O1E. If one finger is injured, the customer just substitutes with a previously scanned finger. *Id*. Residue on the fingers also

The use of biometrics for identification and verification implicates concerns from many sectors. The use of biometric identifiers worries privacy advocates as well as religious groups.[43] Pat Robertson, founder of the Christian Coalition, believes that the Bible foretells of the danger associated with the increased use of biometric identifiers.[44] He announced that "[t]he Bible says the time is going to come when you cannot buy or sell except when a mark is placed on your hand or forehead."[45] Other problems stem from some cultures objecting to the physical aspects of scanning.[46] Also, some people may fear that the scanners contribute to the spread of germs.[47] Other disadvantages relate to the development of systems that adequately accommodate the disabled.[48]

B. Applications of Biometrics

---

affects the system, and natural oils present in the skin may adhere to the scanner, creating difficulties for future scanning. Woodward, *supra* note 18, at 105. Similarly, weather conditions may create problems for scanning equipment when the scanner becomes wet and dirty from users coming in from winter weather. Britt, *supra* note 13, at 22.

[43] Chandrasekaran, *supra* note 37, at H01.

[44] *See* Chandrasekaran, *supra* note 37, at H01. *See also* Eric Niiler, *Human Bar Codes; Forget Those Passwords, Biometrics is the Future – and Present – Identifier*, SAN-DIEGO UNION-TRIBUNE, May 13, 1998, at E-1 ("[Religious leaders] point to biblical warnings about the 'mark of the beast' in the Book of Revelations that described a world in which everyone was required to have three 6's tattooed on their forehead and right hand in order to buy or sell goods in the pre-apocalyptic world.").

[45] Chandrasekaran, *supra* note 37, at H01.

[46] The Japanese and other Asian cultures are adverse to the physical aspects of some of these systems. Woodward, *supra* note 18, at 104, n.47.

[47] Germs can be transferred from one user to the next when the users share a scanner. *See* Chandrasekaran, *supra* note 37, at H01. However, systems using iris or retinal scanning do not require physical touching. *See supra* notes 38-42. Therefore, these systems do not implicate any fears of transferring germs from one user to the next.

[48] Chandrasekaran, *supra* note 37, at H01. Kevin McQuade, the president of marketing for Sensar, one of the companies currently marketing iris-scanning equipment for use in Automatic Teller Machines, noted that the system accommodates anyone from the four-foot-nine to six-foot-nine range. Latka-Davis, *supra* note 20, at C1. That range should accommodate wheelchair users. *Id*. McQuade also notes that one form of cancer alters the iris over time. *Id*. Individuals suffering from tremors, as those with advanced stages of Huntington's Disease or Parkinson's Disease, may encounter problems with inaccurate data. *Id*. Blind individuals can still use a system based on iris recognition if their irises are intact. Loft, *supra* note 38, at 4.

Biometrics has many applications from varied governmental functions[49] to those utilized in private organizations.[50] Government applications range from military[51] and national security measures[52] to the use in law enforcement and prison population identification.[53] Recently, there has been a movement in the states to use biometrics in efforts to prevent welfare fraud.[54] Other

[49] In the Turkish Parliament, finger scanners guarantee that it is the members themselves casting votes. Ruisseaux, *supra* note 19, at O16. Jamaica uses biometrics for their national registration system. *Reports from the States*, in BIOMETRICS HUM. SERV. USER GROUP (Conn. Dep't of Soc. Serv.), Aug. 1999, available at <http://www/dss.state.ct.us/digital/news15/bhsug15.html> (visited Oct. 23, 1999). The Jamaican government issues cards to citizens for a variety of purposes including voter registration, health-care benefits and driver's licenses. *Id*.

[50] In 1998, the United States government was the largest user of biometrics. Deibel, *supra* note 36, at C02. During that year, the government spent $140 million on biometric equipment, while private industries spent only $33 million. *Id*.

[51] In Fort Sill, Oklahoma, military officials issue basic training inductees a stored value card using fingerprint recognition for various military services like shopping at the PX , buying clothes, and getting haircuts. *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium). A similar program was being tested on military retirees who receive benefits overseas. *Id*.

[52] Woodward, *supra* note 18, at 109. *See also* Campbell, *et al*., *supra* note 18. Biometrics ensures security at the Pentagon, the White House, and missile silos. Ruisseaux, *supra* note 19. Retina scanning devices control access to secure areas for the CIA, the FBI, and NASA. Eric Slater, *Not All See Eye to Eye on Biometrics; Iris and Fingerprint Scanners May Soon Come to the Corner Bank or Market, Critics Fear Loss of Privacy and Theft of Electronic Identities*, L.A. TIMES, Apr. 28, 1998, at A1.

[53] The Cook County Sheriff's Department in Illinois reportedly uses eye scanning to ensure the identity of prisoners. Chandrasekaran, *supra* note 37, at H01. Persons under house arrest in some areas check in with the authorities by using a voice recognition system. *Id*. In Pennsylvania, the Lancaster County Prison releases prisoners only after verifying their identity through iris scanning. Slater, *supra* note 52, at A1. The Sarasota County Detention Center in Florida was installing a similar system. Siuru, *supra* note 21, at 41.

[54] Woodward, *supra* note 18, at 110. The General Accounting Office (GAO) estimates the costs of fraud in state entitlement programs as over $10 billion a year. Campbell, *et al*., *supra* note 18. As of March 1998, the states using biometric identifiers included Arizona, California, Connecticut, Illinois, Massachusetts, New Jersey, New York and Texas. CONNECTICUT DEP'T OF SOC. SERV., REPORT TO THE GENERAL ASSEMBLY DSS DIGITAL IMAGING PROJECT (1998). While most states' programs use finger imaging, Massachusetts was testing facial imaging, and Sacramento County, California was using hand geometry. *Id*. Connecticut has since chosen to use facial recognition. *Reports from the States*, in BIOMETRICS HUM. SERV. USER GROUP (Conn. Dep't of Soc. Serv.) June 1999, available at <http://www/dss.state.ct.us/digital/news14/bhsug14.html> (visited Oct. 23, 1999). The use of finger imaging in state entitlement programs prevents an individual from registering under

governmental uses include controlling international borders and immigration,[55] preventing unauthorized access to secured buildings and computer systems,[56] and monitoring driving records of certain commercial drivers.[57]

---

multiple names. *See generally* James J. Killerlane III, Note, *Finger Imaging: A 21st Century Solution to Welfare Fraud at our Fingertips*, 22 FORDHAM U. L.J. 1327 (1995) (detailing the problem of fraud in entitlement programs). *See also* Jennifer K. Constance, Comment, *Automated Fingerprint Identification System: Issues and Options Surrounding Their Use to Prevent Welfare Fraud*, 59 ALB. L. REV. 399 (1995) (presenting potential Constitutional invasion of privacy and due process concerns in the use of fingerprint identification for welfare programs). One of the problems in using fingerprints as a method of identification is that applicants may feel stigmatized because the most common use of fingerprints is by law enforcement officials in solving crimes. *See id*. at 406-407. *But see Few See Stigma in Fingerprinting, Survey Indicates*, AMERICAN BANKER, Dec. 23, 1996, at 2A (relating data that seventy-five percent of those subjects surveyed felt "somewhat comfortable" or "very comfortable" with the use of fingerprint scans to prevent identity fraud).

[55] The United States Immigration and Naturalization Service (INS) implemented a system at several airports in the United States to ease check in of frequent international travelers. Woodward, *supra* note 18, at 111. Called INSPASS (INS Passenger Accelerated Service System), this system allows frequent travelers to the United Stated to forego the traditional personal interview and inspection portion of the entry process, providing quicker admission. Campbell, *supra* note 18. INSPASS uses hand geometry for verification. *Id*. The traveler enters a previously-issued card into an automated machine, enters his flight number, and places his hand into the hand geometry reader. United States Immigration and Naturalization Service (INS) Office of Inspections, *INS Passenger Accelerated Service System (INSPASS) Briefing Paper*, available at <http://www.biometrics.org/REPORTS/INSPASS2.html> (visited Oct. 23, 1999). If the hand geometry pattern matches that obtained when the traveler enrolled in the program, the traveler gains admission. *Id*. Travelers currently use INSPASS at international airports in Los Angeles, California; Miami, Florida; Newark, New Jersey; New York (JFK) and San Francisco, California. *Id*. Enrollment in the INSPASS program is open to citizens of the United States, Bermuda, and Canada who do not have a criminal record and travel to the United States at least three times a year. *Id*. An enrollment form may be obtained via the Internet at <http://www.ins.usdoj.gov/graphics/formsfee/forms/i-823.htm>.

Canada uses a version of INPASS called CANPASS. Ronald J. Hays, INS, *INS Passenger Accelerated Service System (INSPASS)*, available at <http://www.biometrics.org/REPORTS/INSPASS.html> (visited Oct. 23, 1999). The system in Canada is similar but uses fingerprint scanning instead of hand geometry. *Id*. CANPASS is used at Vancouver International Airport, with the goal of easing the transfer of people and goods between Canada and the United States. Campbell, *supra* note 18. In Scobey, Montana, officials at the United States-Canadian border use a voice recognition system to assist in border crossings. Woodward, *supra* note 18, at 110.

The INS also has a program called PORTPASS. *See id*. PORTPASS uses voice recognition at a vehicle crossing at the United States-Canadian border. *Id*.

At the United States-Mexican border at Otay Mesa, a facial recognition system is in place to ease travel between the two countries. *See* Niiler, *supra* note 44, at E1. As the

In response to the increasing use of biometrics, the Biometrics Consortium was chartered in 1995 by the Facilities Protection Committee, a committee that reports to the Security Policy Board.[58] The Biometrics Consortium is a working group to "serve as a Government focal point for research, development, test, evaluation, and application of biometric-based personal identification / authentication technology."[59] While the Biometrics Consortium deals exclusively with governmental applications, the group also assesses issues that arise in varying biometric applications.[60]

---

vehicle approaches the border in a special commuter lane, a transponder attached to the vehicle signals the booth and activates the system. *Id*. The driver's facial features are then compared to information compiled in the database. *Id*. The system saves time for those travelers who often commute between the two countries. *Id*.

[56] Woodward, *supra* note 18, at 111.

[57] Woodward, *supra* note 18, at 111, n.107. Through the use of biometric identifiers in identifying commercial drivers, the government can better monitor their driving records, in response to concerns that some drivers obtained licenses in multiple states to reduce the appearance of traffic violations. *Id*. Congress mandated that the Secretary of Transportation adopt standards that include requirements that commercial licenses issued after January 1, 2001 "include unique identifiers (which may include biometric identifiers) to minimize fraud and duplication." 49 U.S.C. § 31308(2) (1999). California is one state that requires a thumbprint or fingerprint on every application for a driver's license, treating commercial licensees the same as all other drivers. *See* CAL. VEH. CODE § 12800 (Deering 1999). The California Supreme Court addressed the collection and dissemination of fingerprint data in *Perkey v. Dep't of Motor Vehicles*, 721 P.2d 50 (Cal. 1986). The Court held that the fingerprint requirement did not violate due process. *Id*. at 53. However, the Court found that the department's dissemination of fingerprint data for purposes unrelated to motor vehicle safety violated several provisions of the state's civil and vehicle codes. *Id*. at 53-54.

[58] *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of Jeffrey S. Dunn, Chairman, Biometric Consortium). President William Clinton established the Security Policy Board. *Id*.

[59] *Id*. (quoting the Biometric Consortium's Charter).

[60] Lisa A. Alyea and Dr. Joseph P. Campbell, Jr., *Update on the US Government's Biometric Consortium*, available at <http://www.biometrics.org/REPORTS/CTST96/> (visited Oct. 23, 1999).

Biometrics is also useful in the private sector. Preventing unauthorized access to computers is just one of many possible applications.[61] In this arena, biometrics replaces a personal identification number (PIN) or password that protects company information from unauthorized access.[62] PIN's or passwords can be lost or forgotten. More importantly, they can be stolen, compromised or observed by prying eyes. Because biometric identifiers are unique to the individual, only the person with a match is allowed access.[63]

The list of possible applications in the private sector is endless.[64] However, some of the more common uses are automated time and attendance records[65] and security measures.[66] Walt Disney World in Orlando, Florida reportedly uses a hand scanning system to prevent unauthorized use of season passes.[67] Biometric identifiers are also being used to limit the sale of alcohol and tobacco to minors.[68] Biometric technology even found its way into the Olympics, when hand-scanning devices controlled access to the Olympic Village during the Atlanta, Georgia Olympic Games.[69] Similarly, an iris recognition system monitored access to weapons in the Nagano, Japan Winter Olympics.[70]

---

[61] James Menendez, *supra* note 31, at 25. Finger-scanners can be attached to computers to eliminate the need for passwords. Chandrasekaran, *supra* note 37, H01. Charles Schwab & Co. uses finger imaging for security checks on employees. Woodward, *supra* note 38, at 11.

[62] Another method similar to biometrics, called the Biopassword, can be used in conjunction with passwords. Dunn, *supra* note 33, at C1. This technology monitors computer keystrokes, determining the differences between typists based on the typist's speed and cadence. *Id*. Biopassword is very affordable, but because the system measures typing rhythm in milliseconds, it is easily subjected to injuries in the hands and fingers. *Id*.

[63] The match does not need to be exact. *See* Britt, *supra* note 13, at 22. In fact, variables in the user and the equipment invariably dictate that the match will never be exact. *See id*. (noting that "[t]here will always be some distortion introduced by the user, the screen or the screening environment").

[64] It seems that any application is possible in the private sector. BMW is investigating the use of fingerprint scanners to deter car theft. *See* Slater, *supra* note 52. BMW hopes to design a car that starts only after the system identifies the correct driver by his fingerprint. *Id*. In the near future, spectators may not even need a ticket to gain access to sporting events, as a system using biometric identifiers is under development that would automatically debit or charge the individual's account. Siuru, *supra* note 21, at 41. The gun industry may see biometrics as a novel safety device. *See* Elizabeth Weise, *Body May Be Key to a Foolproof ID*, USA TODAY, Apr. 8, 1998, at 4D. Only the registered gun-owner, with a matching fingerprint, will be able to fire it. *Id*.

[65] Coca-Cola Co. replaced time cards with hand-scanning machines. Chandrasekaran, *supra* note 37. Woolworth stores in Australia also substituted time clocks with biometrics, using a system of finger scanning. Slater, *supra* note 52, at A1.

[66] The use of security systems based on biometrics ranges from applications in places with very limited access to common places where the public in general would not expect such high

technology. Fingerprint scanners limit access to the inner vault of the Encino, California branch of Century Bank. Slater, *supra* note 52, at A1. Wells Fargo Bank uses hand geometry to prevent unauthorized access to the bank's data centers. Kate Henry, *Biometrics Prevent Sleight of Hand at Wells Fargo*, ACCESS CONTROL & SECURITY INTEGRATION, August 1999. An elementary school in New Mexico, also using a hand geometry system, prevented a father who lost a custody fight from attempting to pick up his child. *See* Deibel, *supra* note 36, at C02.

[67] Weise, *supra* note 64, at 4D. In a somewhat related application, the University of Georgia has used a hand geometry system since 1972 to identify students on the unlimited meal plan, thus preventing them from loaning their cards to others. *Id*.

[68] Vending machines in Salem, Utah compare a user's fingerprints with information stored on a magnetic stripe card to ensure that the customer is eligible to purchase such age-restricted items like tobacco and alcohol. *Biometric Vending Machines in Full Swing at Salem Store*, SUPERMARKET NEWS, Oct. 4, 1999, at 32.

[69] Chandrasekaran, *supra* note 37, at H01.

[70] Officials regulated access to rifles and ammunition used in the biathlon at the Winter Olympics in Nagano, Japan with an iris recognition system. Weise, *supra* note 64, at 4D.

The use of biometrics is also catching on in the banking industry. Customers without a bank account wishing to cash a payroll check are often required to provide a fingerprint or thumbprint.[71] Some banks even require a thumbprint when a customer opens an account.[72] In a related application, one retail store uses fingerprint scanners to verify the identity of a customer wishing to write a check for her purchase.[73] MasterCard International and Visa USA Inc. are studying the use of point-of-sale finger-scanners to prevent fraud by verifying that the shopper truly is the authorized credit card user.[74]

Voice recognition software can be used in the banking industry to control access to account information.[75] The technology can be linked with existing telephone information systems.[76] Voice recognition would be most useful in situations when customers wish to transfer funds or obtain account balances by telephone.[77]

---

[71] *See generally* Patrick J. Waltz, Comment, *On-Site Fingerprinting in the Banking Industry: Inconvenience or Invasion of Privacy*, 16 J. MARSHALL J. COMPUTER & INFO. L. 597 (1998) (discussing privacy concerns associated with fingerprinting as a requirement for check cashing). Several banks in Colorado, Utah, Nevada, Arizona, and Texas require a fingerprint before cashing a check for a non-account holder. *Colorado Banks to Fingerprint to Stem Fraud*, ACLU NEWS WIRE, July 30, 1996, available at <http://www.aclu.org/news/w073096a.html> (visited Sept. 9, 1999). The procedure is as follows: the customer provides a fingerprint in order to cash a check. If the check clears, nothing is done with the print. If the check is forged or counterfeit, the bank gives the check and the fingerprint to law enforcement. *Id*. Florida banks are following suit. *Banks Increasingly Turn to Fingerprints*, ACLU NEWS WIRE, Jan. 8, 1997, available at <http://www.aclu.org/news/w010897b.html> (visited Sept. 3, 1999). Instead of the traditional ink and paper method of fingerprinting, Florida banks use inkless pads to obtain the thumbprint of customers. *See id*. No ink remains on the customer's finger, but an ink-like fingerprint appears on the check. Britt, *supra* note 13, at 22.

[72] Great Western Bank in Florida requires a thumbprint before customers open an account. *Banks Increasingly Turn to Fingerprints*, ACLU NEWS WIRE, Jan. 8, 1997, available at <http://www.aclu.org/news/w010897b.html> (visited Sept. 3, 1999).

[73] Fingerprint scanners are used in Kroger stores in Texas. Sunil Taneja, *Keep an Eye on Biometrics*, CHAIN STORE AGE EXECUTIVE WITH SHOPPING CENTER AGE, July 1, 1999. The system is voluntary for personal checks but mandatory for those customers wanting to cash payroll checks. *Id*.

[74] Chandrasekaran, *supra* note 37, at H01.

[75] Sherrid, *supra* note 31, at 49.

[76] *Id*. Chase Manhattan Bank investigated the use of voice recognition software to ensure proper access to account information given over the telephone. Woodward, *supra* note 38, at 11.

[77] *See* Sherrid, *supra* note 31, at 49.

The trend of using biometric identifiers for identification at banks has led to their use at many Automatic Teller Machines (ATM's). The Purdue Employees Federal Credit Union at Purdue University uses finger imaging at remote ATM's.[78] Rapid Pay Machines, self-service check-cashing machines, use facial recognition to identify customers.[79] Banks in Texas use iris scanning for identification of their customers.[80] Customers of those banks do not even need an ATM card.[81] These machines use iris recognition in identification mode, matching the customer's iris to all those enrolled in the system.[82]

What does the collection of such personally identifiable information mean to the privacy of American citizens? In order to reach an answer to that question, the right to privacy in the United States must first be examined.

III. THE RIGHT TO PRIVACY

"Privacy is like freedom: we do not recognize its importance until it is taken away. In that sense, it is a personal right that we assume we have yet take for granted – until something or someone infringes upon it."[83]

A. Background of the Right to Privacy

[78] *Technology: Banks' Future Security Could Be Built on Biometrics House Banking Panel Told*, BNA BANKING DAILY, May 21, 1998.

[79] Helen Stock, *Firm Uses Biometrics to Serve the Unbanked*, AMERICAN BANKER, Oct. 1, 1999, at 12. The rapid pay machines are aimed towards those individuals without bank accounts. *Id*. A similar system was first used by Mr. Payroll. *Id*. These companies cash checks for a fee, marketing their services toward those individuals without access to traditional bank accounts. *Id*.

[80] Bank United installed ATM's inside certain Kroger grocery stores in Dallas, Houston, and Fort Worth, Texas. Leslie J. Nicholson, *Iris-scanning ATMs Coming Online Today*, DALLAS MORNING NEWS, May 13, 1999, at 10D.

[81] *Id*. The ATM's cameras are directly linked to the database that contains the customer's previously installed iris pattern. *Id*.

[82] *See id*. Other biometric ATM systems store the customer's identification information in his ATM card or on a smart-card, rather than in the bank's database. *Id*. *See infra* note 25-26 (describing the difference between identification and verification).

[83] David H. Flaherty, Symposium, *The Right to Privacy One Hundred Years Later:* Article*: On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE. W. RES. 831 (1991).

Neither the text of the United States Constitution nor the Bill of Rights explicitly mentions the right to privacy. However, the right to privacy is regarded as one of the most fundamental of rights.[84] One of the problems in fashioning an appropriate scheme for privacy protection is the plethora of ways in which to define privacy.[85]

B. Sources of Privacy Protection

[84] *See, e.g.*, 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."). *See also* Griswold v. Connecticut, 381 U.S. 479, 494 (1965) (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)). In *Griswold*, Justice Harlan felt that the natural law approach was the acceptable way to recognize privacy as a fundamental right. *Griswold*, 381 U.S. at 499 (Harlan, J., concurring). *See also* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 11.7, at 390 (4th ed. 1991).

[85] *See* BeVier, *supra* note 11, at 458 ("Privacy is a chameleon-like word; used denotatively to designate a range of wildly disparate interests – from confidentiality of personal information to reproductive autonomy – and connotatively to generate good will on behalf of whatever interest is being asserted in its name."). *See also* Richard S. Murphy, Article, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996). Murphy describes the right to privacy as follows:

> The phrase "right to privacy" is a bit of a chameleon. Its uses range from the right to be free from physical invasion of one's home or person, the right to make certain personal and intimate decisions free from government interference, and the right to prevent commercial "publicity" of one's own name and image, to name three.

Id. Murphy's article concerns the right to privacy as defined as the "control of information concerning an individual's person." *Id*. Black's Law Dictionary defines an invasion of privacy as "an unjustified exploitation of one's personality or intrusion into one's personal activity, actionable under tort law and sometimes under constitutional law." BLACK'S LAW DICTIONARY 829 (7th ed. 1999).

Privacy receives protection from many sources. The United States Constitution protects individuals from governmental intrusion into privacy in varying contexts.[86] Federal legislation protects invasions of privacy in a variety of industries and circumstances.[87] Constitutions and statutes of many states similarly provide protection for their citizens.[88] Various actions are also available under common law.[89]

1. Privacy Protections Under the United States Constitution

As noted earlier, the right to privacy is not explicitly mentioned in the Constitution. However, in *Griswold v. Connecticut*,[90] the United States Supreme Court first held that the guarantees in the Bill of Rights create "zones of privacy."[91] "[The] specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance,"[92] thus creating "zones" of privacy. Since *Griswold*, the Court has extended privacy protection to areas concerning marital decisions,[93] reproductive choices,[94] and judgments relating to the rearing and education of children.[95]

---

[86] Most of the amendments to the United States Constitution explicitly protect an individual from governmental intrusion. *See infra* notes 107-109 and accompanying text.

[87] *See infra* notes 115-148 and accompanying text.

[88] *See infra* notes 149-154 and accompanying text.

[89] *See infra* notes 155-182 and accompanying text.

[90] 381 U.S. 479 (1965).

[91] *Id.* The *Griswold* Court struck down a Connecticut statute prohibiting the distribution and use of contraceptives among married couples. *Id*.

[92] *Id*.

[93] *See generally* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 14.28 (4th ed. 1991). *See also* Loving v. Virginia, 388 U.S. 1 (1967) (holding that Virginia's law banning interracial marriages violates the Equal Protection Clause).

[94] *See generally* NOWAK & ROTUNDA, *supra* note 84 §§ 14.27 and 14.29. *See* Roe v. Wade, 410 U.S. 113 (1973) (invalidating a Texas law banning all abortions except to save the life of the mother). *See also* Skinner v. Oklahoma, 316 U.S. 535 (1941) (holding that an Oklahoma law that required the sterilization of all habitual criminals violated the Equal Protection Clause of the Fourteenth Amendment). In *Bowers v. Hardwick*, 478 U.S. 186 (1986), the Court declined to extend the right to privacy to include the right of homosexuals to engage in consensual sodomy. The *Bowers* Court limited the right to "a fundamental individual right to decide whether or not to beget or bear a child." *Id*. at 190.

[95] *See* Pierce v. Society of Sisters, 268 U.S. 510 (1925) (invalidating an Oregon law that required all children aged eight to sixteen to attend public school). *See also* Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (finding that a Nebraska statute that prohibited the teaching of subjects in schools in any language other than English was unconstitutional). In *Prince v. Massachusetts*, 321 U.S. 158 (1944), the Court stated that "the custody, care and nurture of the child reside first in the parents, whose primary function and freedom include

The right of association in the First Amendment[96] creates one such zone of privacy.[97] Similarly, the Third Amendment[98] protects the privacy of one's home.[99] The Fourth[100] and Fifth[101] Amendments protect against government intrusions "of the sanctity of a man's home and the privacies of life."[102] The Court has said that the Ninth Amendment[103] also creates zones of privacy.[104] The Fourteenth Amendment[105] finds some support among the Justices for creating a right to privacy.[106]

---

preparation for obligations the state can neither supply nor hinder." *Id* at 166. *See also* Moore v. City of East Cleveland, 431 U.S. 494 (1977)

[96] "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. CONST. amend. I

[97] *Griswold*, 381 U.S. at 483-84. Freedom of association is a peripheral First Amendment right. *Id*. *See also* NAACP v. Alabama, 377 U.S. 288, 307 (1964).

[98] "No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law." U.S. CONST. amend. III.

[99] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[100] The Fourth Amendment provides:

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

U.S. CONST. amend. IV.

In Mapp v. Ohio, 367 U.S. 643 (1961), the right to privacy created by the Fourth Amendment was described as "a right to privacy, no less important than any other right carefully and particularly reserved to the people." *Id*. at 656.

[101] "No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law. . ." U.S. CONST. amend. V. "The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." *Griswold*, 381 U.S. at 484.

[102] *Id*. (quoting Boyd v. U.S., 116 U.S. 616, 630 (1886)).

[103] "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people." U.S. CONST. amend. IX.

[104] In his concurring opinion in *Griswold*, Justice Goldberg stated that "[t]o hold that a right so basic and fundamental and so deep-rooted in our society as the right of privacy in marriage may be infringed because that right is not guaranteed in so many words by the first eight amendments to the Constitution is to ignore the Ninth Amendment and to give it no effect whatsoever." Griswold v. Connecticut, 381 U.S. 479, 491 (1965) (Goldberg, J., concurring).

[105] "No state shall make or enforce any law which shall abridge the privileges or immunities of

Regardless of which Constitutional Amendment creates a right to privacy, the Constitution only protects an individual from government actors infringing that individual's privacy.[107] The Thirteenth Amendment, prohibiting slavery, is the only Amendment that regulates conduct of individuals or private entities rather than action by the government.[108] "With respect to the conduct of private individuals, the Supreme Court has been reluctant to find a privacy right in personal information given voluntarily by an individual to private parties."[109]

---

citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws." U.S. CONST. amend. XIV, § 1, cl. 2.

[106] Waltz, *supra* note 71, at 602 ("Some Supreme Court Justices also suggest that the Fourteenth Amendment independently preserves privacy rights," citing Meyer v. Nebraska, 262 U.S. 390, 399 (1923) (finding that a Nebraska statute that prohibited the teaching of subjects in schools in any language other than English was unconstitutional)). In *Meyer*, the Court described the liberty guaranteed by the Fourteenth Amendment as "not merely freedom from bodily restraint but also the right of the individual to contract, to engage in any of the common occupations of like, to acquire useful knowledge, to marry, establish a home and bring up children, to worship God according to the dictates of his own conscience, and generally to enjoy those privileges long recognized at common law as essential to the orderly pursuit of happiness by free men." (citations omitted) *Meyer*, 262 U.S. at 399. As Justice Harlan stated in *Griswold*:

> [T]he proper constitutional inquiry in this case is whether this Connecticut statute infringes the Due Process Clause of the Fourteenth Amendment because the enactment violates basic values 'implicit in the concept of ordered liberty.' While the relevant inquiry may be aided by resort to one or more of the provisions of the Bill of Rights, it is not dependent on them or any of their radiations. The Due Process Clause of the Fourteenth Amendment stands, in my opinion, on its own bottom.

Griswold, 381 U.S. at 500 (Harlan, J. concurring). *See also*, Roe v. Wade, 410 U.S. 113 (1973) (invalidating a Texas law banning all abortions except when to save the life of the mother) ("This right of privacy, whether it be founded in the Fourteenth Amendment's concept of personal liberty and restriction upon state action, as we feel it is, or, as the District Court determined, in the Ninth Amendment's reservation of rights to the people, is broad enough to encompass a woman's decision whether or not to terminate her pregnancy.").

[107] State action is required in order to prevail on a claim for invasion of a federal constitutionally-based right of privacy. *See generally*, NOWAK & ROTUNDA, *supra* note 84 at §§ 12.1. Joint participation between the government and a private actor is considered state action. Burton v. Wilmington Parking Authority, 365 U.S. 715, 725 (1961) (holding that a restaurant located on state-owned property and operating under a lease of said premises could not discriminate). State action is not established merely because the government is involved in some way. There must be a close nexus between the private and government action. Jackson v. Metropolitan Edison Co., 419 U.S. 345, 350-51 (1974) (holding that a

The closest the Court came to identifying a right to information privacy was in *Whalen v. Roe*.[110] In upholding a New York state law, which required the recording of the names and addresses of individuals prescribed certain drugs,[111] the Court noted, in dicta, "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[112] However, the Court upheld the law, finding that it was rationally related to a legitimate governmental goal of controlling the distribution of illegal drugs.[113] The Court did not reach any decision concerning "the unwarranted disclosure of accumulated private data – whether intentional or unintentional – or by a system that did not contain comparable security provisions."[114]

2. Federal Statutory Privacy Protection[115]

---

decision by a highly regulated utility company to discontinue service is not state action unless the state was actively involved in the decision or otherwise coerced it). A mere scheme of regulations is not sufficient for state action. *See* Moose Lodge v. Irvis, 407 U.S. 163, 176 (1972) (holding that mere regulations like liquor licensing are not sufficient state action for the Fourteenth Amendment to apply). The "public function doctrine" stands for the proposition that even a private enterprise may meet the state action requirement if it performs a function that is traditionally and exclusively a government function. *See* Marsh v. Alabama, 326 U.S. 501 (1946) (holding that company-towns serve a public or governmental function so that the First Amendment freedom of speech protections apply).

[108] *Hearing on Biometrics and the Future of Money Before the Subcomm. on Domestic and Int'l Monetary Policy Comm. on Banking and Fin. Serv.*, 105th Cong., 2nd Sess. (1998) (statement of John D. Woodward, Attorney-at-Law) (citing Smith v. Maryland, 442 U.S. 735 (1979) and United States v. Miller, 425 U.S. 435 (1976).

[109] *Id*.

[110] 429 U.S. 589 (1977).

[111] The New York State Controlled Substances Act of 1972, N.Y. Pub. Health Law § 3300 *et seq*. (McKinney, Supp. 1976-1977), required doctors and pharmacists to provide the State with copies of prescriptions for medicines containing narcotics for which there is a lawful and unlawful market. *Whalen,* 429 U.S. at 591. *See also,* NOWAK & ROTUNDA, *supra* note 84 at § 14.30.

[112] *Whalen*, 429 U.S. at 605.

[113] *Id* at 597-98.

[114] *Id*. at 605-606.

[115] This section presents only a sampling of federal statutory provisions, with an emphasis on those statutes specific to financial institutions. It is beyond the scope of this article to detail every federal statute with privacy provisions. For a more in depth analysis, see Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier For Individual Rights?,* 44 FED. COMM. L.J. 195, 209-21 (1992).

There are several federal statutes designed to protect a citizen's privacy. However, most of them provide protections only from a governmental agency intruding into a citizen's privacy. For example, the Privacy Act of 1974[116] requires governmental executive agencies to follow certain procedures in the collection and disclosure of the personal information that these agencies collect.[117] The Tax Reform Act of 1976[118] similarly provides that the IRS should limit the disclosure of an individual's tax information.[119]

Congress enacted most of these statutes reactively, rather than proactively. That is, Congress acted only as a reaction to some other event. For example, Congress passed the Driver's Privacy Protection Act (DPPA)[120] in reaction to the stalking death of actress Rebecca Schaeffer.[121] The DPPA regulates the indiscriminate dissemination of personal information contained in motor vehicle records.[122] Various states challenged the Act on several bases,[123] one of which was that Congress infringed on the states' powers under the Tenth Amendment.[124] The federal circuit courts that ruled on the issue are split, with two holding that the Act is unconstitutional, and two finding that it is a valid exercise of Congressional power.[125]

---

[116] 5 U.S.C. § 552(a) (1999).

[117] *Id*.

[118] Pub. L. No. 94-455, 90 Stat. 1520 (codified in scattered sections of 26 U.S.C.).

[119] *See* 26 U.S.C. § 6103.

[120] 18 U.S.C. §§ 2721-2725 (1999).

[121] After an unsuccessful attempt to present tokens of affection to Rebecca Schaeffer, John Bardo hired a private investigator to determine his favorite actress's home address. Tracy Wilkinson, *Murder Suspect's "Obsession" Foretold in Studio Visit*, L.A. TIMES, Aug. 2, 1989, at 1. The private investigator obtained her address by purchasing the information from the California Department of Motor Vehicles. *Id*. Bardo went to her house, where he found her and shot her to death. *Id*. No federal or California law existed at the time to prevent the release of information on a driver's license. *See* Oliver J. Kim, Note, *The Driver's Privacy Protection Act: On the Fast Track to National Harmony or Commercial Chaos?*, 84 MINN. L. REV. 223, 223-24 (1999) (presenting the background of the Driver's Privacy Protection Act (DPPA) and concluding that the DPPA is a constitutionally permissible exercise of federal authority).

[122] For instance, states must provide drivers with an option to opt out of the mass distribution of their information. 18 U.S.C. § 2721 (1999). There are several exceptions to the DPPA, such as allowing the release of information to insurance companies, employers of commercial drivers, and to law enforcement agencies. *Id*. *See also* Kim, *supra* note 121, at 241-43.

[123] For a full discussion of the arguments for and against the constitutionality of the Driver's Privacy Protection Act, *see* Thomas J. Odom and Gregory S. Feder, *Challenging the Federal Driver's Privacy Protection Act: The Next Step in Developing a Jurisprudence of Process-Oriented Federalism Under the Tenth Amendment*, 53 U. MIAMI L. REV. 71 (1998) (noting that states are challenging the DPPA based on the First, Tenth, Eleventh, and Fourteenth Amendments, as well as on the Commerce Clause and the Guarantee Clause). *See also*, Kim,

The future of the Act is unknown, as the United States Supreme Court granted certiorari in one of the cases in May of 1999 and heard oral arguments in November, 1999.[126] Recently, Congress acted in response to the court battles over the DPPA by amending the Act and placing restrictions in the Appropriations Act for the Department of Transportation and related agencies for the fiscal year 2000.[127]

---

supra note 121, at 223. Several states took in a considerable amount of money through the sales of driver's license information prior to the passage of the DPPA. *Hearing in Support of H.R. 3365 – the Driver's Privacy Protection Act Before the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm.,* (Feb 3, 1994) (statement of Janlori Goldman, Director, American Civil Liberties Union). In one year, New York received $17 million, and Wisconsin made $8 million per year. *Id*. *See also* Travis v. Reno, 163 F.3d 1000, 1002 (7th Cir. 1998), *petition for cert. filed*, 67 U.S.L.W. 3717 (U.S. May 11, 1999) (No. 98-1818). In a related news article, a New Hampshire company was reported to purchase license photographs from some states in hopes of building a national database for use in the fight against retail fraud. *Some States Sell Drivers' Photos; W. Va. Motor Vehicle Official Questions Legality of Sales*, CHARLESTON DAILY MAIL, Feb. 2, 1999, at 10A. The company designed a system that displayed the driver's license photo of a shopper writing a check or using a credit card to ensure her identity. *Id*. The company acquired 14 million photographs of Florida drivers and more than 5 million from Colorado. *Id*.

[124] The Tenth Amendment delegates those powers not specifically enumerated in the Constitution to the States. "The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people." U.S. CONST. amend. X.

[125] *See* Condon v. Reno, 155 F.3d 453 (4th Cir. 1999) (finding that the Act is unconstitutional), *cert. granted*, 119 S.Ct. 1753 (U.S. May 17, 1999) (No. 98-1464); Pryor v. Reno, 171 F.3d 1281 (11th Cir. 1999) (same), *petition for cert. filed*, 68 U.S.L.W. 3079 (U.S. July 6, 1999) (No. 99-61); Travis v. Reno, 163 F.3d 1000 (7th Cir. 1998)(determining that the Act is constitutional), *petition for cert. filed*, 67 U.S.L.W. 3717 (U.S. May 11, 1999) (No. 98-1818); Oklahoma *ex rel.* Okla. Dep't of Pub. Safety v. U.S., 161 F.3d 1266 (10th Cir. 1999) (same), *petition for cert. filed*, 67 U.S.L.W. 3684 (U.S. May 3, 1999) (No. 98-1760).

[126] Condon v. Reno, 155 F.3d 453 (4th Cir. 1999).

[127] Pub. L. No. 106-69, 113 Stat. 986 (1999). The Act places certain restrictions on those states accepting funds, such as not disseminating driver's license personal information except as permitted under the DPPA, and requiring a person's consent before releasing a driver's license photograph, social security number, or medical and disability information. *Id*. at § 350. The Act further amends the DPPA by allowing the release of information in certain instances only after the consumer gives express consent. *Id*. (modifying 18 U.S.C. § 2721(b)). This particular provision is not conditioned on the receipt of federal funding, and, unlike the other restrictions, would continue to be in effect after the 2000 fiscal year. *Id*. *See also* Petitioner's Supplemental Brief at 3-5, Reno v. Condon (U.S.S.Ct. Oct. 20, 1999) (No. 98-1464).

Like the DPPA, the Video Privacy Protection Act[128] was enacted as a reaction to other events, in this case, to the events surrounding the confirmation hearings of Supreme Court nominee Robert Bork.[129] Commonly known as Bork's Bill, the Video Privacy Protection Act was enacted only after a newspaper article revealed which movies Bork rented from his neighborhood video store.[130] In commenting on the Video Privacy Protection Act, Senator Leahy echoed the thoughts of Samuel Warren and Louis Brandeis,[131] voiced over 100 years ago, that Americans "want to be left alone."[132]

Many statutes specifically regulate the banking industry. For instance, after the Supreme Court, in *United States v. Miller*,[133] held that microfilm records of a bank customer's activity were business records and not entitled to personal privacy protection, Congress responded by enacting the Financial Privacy Act of 1978.[134] The Financial Privacy Act of 1978 protects certain customer financial records from disclosure.[135]

---

[128] 18 U.S.C. § 2710 (1999). The Video Privacy Protection Act provides relief for the unauthorized disclosure of video rental records in the form of civil remedies such as actual damages of a minimum amount of $2500, punitive damages, and attorneys' fees. 18 U.S.C. § 2710(c). The Cable Communications Policy Act of 1984 similarly regulates the disclosure of the viewing habits of cable subscribers. *See* 47 U.S.C. § 551 (1999).

[129] *See generally*, Joshua D. Blackman, *A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector*, 9 SANTA CLARA COMPUTER & HIGH TECH. L.J. 431, 432-33 (1993) (providing examples of invasion of privacy due to the lack of laws regulating the dissemination of personal information).

[130] Aaron Epstein, *Bork's Right to Privacy Inspires Bill; Would Veil Library, Video Borrowings*, THE RECORD (NORTHERN NEW JERSEY), May 11, 1988, at A08. The article noted that Bork's interest in movies ranged from Alfred Hitchcock mysteries to sophisticated comedies. *Id*. The article went on to say that Bork appeared to be a "PG-to-G" type of person and that he rented "nothing racier than a fleetingly topless Vanessa Redgrave in 'Blowup.'" *Id*.

[131] Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). This seminal article is discussed further in *infra* notes 156-157.

[132] S. Rep. No. 100-599, at 6 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342. Senator Leahy's full comment was "[privacy] is not a conservative or a liberal or moderate issue. It is an issue that goes to the deepest yearnings of all Americans that we are free and we cherish our freedom and we want our freedom. We want to be left alone." *Id*.

[133] 425 U.S. 435 (1976).

[134] 12 U.S.C. §§ 3401-3422 (1999). *See* Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L. Q. 461, 482 (1999).

[135] 12 U.S.C. §§ 3401-3422 (1999).

The Fair Credit Reporting Act,[136] (FCRP), also applies to financial institutions. The FCRP regulates the disclosure of consumer credit information.[137] By and large, the FCRP does not speak to the accumulation of information, but does address the accuracy of a credit reporting agency's information.[138] As a result of abusive, deceptive, and unfair practices in debt collection, often resulting in invasions of privacy,[139] Congress enacted the Fair Debt Collection Practices Act of 1977.[140]

On November 16, 1999, President Clinton signed the Gramm-Leach-Bliley Act, also known as the Financial Modernization Act of 1999.[141] The Gramm-Leach-Bliley Act removes former restrictions on banks and other financial institutions, allowing them to enter the securities market and to merge with insurance companies.[142] The new conglomerates can freely share information with affiliates within the organization, without the consumer's consent.[143]

Currently, this is the only wide reaching federal legislation in the United States to prevent financial institutions from buying and selling personal information without the individual's permission. The information distributed would include the biometric information collected by the banking industry, whether the information is gained from iris scans, fingerprints, or thumbprints.

---

[136] 15 U.S.C. § 1681–1681(u) (1999).

[137] The FCRA prohibits consumer credit reporting agencies from disclosing consumer data except in specified circumstances. *See id.*

[138] *See id*. *See also,* Reidenberg, *supra* note 115, at 211-12.

[139] *See* 15 U.S.C. § 1692(a) (1999).

[140] 15 U.S.C. § 1692-1692n (1999).

[141] P.L. 106-102, 113 Stat. 1338 (1999) (to be codified at scattered sections of 12 U.S.C. and 15 U.S.C.).

[142] *See id*. *See also,* Jane Bryant Quinn, *Banking Overhaul May Lower Prices But Strip Privacy*, ORLANDO SENTINEL, Nov. 20, 1999, at B1. The Gramm-Leach-Bliley Act repeals portions of the Glass-Steagal Act, which forbid affiliations between banks and securities firms, and amends the Bank Holding Company Act, which restricted affiliations between banks and insurance companies. The White House, *Statement by the President*, M2 PRESSWIRE, Nov. 16, 1999.

[143] *See* Quinn, *supra* note 142, at B1. ("Financial institutions will be able to hand out personal information from your bank account, brokerage account or insurance records to all of its divisions and affiliates."). As part of the requirement that banks disclose their privacy policy, consumers will know what information will be shared with the banks' affiliates. Stephen Horn, Representative, House, *Modernizing Banking, Protecting Privacy*, CONGRESSIONAL PRESS RELEASES, Nov. 18, 1999.

However, the Gramm-Leach-Bliley Act provides exceptions to the restrictions on the sharing of personal information.[144] Financial institutions may release information to a third party if the third party is acting on behalf of the bank and will keep the information confidential.[145] Similarly, the Act allows the release of information to third parties with whom the banks have a joint marketing arrangement.[146] This means that some telemarketers will still have access to private, personal information.[147] The Act also provides exceptions for law enforcement use.[148]

3. Privacy Protections Found in State Constitutions and Statutes

Many state constitutions provide a more explicit right to privacy of their citizens than that found in the United States Constitution.[149] However, most require state action in order for the plaintiff to prevail.[150]

---

[144] Gramm-Leach-Bliley Act.

[145] *See* Horn, *supra* note 143; Gramm-Leach-Bliley Act.

[146] *See* Horn, *supra* note 143; Gramm-Leach-Bliley Act.

[147] *See* Quinn, *supra* note 142.

[148] Gramm-Leach-Bliley Act.

[149] Below is a sampling of state constitutional privacy provisions:

Alaska: "The right of the people to privacy is recognized and shall not be infringed." ALASKA CONST., art. I, § 22. Alaska's constitutional privacy protections apply only to state actors. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1129-30 (Alaska 1989).

Arizona: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." ARIZ. CONST. art. II, § 8. Courts in Arizona maintain that this protection only applies against the State. *See* Hart v. Seven Resorts Inc., 947 P.2d 846, 850 (Ariz. Ct. App. 1997) (holding that Arizona's constitutional right to privacy does not extend to a claim brought for wrongful termination) ("This constitutional provision was not intended to give rise to a private cause of action between private individuals, but was intended as a prohibition on the State and has the same effect as the Fourth Amendment of the Constitution of the United States.").

California: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." CAL. CONST. art.I, § 1. The Court of Appeals of California interpreted this provision in *Wilkinson v. Times Mirror Corp.*, 264 Cal. Rptr. 194 (Cal. Ct. App. 1989). In interpreting the ballot language of the 1972 amendment, the Court said that "[I]f the collection and retention of information by private businesses were intended to be excluded from the reach of the amendment, the ballot argument would not have mentioned credit card applications and insurance policies. The argument's repeated references to information-gathering activities by both government and business lead inexorably to the conclusion that the amendment was intended to reach both governmental and nongovernmental conduct." *Id.* at 198. Thus, the California

Constitution protects against intrusions into privacy by private actors as well as state actors. *See also* Hill v. NCAA, 865 P.2d 633, 643-44 (Cal. 1994).

Florida: "Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law." FLA. CONST. art I, § 23. For a discussion of privacy law in Florida, *see* John Sanchez, *Constitutional Privacy in Florida: Between the Idea and the Reality Falls the Shadow*, 18 NOVA L. REV. 775 (1994).

Hawaii: "The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest." HAW. CONST. art. I, § 6. In *McCloskey v. Honolulu Police Dept*., the Supreme Court of Hawaii referred to the Hawaiian Constitutional Convention, which adopted this provision, and reported, "[p]rivacy 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 but is not intended to deter the government from the legitimate compilation and dissemination of data." 799 P.2d 953, 956 (Haw. 1990).

Illinois: "Every person shall find a certain remedy in the laws for all injuries and wrongs which he receives to his person, privacy, property or reputation. He shall obtain justice by law, freely, completely, and promptly." ILL. CONST. art. I, § 12.

Louisiana: "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy." LA. CONST. art. I, § 5. Louisiana is one state whose privacy protection applies to private actors as well as to those of the state. *See* Moresi v. Dept. of Wildlife & Fisheries, 567 So.2d 1081 (La. 1990). In construing the state constitution, the Supreme Court of Louisiana stated, "the expression 'no law shall' was not used, indicating that the protection goes beyond limiting state action. *Id*. at 1092. The court also noted that invasion of privacy involves a "fear of unreasonable gathering and dissemination of information on individuals through use of computer data banks." Id.

Montana: "The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest." MONT. CONST. art. II, § 10. The Supreme Court of Montana interpreted this provision as applying only to state actors. State v. Long, 700 P.2d 153, 157 (Mont. 1985) ("[I]n accordance with well-established constitutional principles, we hold that the privacy section of the Montana Constitution contemplates privacy invasion by state action only.").

New York: A bill proposing a state Constitutional Amendment to establish an inherent right of personal privacy is currently in the legislature. *See* A.B. 1174, 222nd Leg., Reg. Sess. (N.Y. 1999) ("The inherent right of each person to personal privacy shall not be infringed.").

South Carolina: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and unreasonable invasions of privacy shall not be violated. . . ." S.C. CONST. art. I, § 10.

Washington: "No person shall be disturbed in his private affairs, or his home invaded, without authority of law." WASH. CONST. art. I, § 7. Washington's constitutional

Some states have criminalized the invasion of privacy.[151] Other states have merely codified the common law actions for invasion of privacy.[152] A uniform law regulating the dissemination of personal information just does not exist. The state legislatures in California and Massachusetts are responding to this gap by introducing bills that explicitly apply to biometric data.[153] With state constitutional and statutory protections as varied as they are, personal information is not adequately protected, especially given the fact that many commercial entities operate across state lines.[154]

4. Actions Under Common Law in Tort

---

protections apply only to actions involving state actors. *See* State v. Farmer, 911 P.2d 1030, 1033 (Wash. Ct. App. 1996) (holding that the defendant's state constitutional right to privacy was not infringed by a warrantless seizure of store receipts) ("The constitutional right to privacy is implicated only if the actors were functioning as agents or instrumentalities of the State.")

[150] *See generally*, Timothy O. Lenz, *"Rights Talk" About Privacy in State Courts*, 60 ALB. L. REV. 1613, 1616 (1997). See *supra* note 107 on what constitutes state action. Louisiana is one state that does not limit invasion of privacy to state actors. Lenz, *supra* note 150, at 1616. California and Hawaii are two others. *See supra* note 149.

[151] Delaware: Section 1335 of Delaware's Code makes violation of privacy a class A misdemeanor. A person is guilty of invasion of privacy if he performs a number of activities that invade one's privacy, including trespassing, intercepting a message, or installing or using listening devices. DEL. CODE ANN. tit. 11, § 1335(a) (1999).

Maine: Section 511 of Maine's Code provides that a violation of privacy is a Class D crime. ME. REV. STAT. ANN. tit. 17-A, § 511 (1998). A person is guilty of violation of privacy if he trespasses with intent to overhear or observe a person in a private place or installs any device for observing, hearing, recording or amplifying sounds or events in a private place without that person's consent. § 511(1).

Massachusetts: "A person shall have a right against unreasonable, substantial or serious interference with his privacy." MASS. GEN. LAWS ch. 214, § 1B (1999).

[152] Rhode Island is one state that codified the common law causes of action for invasion of property. *See* R.I. Gen. Laws § 9-1-28.1 (1997). The common law protections of privacy are discussed at *infra* notes 156-182 and accompanying text.

[153] California Senate Bill 71 would prohibit anyone from using biometric identifiers unless specified conditions are met. S.B. 71, 1999-00 Cal. Leg., Reg. Sess. (1999). The data must be used solely for identification purposes, cannot be sold or transferred to third parties, and must be protected from unauthorized access. *Id.* A similar bill was introduced in Massachusetts. *See* H.B. 4483, 181st Gen. Ct., 1999 Reg. Sess. (Mass. 1999).

[154] *See* Thomas B. Kearns, Note, *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns*, 7 WM. & MARY BILL RTS. J. 975, 1003-1009 (1999) (noting that constitutionally-based safeguards, based on a change in judicial interpretation, would be most effective for multistate companies).

Because of the necessity of state action in order to utilize federal and state constitutional protections,[155] many plaintiffs turn to the common law to provide redress for any invasion of privacy. The development of privacy rights under common law began with the often-quoted, famous law review article of Samuel Warren and Louis Brandeis of 1890.[156] In that article, Warren and Brandeis characterized privacy as the "right to be let alone."[157] In 1960, Dean William Prosser took the development of the right to privacy a step further by classifying invasions of privacy into four distinct torts.[158] These four categories are (1) appropriation,[159] (2) unreasonable intrusion upon the plaintiff's seclusion or solitude,[160] (3) public disclosure of private facts,[161] and (4) false light in the public eye.[162] These distinctions were later adopted in the Restatement (Second) of Torts.[163]

---

[155] *See supra* note 107. *But see, supra* note 150.

[156] Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). "The recognition and development of the so-called 'right of privacy' is perhaps the outstanding illustration of the influence of legal periodicals upon the courts. Prior to the year 1890, no English or American court ever had granted relief expressly based upon the invasion of such a right." W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 849 (5th ed. 1984).

[157] Warren & Brandeis, *supra* note 156, at 195. However, Thomas Cooley is said to have coined the phrase "the right to be let alone" in 1888 in COOLEY, THE LAW OF TORTS, at 29 (2d ed. 1888). KEETON ET AL., *supra* note 156, § 117, at 849.

[158] William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[159] The tort of appropriation is "an invasion of privacy whereby one person takes the name or likeness of another for commercial gain." BLACK'S LAW DICTIONARY 98 (7th ed. 1999). "It is the plaintiff's name as a symbol of his identity that is involved here, and not as a mere name. . . . It is only when he makes use of the name to pirate the plaintiff's identity for some advantage of his own. . . that he becomes liable." KEETON ET AL., *supra* note 156, § 117 at 852. *See infra* notes 164-67 and accompanying text.

[160] The tort of intrusion upon seclusion is "an action for invasion of privacy, a highly offensive invasion of another person's seclusion or private life. BLACK'S LAW DICTIONARY 829 (7th ed. 1999). It requires an "intentional interference with another's interest in solitude or seclusion, either as to his person or to his private affairs or concerns." KEETON ET AL., *supra* note 156, § 117 at 854. *See infra* notes 168-73 and accompanying text.

[161] Public disclosure of private facts is the highly offensive and objectionable publication of private information. KEETON ET AL., *supra* note 156, § 117 at 856. It is also described as "the public revelation of some aspect of a person's private life without a legitimate public purpose. The disclosure is actionable in tort if the disclosure would be highly objectionable to a reasonable person." BLACK'S LAW DICTIONARY 1243 (7th ed. 1999). *See infra* notes 174-76 and accompanying text.

[162] A false light claim consists of "a plaintiff's allegation that the defendant attributed to the plaintiff views that he or she does not hold and placed the plaintiff before the public in a highly offensive and untrue manner." BLACK'S LAW DICTIONARY 619 (7th ed. 1999). False light privacy is a variation of defamation. Murphy, *supra* note 85, at 2390. "The paradigmatic case

The tort of appropriation provides a remedy against someone who uses another's name or likeness for his own benefit.[164] This has also been called the "right to publicity."[165] The right is essentially the right to "control the commercial use of his or her identity."[166] The Restatement Second of Torts refers to this action as "appropriation of name or likeness."[167]

---

of false light is the publication of a person's photograph beside an article on drug abuse, though the person pictured is not a drug user." *Id*. *See also, infra* notes 177-82 and accompanying text.

[163] Murphy, *supra* note 85, at 2390. The Restatement (Second) of Torts § 652A provides:

> (**Error! Main Document Only.**) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
>
> (**Error! Main Document Only.**) The right of privacy is invaded by
>
> (**Error! Main Document Only.**) unreasonable intrusion upon the seclusion of another, as stated in § 652B; or
>
> (**Error! Main Document Only.**) appropriation of the other's name or likeness, as stated in § 652C; or
>
> (**Error! Main Document Only.**) unreasonable publicity given to the other's private life, as stated in § 652D; or
>
> (**Error! Main Document Only.**) publicity that unreasonably places the other in a false light before the public, as stated in § 652E.

RESTATEMENT (SECOND) OF TORTS § 652A (1977).

[164] *See also*, Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1412 (1987).

[165] Murphy, *supra* note 85, at 2391.

[166] J. Thomas McCarthy, *Melville B. Nimmer and the Right of Publicity: A Tribute*, 34 UCLA L. REV. 1703, 1704 (1987) (providing the history of the right of publicity).

[167] The Restatement (Second) of Torts § 652C states: "One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." RESTATEMENT (SECOND) OF TORTS § 652C (1977).

Intrusion upon seclusion[168] consists of one's intentional interference with another's privacy.[169] Intrusion upon seclusion requires an intentional intrusion, so an action will not lie by an intrusion of a purely accidental nature.[170] Another requirement for this tort is that the intrusion be unreasonable and highly offensive.[171] The best example of an action for intrusion is illustrated in *Galella v. Onassis.*[172] In *Galella*, Jacqueline Onassis succeeded in an invasion of privacy action against a photographer who followed her and her children practically everywhere.[173]

The public disclosure of private facts is a cause of action for the publicity of a highly objectionable kind of private information.[174] The information made public must be regarded as "highly offensive and objectionable to a reasonable person of ordinary sensibilities."[175] The Restatement (Second) of Torts adds the requirement that the information not be of legitimate concern to the public.[176]

---

[168] "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." *Id*. at § 652B (1977).

[169] KEETON ET AL., *supra* note 156, § 117 at 854.

[170] *See id*. at 855.

[171] *Id*.

[172] 487 F.2d 986 (2d Cir. 1973).

[173] To be completely accurate, Ronald Galella originally sued Ms. Onassis. She counterclaimed for invasion of privacy, among other claims. *Id*. at 998. Galella was also found guilty of harassment, intentional infliction of emotional distress, assault and battery, and the commercial exploitation of the defendant's personality. *Id*. at 994. The Court also found that Galella "intentionally physically touched Ms. Onassis and her daughter, caused fear of physical contact in his frenzied attempts to get their pictures, followed [Mrs. Onassis] too closely in an automobile, [and] endangered the safety of the children while they were swimming, water skiing, and horseback riding." *Id*.

[174] KEETON ET AL., *supra* note 156, § 117 at 856.

[175] *Id.* at 856-57.

[176] Restatement (Second) of Torts § 652D. The full text of this section is as follows:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
>
> (**Error! Main Document Only.**)would be highly offensive to a reasonable person, and
>
> (**Error! Main Document Only.**)is not of legitimate concern to the public.

RESTATEMENT (SECOND) OF TORTS § 652D (1977).

The last category is publicity that places the individual in a false light in the public eye.[177] It is said to often resemble defamation, although the two can be distinguished.[178] An action for false light publicity "is to protect a person's interest in being let alone,"[179] while defamation protects a person's good reputation.[180] The publicity must be of a kind that is highly offensive.[181] If the plaintiff is a public figure or the matter is one of public interest, Constitutional protections of freedom of speech apply to these actions.[182]

IV. ANALYSIS

A. Privacy Implications in the Use of Biometric Identifiers in the Banking Industry

The level of intrusion into privacy by the banking industry's growing use of biometric identifiers depends upon which method of biometrics is selected and how the data is stored. Because this information is given voluntarily, consumers are not as protected as they otherwise would be.[183] The main concern centers on which biometric identifier is chosen, since certain medical and health information may be inadvertently captured by the scan.[184] The

---

[177] The Restatement (Second) of Torts describes the tort of false light publicity as:

> One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if:
>
> (**Error! Main Document Only.**) the false light in which the other was placed would be highly offensive to a reasonable person, and
>
> (**Error! Main Document Only.**) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

Id. at § 652E.

[178] KEETON ET AL., *supra* note 156, § 117 at 864.

[179] *Id*.

[180] *Id*.

[181] *Id*.

[182] *Id*. at 865. For a discussion of the standard to be applied in these cases, see *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). Generally, actual malice is required, defined as either knowingly false, or with reckless disregard as to whether the information was false or not. *Id*. at 279. "If the matter involves the public interest, the plaintiff must prove the defendant's malice." BLACK'S LAW DICTIONARY 619 (7th ed. 1999).

[183] "Whereas the consumer voluntarily consents to give identification information to a private sector institution, federal courts generally turn a blind eye." Woodward, *supra* note 38, at 102.

[184] Woodward, *supra* note 18, at 115. ("[P]rivacy concerns may be implicated because in addition to the identification data captured, information about a person's health and medical history may also be incidentally obtained."). By examining an individual's iris or retina, a

unauthorized dissemination of medical information has long been closely scrutinized by the courts.[185]

---

doctor can diagnose diseases such as diabetes, high blood pressure, and arteriosclerosis. *Id.* Similarly, doctors can detect diseases specific to the iris and retina upon an exam. *Id*.

> As Dr. F.P. Nasrallah, an Assistant Professor of Ophthalmology at George Washington University explains, "examination of both the iris and the retina provides important diagnostic clues about a person's health, the retina more so." Nasrallah adds: "If I see certain lesions on the retina, I can become suspicious that the patient has AIDS, diabetes or high blood pressure for example." Intravenous drug abuse can also be suspected from a retina exam.

Id.

Similar concerns are implicated with fingerprint scanning. *See id*. "For example, Dr. Marvin M. Schuster, director of the division of digestive diseases at Johns Hopkins Bayview Medical Center, has discovered a 'mysterious relationship' between an uncommon fingerprint pattern, known as a digital arch, and a medical disorder called chronic, intestinal pseudo-obstruction (CIP) which affects 50,000 people nationwide." *Id* at 116. CIP is "a motility disorder, caus[ing] its victims 'to experience excruciating physical pain, vomiting, nausea, alternating bouts of severe constipation and diarrhea, and debilitating weight loss.'" *Id*. at n.146 (quoting *Gastroenterology: Fingerprinting GI Disease*, JOHNS HOPKINS PHYSICIAN UPDATE, Apr. 1996, at 5). Certain patterns on the feet and hands may indicate chromosomal disorders like Down Syndrome, Turner Syndrome, and Klinefelter Syndrome. *Id*. at 116. Unusual fingerprint patterns may also indicate CIP, breast cancer, leukemia, and Rubella Syndrome. *Id*. Some researchers have also reported a link between asymmetric fingerprint patterns and homosexuality. *Id.* (noting that the findings are controversial among the scientific and gay communities).

The International Biometric Industry Association, a nonprofit trade organization composed of the manufacturers, integrators, and end users of biometric technology, states that the digital code of the biometric identifier cannot be reconstructed, or reverse engineered, to reveal a person's identity or to obtain a true image of the biometric identifier. *See* International Biometric Industry Association, *Frequently Asked Questions About Biometric Technology* (last modified Mar. 28, 1999) <http://www.ibia.org/faqs.htm>. The digital code, a mathematical model, is actually what is stored, not an image of the scan itself. *See* Slater, *supra* note 52, at A1. It is possible, given the rapid advances in technology, that someday technology will reach a point where scientists can indeed reconstruct an accurate picture and doctors can determine medical information from a digital code. This is merely one reason why any privacy protection solution must be broad enough to cover future developments in technology. *See* Kearns, *supra* note 154, at 1002 (noting that past experience illustrates that current legislation is ineffective against new developments in technology by providing the example of Congress enacting the Electronic Communications Privacy Act of 1986, because the Wiretap Act of 1968 did not apply to cellular phone transmissions, pagers, or e-mail).

[185] "Information about one's body and state of health is a matter which the individual is ordinarily entitled to retain within the 'private enclave where he may lead a private life.'" United States v. Westinghouse Elec. Corp. 638 F.2d 570, 576 (3d Cir. 1980) (quoting United

In ATMs where the biometric information is stored in a card, there is little implication for invasion of privacy, provided that the banks do not store a copy of the digital code in a separate database.[186] In these systems, the biometric identifier is used for verification – that is, ensuring that the person in possession of the card is the one actually authorized to use it.[187] The biometric blueprint of the iris is located on the card itself.[188] If the card is lost or stolen, no one else can use it. The data is not stored in a database, where it can be accessed by the prying eyes of computer hackers or distributed to other organizations.[189] The banks utilizing this type of system have the added advantage of needing small amounts of storage capabilities.[190]

The systems that rely on biometric scanning for identification purposes,[191] that is, comparing the individual to all those enrolled, implicate more concerns over privacy. The digital code extracted from the iris or fingerprint is stored in the financial institution's database.[192] There, the information should be subject to heightened security measures to protect the data from computer hackers and other unauthorized access.[193] Banks should also be restricted from transferring that information to other entities.

B. Possible Sources of Protection for Biometric Information

The United States Constitution provides no protection for biometric

---

States v. Grunewald, 233 F.2d 556, 581-82 (2d Cir. 1956) (Frank, J., dissenting)). "In the cases in which a court has allowed some intrusion into the zone of privacy surrounding medical records, it has usually done so only after finding that the societal interest in disclosure outweighs the privacy interest on the specific facts of the case." *Id*. at 578. Nevertheless, in *Westinghouse*, the Court held that the release of a private sector employee's medical records to a government agency was allowed upon a showing of governmental interest. *Id*. at 577.

[186] If financial institutions store biometric data in a database, the bank retains control over it and can transfer it along with any other data. *See* Siuru, *supra* note 21, at 41.

[187] *See supra* notes 25-26 and accompanying text for the differences between identification and verification.

[188] Siuru, *supra* note 21, at 41.

[189] See id.

[190] Iris recognition requires a large amount of computer memory for the database. *See* Chandrasekaran, *supra* note 37, at HO1. By storing the digital code on the card itself, rather than on a master computer, the financial institutions require much less in the way of computer memory and storage. *See* Siuru, *supra* note 21, at 41; Woodward, *supra* note 18, at 110.

[191] *See supra* notes 25-26 and accompanying text (discussing the difference between identification and verification).

[192] *See* Nicholson, *supra* note 80, at 100.

[193] *See* International Biometric Industry Association, *Frequently Asked Questions About Biometric Technology* (last modified Mar. 28, 1999).

information gathered throughout the financial industry. The financial institutions are not state actors. Furthermore, federal statutes regulating the financial industry deal solely with specific types of information, and not biometric information.[194]

The Gramm-Leach-Bliley Act[195] represents a good start in the protection of informational privacy. However, the Gramm-Leach-Bliley Act implicates concerns over the privacy of personal information.[196] While some privacy protections were included in the Act,[197] others still need to be addressed.[198]

Prior to granting or extending credit, a bank can consult with its affiliated insurance company to ensure the customer is a risk worth taking.[199] The information shared between the affiliates would likely include the biometric information collected by the banks. Customers should be able to protect themselves from this type of intrusion into privacy. The privacy of biometric information gathered by banks cannot be adequately protected through current federal sources of privacy rights.

Similarly, state constitutions and statutes are inadequate when it comes to the protection of biometric data. Currently, with the exception of pending legislation in California and Massachusetts,[200] there are no laws that serve to prevent the banking industry from disseminating biometric information. Furthermore, fifty different states can each have their own law, resulting in fifty different laws.[201]

---

[194] *See supra* notes 134-148 and accompanying text (detailing current statutes regulating the financial service industry).

[195] *See supra* notes 141-148 and accompanying text.

[196] *See* Quinn, *supra* note 142, at B1.

[197] Under the Gramm-Leach-Bliley Act, banking customers can choose to opt out of having their personal financial information shared with third parties, but not with banking affiliates. *See* Pub. L. 106-102, 113 Stat. 1338 (1999). *See also,* Stephen Horn, Representative, House, *Modernizing Banking, Protecting Privacy*, CONGRESSIONAL PRESS RELEASES, Nov. 18, 1999. The Act also requires banks to disclose their privacy policy to customers on a yearly basis. *Id*.

[198] One area that the Gramm-Leach-Bliley Act did not address was allowing the consumer to opt out of sharing information between affiliates.

[199] *See* Quinn, *supra* note 142, at B1. Financial institutions can share their information with affiliates without first obtaining the customer's consent. *See* Pub. L. 106-102, 113 Stat. 1338 (1999).

[200] *See supra* note 153.

[201] The Gramm-Leach-Bliley Act allows states to override the privacy provisions if the state laws provide greater consumer protection than the federal protections. *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999); *Lenders Hit Privacy Stumbling Blocks,*

The common law actions also provide no protection. The collection and distribution of biometric data does not fit neatly into any one category. The tort of appropriation does not apply, as banks are not appropriating "the name or likeness" of the customer for the banks' commercial gain.[202] Appropriation involves a commercial use of one's identity, action that the banks are not taking.[203] Dissemination of biometric information does not rise to "unreasonable or highly offensive" conduct, as required by the tort of intrusion upon seclusion.[204] The torts of public disclosure of private facts and false light privacy do not apply, because the banks are not publicizing any "highly objectionable" information.[205] As one author notes, Prosser's categorization of invasion of privacy into the four common law torts "has effectively frozen the development of privacy law despite the creation of new technologies that detrimentally affect individual privacy."[206]

V. SUGGESTIONS FOR PRIVACY PROTECTION LEGISLATION[207]

The biometric information gathered by the banking industry will not be adequately protected by federal or state constitutions,[208] current statutes,[209] or

---

CREDIT RISK MANAGEMENT REPORT, Nov. 15, 1999; Lisa Fickenscher, *Reporter Notebook: States Expected to Tighten Reform's Privacy Provisions*, AMERICAN BANKER, Nov. 19, 1999, at 11 ("'The worse scenario is 50 different privacy regimes.'" (quoting Christine Varney, a former Federal Trade Commissioner)).

[202] *See supra* notes 164-67 and accompanying text (explaining the requirements for the appropriation tort).

[203] *Id*.

[204] *See supra* notes 168-73 and accompanying text (noting the requirements for the tort of intrusion upon seclusion).

[205] *But see*, Graham, *supra* note 164, at 1413 (suggesting that the public disclosure of private facts tort would be the most suitable for protection of information privacy but also noting that the courts have defined "publicity" rather narrowly). *See supra* notes 174-82 and accompanying text (detailing the requirements for the torts of public disclosure of private facts and false light privacy).

[206] Graham, *supra*, note 164, at 1406.

[207] One author notes that the best solution would provide protection from many difference sources, such as laws and regulations, industry norms, and business practices. Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 511 (1995). Reidenberg also urges the creation of a federal privacy commission to oversee informational privacy. *See id*. at 551.

[208] *See supra* note 194 and accompanying text.

[209] Some state legislatures have reacted to the growing use of biometrics with legislation to control the collection, use, and distribution of biometric information. *See supra* note 153. Although bills in the California and Massachusetts legislatures would protect the privacy of biometric information, these two states are the exception, rather than the rule. Congress

actions in common law.[210] Therefore, it is up to the federal legislature to regulate the accumulation and distribution of biometric information.[211]

Thus far, Congress has been silent on the widespread use and regulation of biometrics in the private sector. However, Congress can regulate the transfer of biometric information. Congress has the authority to regulate conduct that concerns or interferes with interstate commerce through the broad powers delegated through the Commerce Clause.[212] State governments can regulate technology, provided that the state statute or regulation does not interfere with federal law.[213]

In response to weaknesses in the privacy protection provisions of the Gramm-Leach-Bliley Act, several members of Congress have introduced legislation designed to more adequately protect consumer information in the financial industry.[214] Those bills, in combination with California's pending

---

needs to act in order to protect all American citizens.

[210] *See supra* notes 202-206 and accompanying text. For another view see Graham, *supra* note 164, at 1428. (urging the creation of an action for the tortious commercial dissemination of private facts to protect information privacy). Another author notes that courts are better suited to protect information privacy, because the courts can keep pace with technology and are not as easily swayed by pressure from interest groups, as are legislatures. Fenrich, *supra* note 9, at 980-83. *But see*, Petersen, *supra* note 4, at 165 (noting that cases often take years to get through the court system).

[211] *Cf.* Kearns, *supra* note 154, at 1002 (noting that legislation is not sufficient, because laws can easily be amended or repealed).

[212] U.S. CONST. art I, § 8, cl. 3. *See also* JOHN E. NOWAK & RONALD D. ROTUNDA, CONSTITUTIONAL LAW § 8.1 at 274 (4th ed. 1991).

[213] When a state statute conflicts with a federal provision, the federal statute preempts that of the state, due to the Supremacy Clause of the United States Constitution. U.S. CONST. art. VI, § 2 ("This Constitution, and the Laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any state to the Contrary notwithstanding."). A state statute may be explicitly preempted if the federal statute expressly states that it preempts the laws of the state. Gade v. Nat'l Solid Waste Management Ass'n, 505 U.S. 88, 98 (1992). Federal law may impliedly preempt state law when the state's regulation conflicts with the purpose and objectives of the federal statute or if compliance with both laws is physically impossible. *Id.* State statutes can also be preempted if Congress intended to regulate the entire field. *Id.*

[214] *See Leahy Banking Bill Calls For Tougher Privacy Rules*, CONGRESS DAILY, Nov. 17, 1999; Consumer's Right To Financial Privacy Act, H.R. 3320, 106th Cong. (1999); Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. (1999); Financial Information Privacy and Security Act, S. 1924, 106th Cong. (1999). H.R. 3320 and S. 1903 contain the same provisions,

legislation restricting the use of biometric information,[215] can and should be used as a model for a uniform federal statute regulating the transfer of biometric data.

The current bills in Congress provide for an opt-in provision, rather than an opt-out provision.[216] An opt-in provision allows the consumer to make an informed choice as to whether he will allow the financial institutions to distribute his personal data,[217] and to whom it will be disclosed.[218] Rather than informing the banks he does not want them to share his data with other companies,[219] the consumer must give the banks explicit permission to distribute his personal information.[220] These provisions apply to banking affiliates as well as third parties.[221] If the customer consents to such disclosure, he will also be afforded the opportunity to examine and dispute the accuracy of any personal information that was made available to other entities.[222]

California Senate Bill 71 prohibits the use of biometrics for identification or verification except when certain safeguards are in place to protect the data.[223] The data shall only be used for the purposes of verifying one's

---

and were just introduced in the different houses of Congress.

[215] S.B. 71, 1999-00 Cal. Leg., Reg. Sess. (1999).

[216] Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. § 502(b) (1999). (Financial institutions are prohibited "from making available any nonpublic personal information to any affiliate or other person that is not an employee or agent of the institution, unless the consumer to whom the information pertains (A) has affirmatively consented . . . ; and (B) has not withdrawn consent."). Advocates for opt-in provisions claim that opt-out provisions put the burden on the consumer to act. Fickenscher, *supra* note 201. Fickenscher quotes Massachusetts Lt. Governor Jane Swift as stating that "[i]t takes an enormous amount of self-education by consumers to understand just exactly to whom they need to say 'No.'" *Id*. Oftentimes, opt-out agreements confuse the customer to the point that he thinks his information is protected, when in reality, it is not. See id.

[217] An opt-in provision "force[s] companies to seek consumers' permission before using or selling personal information." Fickenscher, *supra* note 201, at 11.

[218] Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. § 502(b)(2) (1999).

[219] Opt-out provisions "let consumers remove themselves from these marketing programs." Fickenscher, *supra* note 201.

[220] *See* Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. § 502(b) (1999).

[221] *See* Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. § 502(b)(1); § 502(d) (1999).

[222] Consumer's Right To Financial Privacy Act, S. 1903, 106th Cong. § 502(c) (1999).

[223] S.B. 71, 1999-00 Cal. Leg., Reg. Sess. (1999).

identity.[224] The information cannot be distributed to third parties.[225] Finally, any databases containing biometric data must be adequately protected.[226] Similar to the Gramm-Leach-Bliley Act and the pending Consumer's Right To Financial Privacy Act, California's bill provides exemptions for law enforcement and other governmental agencies.[227]

A uniform federal legislation, one that adequately addresses biometric information and provides the necessary protection of that data, can be based on these acts. A model based on these acts would include opt-in provisions, a system for review and correction of inaccurate data, and requirements that the database be secure from unauthorized users.

An article on current privacy protections would not be complete without at least acknowledging actions other countries have taken. European countries have enacted sweeping provisions for data protection.[228] The objective of the European Directive for Data Protection ("Directive") is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[229] A provision in the Directive restricts the transfer of data to countries

---

[224] *Id*.

[225] *Id*. ("[T]he person shall not sell, transmit, exchange, or otherwise provide to third parties biometric identifiers or data containing biometric identifiers in the person's possession.").

[226] *Id*. ("[T]hese procedures shall be designed to make that data as secure from tampering and unauthorized access as current procedures used by the person to secure an individual's confidential information.").

[227] California Senate Bill 71 does not affect biometric data collection for use by the State Department of Social Services or the Department of Motor Vehicles. *See id*.

[228] *See, e.g.,* Council Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) (Nov. 23, 1995), available at <http://europa.eu.int/eur-lex/en/lif/dat/en_395L0046.html> (visited Nov. 7, 1999) (hereinafter EU Directive). The EU Directive defines personal data broadly enough to encompass biometric data. EU Directive, *supra*, art. 2 ("'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity"). For an in-depth analysis of the provision of the EU Directive, *see* Fred H. Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest,* 80 IOWA L. REV. 431 (1995).

[229] EU Directive, *supra,* art. 1

whose privacy protections are not adequate.[230] This provision could cripple multinational American corporations wishing to receive information from European Union member countries.[231] This is merely one more reason why it is imperative that Congress enacts a uniform law protecting information privacy.

VI. CONCLUSION

As the Supreme Court noted in *Whalen v. Roe*, [232] there is a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files."[233] The threat that the Supreme Court noted is very real, even more so today with the increased use of biometrics in industry.

Currently no federal or state constitutional source of privacy will protect biometric information from being disseminated by financial institutions without the individual's consent or knowledge. Current federal statutes, including the recently-enacted and highly praised Gramm-Leach-Bliley Act[234] are inadequate. Similarly, the common law tort system cannot adequately address the issue. Uniform federal legislation is the only viable method of protecting an individual's biometric information. A federal statute based on current California law and pending bills should be adopted to protect American's biometric identities

.

Lisa Jane McGuire

---

[230] *See* EU Directive, *supra* note 228, art. 25. *See also,* Paul M. Schwartz, *European Data Protection Law and Restrictions on International Data Flows*, 80 IOWA L. REV. 471 (1995); Patrick J. Murray, *The Adequacy Standard Under Directive 95/46/EC: Does U.S. Data Protection Meet This Standard?*, 21 FORDHAM INT'L L.J. 932 (1998) (analyzing the adequacy of current protection standards in the United States).

[231] *See* Murray, *supra* note 230, at 938 ("[t]he Article 25 requirement that a third country have adequate protection could lead to a data or information embargo."); Schwartz, *supra* note 230, at 487 ("No provision in the Directive has potentially greater consequences for the United States.").

[232] 429 U.S. 589 (1977).

[233] *Id.* at 605.

[234] Pub. L. 106-102, 113 Stat. 1338 (1999). *See also* The White House, *Statement by the President*, M2 PRESSWIRE, Nov. 16, 1999.