Ethics and Information Technology **5:** 139–150, 2003.

"A piece of yourself": Ethical issues in biometric identification

Anton Alterman
Baruch College, C.U.N.Y., Department of Philosophy, 1 Bernard Baruch Way, New York, NY 10010-5585, USA
E-mail: tonyalt@prodigy.net (home); altermana@hra.nyc.gov (office)

I. "Biometric identification" is a general term for technologies that permit matches between a "live" digital image of a part of the body and a previously recorded image of the same part, usually indexed to personal or financial information.[1] Biometric identifiers include digital fingerprints, retinal scans, hand geometry, facial characteristics, and vocal patterns. Biometric scanning systems typically do not record the entire imprint of a physical feature but only that portion, or "template", that should be time-invariant within some statistical limit. Since the body changes over time, the statistical algorithm must be elastic enough to match a stored image with a later live scan from the same person, without normally matching two similar individuals. This creates limitations on the uniqueness of the images, which are overcome by using multiple images from one person or a biometric image plus other information. In some applications identities can be verified within a population of millions.

Someone browsing a biometric database would not see any pictures, and would need the algorithms to see the data as a retinal or fingerprint image. Since the formulas are proprietary, someone with algorithms from Company A could not decrypt data from Company B. There are economic incentives for the development of encryption standards, however; for example, two banks using different biometrics vendors would need such standards to provide cross-recognition of fingerprints for ATM transactions.

Compared to a visual comparison of signatures or photo ID's, biometric identification is less fallible and potentially much faster. This has prompted the use of biometrics for noncriminal governmental and commercial applications. James L. Wayman, Director of Biometrics Test Center at San Jose State University,[2] mentions a number of such applications that were live as of May 1998, including immigration systems, airport security systems, employee time recording, social service benefits distribution, and driver's licensing programs. "Disney World is using finger geometry with their season passes ...", he notes.[3] If the combination of high-tech identification with amusement seems bizarre, consider the fact that a common use of facial recognition systems is to bar unwanted patrons from casino tables.[4] The International Biometric Industry Association (IBIA) has offered a candid list of other potential applications, including voter registration, access to healthcare records, banking transactions, "national identification systems", and "parental control".[5] They do not elaborate on these last two items. In 2001 VeriStar Corporation introduced the Smarttouch digital fingerprint system for use in fast food restaurants. According to a report in *InformationWeek*, "within the next few months, some McDonald's customers will be able to charge Big Macs to their Visa cards simply by touching a finger to a screen".[6] VeriStar's web site emphasizes

[1] The term "biometric", and the concept of biometric identification, originated before the digital era. But today, and presumably for the future, every form of biometric identification is based on the comparison of an image with information stored in a computer database. For a history of pre-digital biometrics see Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (Sebastopol, CA: O'Reilly & Associates, 2000), Chapter 3. My definition of "biometric" is narrower than his. I do not, for example, consider signatures "biometric" because the prefix does not apply: signatures are *biological* only in the sense that behavior patterns are. Nor do I think of facial photographs as biometric, for the suffix does not apply: there is too much information in a photograph, even under controlled conditions, to reliably compare them *metrically* with a live subject. This is not to deny that the attempt has been made to use them this way.

[2] The center served as the U.S. Biometrics Test Center from 1997–2000.

[3] James L. Wayman. "Biometric Identification and the Financial Services Industry". Congressional testimony of May 20, 1998; in *National Biometric Center: Collected Works*, p. 263; www.engr.sjsu.edu/biometrics/nbtccw.pdf.

[4] See the online journal of the Biometrics in Human Services User Group (BHSUG), Volume 4, Issue 5, p. 7; www.dss.state.ct.us/digital/news21/bhsug21.htm, 11/1/2001.

[5] IBIA, "Removing Export Controls on Biometric Technology", February 2000; www.ibia.org/bxacomments.htm.

[6] *InformationWeek*, April 30, 2001, p. 22; cited by Bob Evans in "Privacy Vs. Paranoia", *InformationWeek*, May 7, 2001, p. 172.

the ease of enrollment in this system, saying that it "takes just a minute or two. And it's free".[7]

Some biometric identification programs are nonvoluntary, like criminal or alien tracking systems;[8] almost all other programs are voluntary. Voluntary programs are either mandatory, where a biometric id is required in order to obtain some benefit, or optional, where some other form of id is permitted. Optional systems either allow users to opt in, by volunteering to use the biometric method, or to opt out if they don't want to do so.[9] All sales and financial applications, where biometric ID's provide faster checkout or access to accounts, will have to be opt-in systems until biometric ID's become as common as email addresses.

II. Biometric identification raises a number of ethical issues, mostly centering on the concept of privacy. Here we must distinguish two questions: (1) Does biometric identification raise the same issues regarding data privacy as other forms of personal identification? (2) Are there any privacy issues specific to biometric ID's? I will take up the first question here and the second in part III.

A good example of the general issue of data privacy is offered by Leslie David Simon in *NetPolicy.Com*. He mentions "a direct marketing company . . . using state prison inmates to process computer tapes containing detailed personal information on more than 90 percent of American households".[10] The case was discovered when a woman began receiving threats from a convicted rapist who had viewed her file. This illustrates two kinds of privacy concerns associated with data storage. One is that someone, say a stalker, or the U.S. Federal Bureau of Investigation (FBI) for that matter, will legitimately gain access to information about you and utilize it to locate and harass or harm you in some manner. A second is that information you provide for a particular purpose will be retrieved or purchased, say by direct marketers or credit bureaus, perhaps to be correlated with other data, and used for purposes that you would neither have predicted nor agreed to.[11] A third kind of concern is that the data will be stolen or illegitmately released, exposing you to risk, embarrassment, or other harm.[12]

It is sometimes suggested that biometric ID's are immune from, or extremely resistant to these abuses, indeed that they are a form of protection against them. Thus Wayman wrote in 1998:

> Only two biometric technologies, fingerprinting and retinal scanning, have been shown . . . to be capable of singling a person out from a group exceeding a thousand people. The current design of the retinal scanning device supports only 'cooperative' applications, those in which the user wants to be singled out. [Biometric] fingerprinting . . . does not save data in a format compatible with large-scale searches . . . Because of lack of standards regarding the method used to develop [the numeric representations of the images], they are useless to any other system, even to the FBI.[13]

Regarding the idea that "if an unscrupulous person gets my biometric data, perhaps they can use it to assemble my health records, my driving record, my banking data", Wayman says, "the lack of standards creates . . . 'biometric balkanization', meaning the inability of systems to communicate . . .".[14] Similarly, Richard Norton, of the IBIA, wrote in 2000–2001 that "biometric technology is used to erect a barrier between personal data and unauthorized access . . ." and that the stored templates "employ proprietary and *carefully guarded algorithms* to safeguard records and protect them from disclosure".[15]

Four main arguments are offered or suggested here in defense of the idea that biometric technology does not raise significant privacy issues:

[7] Veristar Corporation, www.veristarcorp.com/solutions/enrollment.html, 5/10/2001. As of September 2001 Veristar Corporation changed its name to Indivos Corporation. Smart Touch became Pay By Touch. Veristar's web sites are no longer reachable.

[8] For a discussion of ethical issues surrounding the implementation of EURODAC, a nonvoluntary European Union system that tracks asylum seekers, see Irma van der Ploeg, "The Illegal Body: 'Eurodac' and the Politics of Biometric Identification", *Ethics and Information Technology*, 1: 295–302, 1999.

[9] An example of an opt-out system with significant implications for privacy is the Verizon implementation of caller id displays. Telephone numbers were automatically set to display on caller id screens unless the customer specifically opted out. For an in-depth discussion of ethical issues with regard to caller id systems, see Judith Wagner DeCew. *In Pursuit of Privacy: Law Ethics and the Rise of Technology*. Cornell University Press, 1997, pp. 153–161.

[10] Leslie David Simon, *NetPolicy.Com: Public Agenda for a Digital World*. Washington, DC: The Woodrow Wilson Center Press, 2000, p. 136.

[11] See Garfinkel, *Database Nation*, pp. 156ff, 275, for further examples.

[12] For examples see Garfinkel, *Database nation*, pp. 274–275.

[13] Wayman, "Biometric Identification and the Financial Services Industry", p. 265.

[14] Wayman, "Biometric Identification and the Financial Services Industry", pp. 265–266.

[15] Richard E. Norton, "Response to Notice of Proposed Rule Making 12 CFR Part 216", Letter of March 29, 2000; www.ibia.org/fedglbcomments32900.htm. See also "Privacy 1", Letter of March 30, 2001, www.ibia.org/hhsprivacycomments033001.htm where more or less the same language is used.

(1) The "technical limits" argument: in a large population the technology has limited capability to identify a particular individual.
(2) The "balkanization" argument: information remains local and restricted because no interoperability standards exist.
(3) The "cooperation" argument: the technology cannot easily be abused because identification requires cooperation.
(4) The "security" argument: the template algorithms are secure because biometrics vendors have a proprietary interest in keeping them confidential.[16]

Though the statements on which these arguments are based were technically accurate at the time they were made, they tend to suggest that raising privacy issues about biometric data is a kind of category mistake. But the context of these claims is a temporally specific technical state of the means for gathering, storing, and searching biometric data. As we shall see, the basis for these arguments is thin and rapidly evaporating.

Let us consider now our first privacy concern, threats to one's person. Whether or not biometric systems present this kind of threat depends on whether they can indeed be used to single you out without your cooperation. The first thing to be addressed here is the "technical limits" argument. What are the actual and potential capabilities of the technology? It is generally agreed that fingerprint technology is the most reliable. Many vendors claim a false acceptance rate (FAR) and false rejection rate (FRR) of 0.01% or less, meaning that less than one out of 10,000 people are matched with someone else's fingerprints (FAR) or fail to be matched with their own fingerprints (FRR). This means that if someone is looking to single you out (i.e., you are on a "watch list", in industry jargon) your fingerprints will identify you in 99.99 cases out of 100. A 2002 study of facial recognition systems showed that the best systems offered a FRR of 10% and a FAR of 1% for images captured indoors – results that represented a 50% improvement in only two years.[17] The study also showed that "for a watch list of 300 people the identification and detection rate was 69% at a false alarm rate of 1%".[18] This does not suggest that these systems could reliably single out individuals from a large population. But the technology is clearly making rapid technical advances. Thus, one cannot safely assume that the technical limitations of biometric identification protect our privacy today, and it is fairly certain that they will do so less and less as time goes on.

Moreover, even if the "technical limitations" argument were sound, there are reasons to think that this only creates different kinds of privacy concerns. For example, Veristar requires a unique 7-digit code "to enable immediate location of your biometric ID" in case a SmartTouch match fails. The company recommends using your telephone number as the code.[19] This minimizes the overhead for the Veristar user and its customers in dealing with forgotten codes. It is anything but secure, however. If I know you have registered with Smarttouch and I either know or can look up your phone number, then I can present myself as you, and when my scan fails, offer your phone number to verify my identity. Presumably I can then charge my purchase to your credit card. No doubt a responsible establishment would require some additional verification, but it is clear that given the technical limitations, the biometric id offers more an illusion than the reality of security.

Does the lack of interoperability standards mean that the threat of surveillance or harm is negligible because the data is only available within a small corporate circle? John D. Woodward, Jr. points out that if "facial recognition or other biometric databases become interlinked, then the threat to information privacy has the potential to increase significantly".[20] Proprietors of biometric technology can agree on data exchange protocols without waiting for industry standards. But standards have already begun to appear. A standard for storing fingerprints on driver's licenses is already widely used.[21] More recently, a "global, harmonized blueprint for the integration of biometric identification information into passports and other machine-readable travel documents" has been adopted by the International Civil Aviation Organization (ICAO).[22] Still more sobering

[16] *Cf.* Clyde Wayne Crews Jr., "Human Bar Code: Monitoring Biometric Technologies in a Free Society", *Policy Analysis*, 452: 1–20, 9/17/2002. The argument here is essentially that competition will force private industry to develop biometrics in a way that respects individual privacy. The author is director of technology studies at the Cato Institute, a libertarian think tank that advocates free enterprise and rejects most government oversight of private industry.

[17] P. Jonathan Phillips et al., "Face Recognition Vendor Test 2002: Overview and Summary". The study was sponsored by the U.S. National Institute of Standards and Technology (NIST) and several federal agencies. It was based on a database representing 37,437 individuals. The statistical results vary with age, sex, and time lag after image capture.

[18] Phillips et al., "Face Recognition Vendor Test 2002", p. 3.

[19] Veristar Corporation, www.veristarcorp.com/solutions/enrollment.html, 5/10/2001.

[20] John D. Woodward Jr., *Superbowl Surveillance; Facing Up to Biometrics*, Rand Arroyo Center, 2001, p. 7.

[21] Tod Newcombe, "Biometric Breakdown", *Government Technology*: 036, May 2001. The standard was developed by the American Association of Motor Vehicle Administrators.

[22] Jennifer D'Alessandro, "Biometric ID To Become Part Of

is NIST's *Common Biometric Exchange File Format* (CBEFF) which, according to NIST, "facilitates biometric data interchange between different system components or between systems", "promotes interoperability of biometric-based application programs and systems", "provides forward compatibility for technology improvements", and "simplifies the software and hardware integration process".[23] Thus the "balkanization" of biometric information is on its way to becoming a thing of the past.

What about the cooperation requirement? One effort to overcome this is a $50 million program initiated by the Defense Advanced Research Projects Agency (DARPA) called "Human ID at a Distance", the goal of which is to "develop biometric technologies ... that can be deployed to identify a known terrorist before he closes on his target".[24] A more notorious effort took place at the 2001 Super Bowl, where the crowd was covertly videotaped by police and the images compared with facial scans of convicted criminals. As *WiredNews* notes, "fans may have resented being ... made part of a digital lineup, but Tampa Police say the technology allowed them to pinpoint 19 people with criminal records in a crowd of over 100,000".[25] Of course, the Tampa police probably overestimated the current capabilities of the technology, and the 19 putative matches may well include false ones.[26] This again shows that potentially intrusive uses of biometrics exist even if the "technical limits" argument is sound. Imagine, for instance, some mismatched individuals being hauled in for questioning: it would be little solace to know that the privacy of the people on the "watch list" was protected by the technical limitations of the software.

But leaving aside misunderstandings of the technology, the Tampa incident clearly demonstrates that biometric identification can potentially be used in a way that threatens harm to individuals, e.g., through violations of civil liberties. Even people with criminal records are not necessarily criminals at present, so it is not clear why anyone's image should be subjected to examination and comparison of this sort. Moreover, law enforcement authorities are not entitled to conduct surveillance on the general population without any evidence of wrongdoing, as was done by the FBI in the infamous COINTELPRO program of the 1970's. Nor is it permissible for them to covertly make people part of a criminal identification program, any more than they can force law-abiding citizens to participate in a police lineup. The Tampa incident already falls short of ethical standards on these grounds, and the increasing accuracy and interoperability of the software means that the potential for much more serious, perhaps criminal, abuses exists.

Let us consider our second concern, the use of biometric id's to collect and collate data for purposes not intended or desired by the individual. An article in a hotel trade publication points out that "with the use of this [biometric] technology a front desk clerk could know instantly at check-in that Mr. John Smith during his last stay purchased three Cokes from the mini-bar, two martini's in the lounge, ate dinner at the hotel restaurant where he ordered the special and since his last visit has moved from Chicago to Atlanta".[27] That is very convenient for the hotel's marketing department, and perhaps for Mr. Smith's boss, who may be curious about his employees' alcohol consumption. But it is hard to see much benefit for Mr. Smith, who is now represented as a table of consumer characteristics and whose movements are tracked like those of a bacterium under a microscope.

Regarding the last of our concerns, unauthorized access to personal information through abuse or theft of data, the proprietary interests of vendors, even when taken together with the lack of standards and complexity of the algorithms, hardly eliminate it. A firm that controls biometric databases could make unethical use of the data for financial gain or other purposes. A technical error could cause the release of decrypted biometric ID's and the personal data associated with them on a corporate intranet or extranet. A disgruntled programmer could alter the data to support false ID matches or make good ones fail. A law enforcement agency could force the data and algorithms to be turned over to them. A computer hacker could access the data and algorithms and post them on a Web site. "Carefully guarded algorithms" do not mean much when Pentagon sites are hacked and disk drives with nuclear secrets are carried around like lunchboxes. The ethics of biometric identification cannot rest on the assumption that the data is absolutely secure.

Passports", *varBusiness*, 8/26/03; http://www.varbusiness.com/sections/ governmentvar/govt.asp?articleid=43467.

[23] NIST web site, 8/31/2003; http://www.itl.nist.gov/div895/isis/bc/cbeff/.

[24] Woodward, "Super Bowl Surveillance", p. 10.

[25] Julia Scheeres, "When Your Mole Betrays You", *Wired News*, 3/14/2001, www.wired.com/news/politics/0,1283,42353,00.html.

[26] Wayman writes in a personal email communication (24 May 2001): "Regarding the ethical debate, picking one person out of a large crowd (SuperBowl XXXV) without complete cooperation from all persons is technically infeasible using any combination of measures".

[27] Geneva Rinehart, "Biometric Payment: The New Age of Currency", *Hospitality Upgrade Magazine*, Spring 2001; reprinted at www.hotel-online.com/Neo/News/PressReleases 2000_1st/Mar00_BiometricCurrency.

In short, threats to privacy in the form of unwarranted identification and threats to the person, undesired collection of personal data, and unauthorized access to personal information, are all possible with biometric data as with any other. It might be said though that biometric ID's themselves, as opposed to the personal or financial information indexed to them, are of no interest to anyone, and therefore pose no general threat to privacy. What harm could a copy of your fingerprints or retinal structure cause if released? In a future that can easily be imagined, plenty. Consider the suggestion that biometric ID's be used for " 'keyless entry' for hotel rooms".[28] This entails more than mere financial dangers in the theft of biometric images.[29] Another example, in connection with the EURODAC system for identifying asylum seekers, is "the danger of retaliation by the country of origin"[30] should they obtain the biometric ID's for their own nationals. But the main problem with the objection is that we may have a privacy interest regarding biometric ID's over and above their immediate practical value, just because they are representations of our bodies. This leads us to the second question I mentioned above.

III. I will defend the view that there is something disturbing about the generalized use of biometric identification apart from standard data privacy issues. This view is based on the claim that privacy is control over how and when we are represented to others. The proliferation of representations that identify us uniquely thus involves a loss of privacy, and a threat to the self-respect which privacy rights preserve. I think we should be wary when an author writes that "increasingly, the way to keep information secure is to offer up a piece of yourself . . . to be recorded and used to verify your identity".[31] My concern is that the metaphysical "piece of yourself" that is offered up may be important to retain control over and hard to recapture once it is put in the form of a proprietary digital image.

I will now briefly sketch a theory of privacy, focusing on just three points that will allow me to defend this view.

First, a word about property. Following Locke, Hegel, and Marx I see property as originating in an externalization of the self by means of labor. This gives us a moral basis in self-respect for the right to own personal property.[32] Now, I agree with Scanlon, Rachels, and others that the right to privacy is not based on property rights,[33] but I think they arise in tandem, and for similar reasons. Personal property rights permit us to enjoy some of the fruits of externalized labor when both labor and its products are normally commodities. They act as a limit to alienation, enabling us to retain enough of the social product for the necessities of life and a modicum of self esteem. Privacy is likewise a barrier against alienation. Since our daily lives are characterized by the endless public interactions of a market system, we require a complementary right *not* to broadcast into the public sphere what is both central to our sense of self and of no legitimate interest to society. Just as personal property rights allow us to maintain the material comfort conditions required to regenerate ourselves as participants in a commodified labor system, privacy rights reproduce the psychological comfort zone we need to (more or less) willingly participate in the system. Thus we defend our capacity to maintain a public self by means of an inalienable shield of privacy.[34]

Second, the concept of privacy as related to an abstract self must be combined with the recognition that as moral agents we are also, noncontingently, biological human beings susceptible to certain types of sensations and emotions. The right to privacy may

[28] Rinehart, "Biometric Payment".

[29] Actually using such data would require reverse engineering it so as to produce a facsimile of the original image. Such efforts to fool biometric identification systems are referred to as "hill-climbing attacks" within the industry, and biometrics engineers are busily at work trying to come up with strategies to defeat them. According to the British Parliamentary Office of Science and Technology (POST), "it is likely that fraudulent identities could be developed . . . Creating a biometric identity could involve either stealing electronic data files, or creating a physical replica (e.g., contact lenses etched with a false iris image)". "Biometrics and Security", *Postnote*, 165: 4, November 2001.

[30] van der Ploeg. "The illegal body . . .", p. 300.

[31] Molleen Theodore, quoted in Rinehart, "Biometric Payment". Van der Ploeg cites a similar remark from "an ABC newsreader": "Biometrics are turning the human body into the universal ID card of the future". "The illegal body . . .", p. 301.

[32] For a development of the Lockian view see Adam D. Moore, "Intangible Property: Privacy, Power, and Information Control", *American Philosophical Quarterly*, 35(4): 365–378, 1998; and references to the author's other articles on p. 376*n*5.

[33] See Thomas Scanlon, "Thomson on Privacy", *Philosophy & Public Affairs*, 4(4): 315–322, 1975; and James Rachels, "Why Privacy Is Important", *Philosophy & Public Affairs*, 4(4): 323–333, 1975. The articles are a reply to Judith Jarvis Thomson, "The Right to Privacy", *Philosophy & Public Affairs*, 4(4): 295–314, 1975.

[34] Judith Wagner DeCew similarly describes privacy as "a shield protecting us from prejudice, coercion, pressure to conform, and the judgment of others". See "Balancing Privacy and Public Safety in an Age of Technology", talk given to the Society for Philosophy and Public Affairs at APA Pacific Division Meeting, March 29, 2002 (unpublished). Similar language is used in her *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997, p. 75.

therefore be thought of as a part of a general social interest in protecting what Natalie Dandekar calls "embodied persons".[35] This interest generates a set of personal rights centered on the body as an integral part of the self, including rights to freedom of movement, self-respect, bodily integrity, and privacy. These rights create an inviolable personal "zone" (to use Scanlon's term) protecting physical and emotional aspects of the self against harm.

A consequence of these two points is that in a system of commodity relations we have an inherent moral interest in preventing the complete alienation of a psychological self that is inseparable from its biological form. It is an *inherent* interest because, given the structure of our social situation, a need for privacy is a feature of personhood; and it is a *moral* interest because the psychological integrity of the embodied self is both a good in itself and a precondition of our ability to experience the world as moral agents.

Third, then, this interest is manifested as a control right over the way we are represented to others, both in our physical appearance to others and in projected, iconic, or indexical representations. Privacy is the right to maintain control over how we represent our embodied selves when there is no overriding moral interest in their publicity. We thereby avoid being represented in ways that may cause us physical or psychological damage, such as harm to our conception of ourselves as autonomous, dignified, and secure.[36] This right of control over representations of ourselves includes the right to manage our self-representation to society at large: to be secure from observation at home, to choose our intimate partners and practices, and to dress and groom ourselves as we wish in public. In addition, in an age where information is easily digitized and networked ("greased", as James Moor puts it[37]) we retain the right to control the creation and use of representations which identify us, either through an image of parts of the body or through information indexed uniquely to an individual.

The theory of privacy I have just outlined establishes that we have a fundamental privacy interest in controlling identifying representations of ourselves, including biometric images.[38] Further discussion is needed, however, before we can say why biometric scans involve special privacy issues beyond those that they share with indexical data and, moreover, with photographic images. To begin, it should be clear that from a moral point of view we have a greater interest in representations centered on the *body* (I shall call this *biocentric* data) than in, e.g., our social security number, driver's license number, or home address (I shall call this *indexical* data). Indexical data has no internal relation to an embodied person; it possesses no property that is tied to our psychological or physical conception of self.[39] From a practical point of view, moreover, indexical data singles us out only if we can be positively identified as its owner by some other method. Needless to say, it can be very damaging for someone else to obtain and misuse this information, as can happen in the case of "identity theft". But such information is only contingently tied to a particular individual. Abuse of it is primarily an attack on one's property rights rather than on one's sense of self – though a loss of self-esteem could indirectly follow from an attack on one's right to certain kinds of property.[40] Control over one's medical data may have intrinsic moral worth on this view, but, other than DNA information, it will only rarely identify an individual uniquely.[41] In general, then, indexical data normally

[35] Natalie Dandekar, "Privacy", *Philosophical Forum*, 24(4): 331–348, 1993, (pp. 333–334 and p. 343).

[36] Harm to those we love occupies a more or less equal position in the order of what we seek to protect by maintaining a shield of privacy. I avoid introducing this into the discussion to keep matters simple. It does not change the theory I am offering but does require theoretical work in itself. For example, one might ask how much the need for privacy is motivated by a direct interest in loved ones and how much by an interest in avoiding the harm to ourselves that follows from harm to others.

[37] See James H. Moor, "Toward a theory of Privacy in the Information Age", *Computers and Society*, 27(3): 27–32, 1997; in Robert M. Baird et al., editors., *Cyberethics: Social and Moral Issues in the Computer Age*. Amherst, NY: Prometheus Books, 2000, pp. 200–212.

[38] In this section I will set aside questions about the current state of the technology and proceed on the ideal assumption that biometric systems can uniquely identify an individual within an arbitrarily large population.

[39] Some people may take an interest in a proper name, or perhaps a social security number that ends with "7777". But I deny that any but a vanishingly small number of people identify with such data as with a hand, or even their hair, much less with their liberty, equality, or privacy.

[40] I was a victim of identity theft in 2001. Fortunately, the perpetrator was caught quickly and the damage only amounted to minor inconveniences. Far worse cases can occur, though, in which people become at least temporarily liable for very large debts and suffer a variety of inconveniences and indignities.

[41] Elizabeth Neill argues that it is not a violation of privacy for someone to share my medical information with others, even if associated with me by name. See *Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self*. McGill-Queen's University Press, 2001, p. 11 and elsewhere. Apart from any other reasons to doubt this claim, the present view clearly leads to the position that medical information is not only private but *inherently* so. I think this matches our intuitions and that this is a place where intuitions should be preserved by theory. This appears to be an advantage of the present theory of privacy over hers. Broadly speaking, though, I commend Neill's attempt to reach more deeply into the nature of privacy than

has no inherent relationship to one's dignity or self-respect, and therefore protecting it has little inherent moral value.

Biocentric data acquires a fundamental privacy interest because it has an impact on one's right to control the use and disposition of one's body. This right is a basic moral tenet of modern Western civilization, and is one of the ideas captured in Kant's famous dictum that one must treat people only as ends in themselves, never merely as a means. The underlying point of this, as I understand it, is that the concept of a person is inextricably tied up with that of having a free will. To use a person as a means to your end is to deny their will, thus reducing them to the status of an unfree object. This amounts to taking the body of another to be only contingently under control of their will. This is what Kant rejects; the body belongs necessarily to the will that inhabits it from birth. For this reason, no rational person can voluntarily surrender their own will, i.e., become unfree. Thus, utilizing a person's body as a means to an end is prohibited under Kantian principles, as is surrendering one's body to the use of another. But providing an image or representation of one's body for use as a means of identification can be a form of just such a surrender. With biometric identification, the image is a tool, the purpose of which is to permit recognition of the body by external entities that have an interest in it. Offering up this "piece of yourself" authorizes and enables others to *use* your body for purposes of their own. It thereby *objectifies* the body by isolating the physical element from the person and providing it as a means to an end in which the person has no inherent interest.

We have seen that biocentric data, unlike indexical data, has inherent moral value. Now we must confront the issue of photographs, a more traditional biocentric form of identification, and their relationship to biometric images. It may appear that they are not logically distinguishable from biometric images with regard to their privacy and moral value. I will show that this is incorrect; but first, let us consider how photographic images differ from indexical data. A clear pictorial representation is integrally related to one's bodily self-esteem, and performs the identifying function of indexical data in a way that leads more directly and reliably to our person. Like a biometric scan, a very clear visual image singles us out physically with greater certainty than, say, a social security card, which can be stolen or forged. As I have suggested, loss of control over bodily representations presents potentially greater threats to one's self-respect and sense of personal security than the release of indexical data. Consider James Rachels' example: a woman finds out that nude photographs of her which were taken to document an assault were distributed for the titillation of police officers.[42] This is surely quite damaging and morally offensive. Control over the representation has been illegitimately removed from the subject, who authorized the creation of the images under the reasonable assumption that their use would be restricted to documenting the assault. As a result she suffers feelings of humiliation and betrayal. A photograph can be put to still worse illegitimate uses by law enforcement authorities, say, to frame and imprison an innocent person; as well as by criminals who might wish to identify someone for purposes of extortion, kidnapping, etc. A photograph can end a political career or a marriage. For reasons like these, people are naturally cautious about being photographed; hence the legal restrictions on the use of such representations.

But if we have a special interest in controlling photographic representations, we have a stronger one in controlling biometric scans of ourselves. Biometric scans are similar to DNA in their relation to a person: they pick out biological traits which by their very nature are unique to the individual and positively identify that individual, within an ever larger population as the technology improves. Unlike a photographic image, from which one can dissociate oneself by various superficial means, the features used for biometrics cannot be altered without serious physical damage, except by the aging process. Surgically modifying the patterns on one's thumbs or irises is, for all but hardened criminals, surely less desirable than the consequences of being identified by a scanner. New methods of scanning hand geometry actually identify internal features of the tissue and blood vessels,[43] making amputation the only means of alteration. This has the consequence that association with the image is all but *irreversible*. Another salient difference is that in a photograph such factors as focus, range, angle, texture, background, contrast, lighting, and density, as well as transient surface features of the subject (facial hair, expression, etc.) can vary widely and decrease their reliability as identifiers. Since the sole purpose of biometric scanning is for identification, these factors either do not exist or are carefully controlled at the outset. Thus the method is far more *reliable*. Moreover, even a very clear photograph or film can only be *visually* compared with a person,

is done in most of the legal and philosophical literature on the subject.

[42] James Rachels, *The Elements of Moral Philosophy*, 3rd edition. New York: McGraw-Hill College, 1999, pp. 111–112. In the case Rachels describes it may be that the photographs were superfluous and objectionable in the first place, but my point holds even if they were originally legitimate.

[43] BHSUG 4(5): p. 6, 11/01/2000.

limiting the certainty of the comparison and creating practical obstacles, such as the need to locate the image and the time to compare a large number of potential matches. Biometric comparisons, on the other hand, are processed by computer and the "images" are data representations from the moment of creation.[44] Thus the method is also far more *efficient*.

This combination of irreversibility, reliability, and efficiency amounts to more than a mere practical difference between biometric and photographic identification. The loss of control that this entails, and the degree to which the body is objectified by the process, suggest that biometric identification alienates a part of the embodied self. The body becomes an object whose identity is instantly determinable by purely mechanical means, and subject to external controls on that basis; while those means themselves are removed from the control of the subject. The representations are infinitely reproducible by their owner, but are not even accessible to the subject whose body they represent. The embodied person now bears, more or less, a label with a bar code, and is in this respect alienated from her own body as well as from the technology used to recognize it. If having an iris scan on file is not quite like being incarcerated in the world at large, being made known to mechanical systems wherever they may be is still a tangible loss of privacy that is not precisely paralleled by any other kind of information technology.[45]

Biometric scans also share many of the properties that make people naturally cautious about photographs. As noted, such scans can potentially be of use to people who want to harm us or to authorities we wish to avoid. Moreover, like photographic representations, we may find the data embarrassing in itself, or fear that by comparison with other biometric images we will stand out as unusual or defective in some way. It is disconcerting to learn that one's facial image, through its biometric representation, was matched with those of murderers, even if it is hard to say why. Other potential forms of embarrassment, though, are easier to understand. If someone has a reason not to want a snapshot of her pimply face juxtaposed with images of *Cosmopolitan* models, then someone who was born with only nine fingers may not want his hand geometry recorded at all. Even intangible fears may develop a basis in fact, for biometric scans might be analyzed for obscure information that is unknown even to those who produce the technology. An HIV-positive gay male may have qualms about biometric imaging which only acquire grounds when it is discovered that his retinal scans are distinguishable from those of HIV-negative individuals.[46]

Our discussion provides a moral foundation for the view that rational individuals should be concerned about having biometric images created, reproduced, or circulated. Representations which uniquely identify a person by means of physical characteristics have inherent moral value as objects connected with one's body, and hence with one's autonomy and self-esteem. Making commodities of them requires justification, not due to a *proprietary* interest in them but because their entry into the public realm denigrates their personal nature. These considerations also suggest that mandating the use of such images without the free consent or deliberation of the subjects is a serious derogation of the right to privacy. Indeed, the use of *mandatory* biometric identification for people who have committed no crime, as with EURODAC, seems like a paradigmatic offense against Kantian principles, for it is a clear case of taking the person as a mere thing, using their body as a means to an end. In light of this, to characterize concerns over the privacy of biometric images as "paranoia", as does Bob Evans of *InformationWeek*,[47] is absurd. There is both a moral basis and a solid set of practical reasons for defending one's right to a controlling interest in physically identifying representations.

It may be objected that common practices like exposing one's face or voice in public, or leaving potential DNA samples at the hair salon, show that we make little effort to prevent the production of such representations. Unlike the demented character in the film *Dr. Strangelove*, we are not obsessively concerned to protect our "precious bodily fluids". Yet we do not anticipate that our physical presence or body matter will be used to create identifying representations we have not endorsed. We do not expect that our Super Bowl ticket will make us part of a digital lineup, and we might be horrified to learn that the barber sold our hair to a DNA research laboratory. Moreover, the fact

[44] Digital photography now makes possible the immediate storage and indexing of a photograph; but unless it is stored in the form of a biometric facial scan it is no more useful for identification purposes than an ordinary photograph scanned into an image database.

[45] I think the above considerations provide grounds for van der Ploeg's perceptive observation that "a space, however small ... still exists between the person and the obligatory pass or identity card, a space that disappears entirely with biometric identifiers, as if the identity card were glued to your body" ("The illegal body ...", p. 301).

[46] Another example, provided by the British POST, is that "a retina scan could reveal if someone is susceptible to stroke; unlikely to be something an individual would want their employer or insurance company to know" ("Biometrics and Security", p. 4).

[47] Bob Evans, "Privacy vs. Paranoia", *InformationWeek*, p. 172, May 7, 2001.

that the *only* widely accepted uses of fingerprinting or DNA sampling are for criminology or equally serious matters is a gauge of the social taboos around the use of such representations. I have suggested that the taboos have ethical grounds as well.

IV. My argument has been that we have both general and special privacy interests in biometric images. This means that privacy is a tradeoff in the use of biometric identification, not that there are no valid uses of such systems. In their "balkanized", sparsely implemented, and somewhat unreliable state the main threat to privacy is from their misuse, not their use. Nevertheless, my thesis leads to conclusions which may not be welcomed by the biometrics industry.

My main conclusion is that the general right to privacy includes the right to control the creation and use of biometric images of ourselves. This right must be a "presumption", as Judith DeCew holds;[48] therefore, derogations of it must be grounded by compelling considerations of public safety or other important norms. If follows from this that we should carefully consider the decision to make biometric images of our bodies available to others. One should think about it on several levels: (1) In making such images available *at all*, one gives up complete control over information that maps distinctively onto one's physical person. (2) In making them available *commercially* one has to ask what degree of safety or convenience would justify the risks of misuse. (3) Making them available for *distribution* or *exchange* involves further risks, to the point where it is difficult to imagine any proportionate gains in security or comfort. (4) Since making them available on public networks maximizes the risk of unauthorized release it is hard to see why anyone should find this acceptable for biometric images, any more than we might want our medical data or signature shared with the entire world without possibility of recall.

By contrast with the careful deliberation I have suggested, consider again biometric payments for fast food, like VeriStar's system. We are given the option of making commodities of our fingerprints in exchange for faster acquisition of cheeseburgers. The choice is portrayed as a casual decision with little or no moral import, and customers are not encouraged to deliberate about it. It is easy to imagine people providing biometric images under time pressure, without forethought. Someone is hungry and late for a meeting; he doubleparks in front of a fast-food restaurant, and finds several cash-paying customers ahead of him. The cash register is malfunctioning, but another register with a biometric scanner is available. In the pressure of the moment the ramifications of sharing his fingerprints with a fast food franchise may not be considered at all.

Financial rewards can have a similar effect. An inset in the hotel magazine article describes how a Berkeley restaurant called High Tech Burrito (HTB) "enticed customers to register their fingerprint image" using the SmartTouch system by giving out "HTB points good for food purchases"; customers were thereby "automatically enrolled in the Club HTB loyalty program" which gave out more points. Within a year, "HTB reported that between 65 and 75 percent of consistent customers had signed up for Club HTB via SmartTouch". A further benefit to HTB was that SmartTouch "helped to increase the average ticket" at the restaurant.[49]

The idea that submission of biometric data is a serious decision is at odds with the practices of biometrics vendors and their clients. Indeed, given all the moral considerations and social risks, I do not believe the benefits of biometric systems are sufficient to warrant their use at all for ordinary financial transactions (as opposed to, say, access to ATM machines) or for potentially dangerous uses such as " 'keyless entry' into hotel rooms". In any case, I offer the following policy recommendations that run counter to current practices. First, anyone who is asked to voluntarily submit biometric identifiers should be (1) fully informed of the potential risks; (2) competent to understand the impact of their actions; and (3) under no threat of harm to agree to such an action.[50] I would interpret "harm" very broadly here, to include such things as the inconvenience of having to wait in a much longer line.[51] Second, the use of financial rewards to promote participation in biometric identification programs should be discouraged. The decision is too serious to be prompted by burrito upgrades. Such rewards encourage people to substitute short-term pecuniary considerations for the healthy skepticism they normally have about permitting the creation of identifying representations, such as photographs and fingerprints. The skepticism flows from the

[48] See DeCew, *In Pursuit of Privacy*, Chapter 4.

[49] Rinehart, "Biometric Payment".

[50] The notion of free and informed consent as an ethical principal for the management of digital technology was first introduced, to my knowledge, by Carol C. Gould. See "Network Ethics: Access, Consent, and the Informed Community", in Carol C. Gould, editor, *The Information Web: Ethical and Social Implications of Computer Networking*, p. 3. Boulder: Westview Press, 1989.

[51] Similarly I would say that encouraging drivers to adopt highway speedpasses, which involve well-known privacy concerns, by severely restricting the available the non-speedpass lanes, constitutes a coercive and therefore unethical policy.

natural impulse to protect one's personal autonomy, and from an ethical point of view this impulse should be sustained, not undermined. Third, one way to inhibit pressured or hasty decision-making would be to require a waiting period between application and recording of biometric ID's. Like the first two points, this serves to encourage serious deliberation, and also partially offsets the public tendency to assume that any commercial technology that is permitted by law must not pose a serious risk to one's person.

Here are some further conclusions. (1) There should be no mandatory biometric imaging for important social privileges like obtaining a driver's license or credit card, nor in most cases as a condition of employment. If the argument of this paper is correct, such policies in effect force people to compromise a fundamental right to privacy. Even a photo on an ID card is not a comparable invasion of one's personal space. It cannot be acceptable social policy to curtail privacy rights in the absence of compelling arguments that show such curtailment to be the best of all feasible alternatives. I know of no convincing argument of this sort that would justify mandatory biometric identification for any general social benefit. (2) The exchange or sale of biometric id's should be closely regulated. On the principles discussed here, submitting to a biometric scan of one's body is justified only in virtue of significant benefits that offset the loss of one form of autonomy. When benefits accrue only to a second or third party, as with the sale or exchange of such representations, the justification for distributing the representation is absent. Social policy should protect the interests of the individual here by blocking all but the most benign instances of the exchange or sale of biometric id's. (3) Except in the case of major criminal offenses (e.g., murder, rape, or kidnapping), courts should not have the power to subpoena or use biometric information that is not publicly available. If you agree to the creation of a biometric image under the premise of restricted use, the presumption should be that you would not have permitted it had you known that such restrictions could be easily voided by public decree. Therefore the original intention should generally be respected. (4) There should be severe penalties for theft or unauthorized use of biometric data, and for negligence in protecting its security. Most biometric data originates and resides in governmental and corporate databases, and the policies of these organizations will determine the security of the data. There should be every incentive to take these responsibilities seriously.

My goal has been to assess the ethical implications of the use and proliferation of biometric identification systems. It would be regrettable if the above recommendations had an adverse impact on the commercial viability of these systems; but that is not the matter under consideration here.

Addendum: Biometric imaging and terrorism

The events of September 11, 2001, created renewed interest in biometric imaging. The technology was somewhat on the defensive politically for several years as the public grew concerned over things like state-mandated biometric ID's on driver's licenses and the Tampa Superbowl surveillance.[52] The attack and subsequent threats by Al Qaeda changed public attitudes rapidly: airports announced near-term implementation of scanning programs, federal agencies undertook expedited reviews of biometrics-based security systems, and stocks of biometrics vendors shot up (Visionics, for example, which sells facial scanning software, gained some 400 percent the day the markets reopened after September 11). How long the change in attitudes lasts, and how far the public is willing to go in offering up pieces of themselves for the sake of security, depends on how long the perception of a serious threat lasts, but it is far from letting up yet. Bill Joy, formerly chief scientist at Sun Microsystems, Inc., which has entered the biometrics market, was quoted as saying that we need new mechanisms to "govern privacy while at the same time resetting expectations about civil liberties"; and that we have a right to privacy but not to "anonymity".[53] This perspective would not have been taken seriously before the attacks.

The extent to which biometric identification systems are implemented also depends on the degree to which the technology lives up the claims of vendors. But the enhanced profit potential provides an incentive to speed up research and improve the technology.[54]

One thing is clear from past experience: even if the motive turns out to be short-lived, the more the tech-

[52] See Newcombe, "Biometric Breakdown", pp. 035–036.

[53] Larry Greenemeier, "Privacy Vs. Security: The Balancing Act", *InformationWeek.Com*, March 6, 2002; www.informationweek.com/shared/printableArticle?doc_id=IWK20020306S0005.

[54] For some large-scale applications, though, the degree of accuracy required is sobering. To cite the POST once again: "63 million passengers travel through Heathrow each year. If fingerprint scans ... [had] 99.9% accuracy there would be 63,000 errors [per year] – more than 1,000 every week. At this level of accuracy, security staff and passengers may lose confidence in the system and not cooperate with its implementation" ("Biometrics and Security", p. 3). But the ICAO has adopted face recognition, not fingerprints, as its standard, and the best error rate for this method stands at 10%. If implemented today that would result in over 1700 errors per day at major airports – enough to significantly slow down international air travel.

nology is accepted, the more difficult it will be to limit it later on. I don't know if there was ever a significant public safety threat to which mandatory random drug testing was a practical and justifiable response,[55] but the mere fact that such programs were implemented for particular populations due to *perceived* threats, after some highly publicized accidents in which drugs may have played a role, has established them as acceptable in the courts and by the public. The perception that biometric identification systems are a reasonable tradeoff of privacy for security will tend to make them appear acceptable even when the tradeoffs are less clearly to our advantage. Besides, another lesson of drug testing is that programs that would likely be rejected by the general public for universal implementation can be imposed on limited populations which do not have the political strength to stop them on their own. It therefore behooves us to be extremely cautious about the logic on which we accept mandatory or opt-out biometric systems, and to consider in advance the conditions under which we might expect to see them removed.

Then again, subcutaneous implantation of radio frequency identification (RFID) chips is already a commercially available technology, which could, for example, be forced on prospective immigrants, four million military personnel, and the entire prison population. Perhaps we will soon see the opportunity to have our retinas scanned as a desirable alternative to having serial numbers implanted in our scalps. That this opportunity should sound even remotely appealing is an indication of the ethical challenges that digital technology has set before us.[56]

An earlier version of this essay was awarded the 2002–3 Abraham J. Briloff Prize in Business Ethics (presented annually by Baruch College, C.U.N.Y., for the best faculty book or essay in business ethics). In the present version, recent technical developments have been taken into account, part II has been substantially reorganized, and I have made minor changes to the conclusions in part IV. Otherwise, the content is essentially the same as the Briloff Prize essay.

[55] DeCew argues reasonably that in most cases it "can be justified only if there is a substantial and demonstrable likelihood that a significant drug problem exists" (*In Pursuit of Privacy*, p. 139). My reasons for taking an even more restrictive stance are beyond the scope of this paper.

[56] I would like to thank Judith Wagner DeCew, Carol C. Gould, Michael E. Smith, and an anonymous reviewer for this journal, for insightful comments which led to significant revisions and additions to the text. Thanks are also due to James L. Wayman for correcting some of my earlier misconceptions about the technical basis of biometric imaging; needless to say, I am solely responsible for any errors which remain.

References

Biometrics in Human Services User Group (BHSUG). Volume 4, Issue 5. www.dss.state.ct.us/digital/news21/bhsug21.htm, 11/01/2001.

Clyde Wayne Crews Jr. Human Bar Code: Monitoring Biometric Technologies in a Free Society. *Policy Analysis*, 452: 1–20, 9/17/2002.

Jennifer D'Alessandro. Biometric ID To Become Part Of Passports. *varBusiness*, 8/26/03. http://www.varbusiness.com/sections/governmentvar/govt.asp?articleid=43467.

Natalie Dandekar. Privacy. *Philosophical Forum*, 24(4): 331–348, 1993.

Judith Wagner DeCew. *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Cornell University Press, 1997. – "Balancing Privacy and Public Safety in an Age of Technology". Talk given to the Society for Philosophy and Public Affairs at APA Pacific Division Meeting, March 29, 2002. Unpublished.

Bob Evans. Privacy Vs. Paranoia. *InformationWeek*, May 7, 2001, p. 172.

Simson Garfinkel. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly & Associates, Sebastopol, CA, 2000.

Carol C. Gould. Network Ethics: Access, Consent, and the Informed Community. In Carol C. Gould, editor, *The Information Web: Ethical and Social Implications of Computer Networking*, pp. 1–35. Boulder: Westview Press, 1989.

Larry Greenemeier. Privacy Vs. Security: The Balancing Act. *InformationWeek.Com*, March 6, 2002. www.informationweek.com/shared/printableArticle?doc_id=IWK20020306S0005.

International Biometric Industry Association (IBIA). Removing Export Controls on Biometric Technology. Report of February 2000. www.ibia.org/bxacomments.htm.

James H. Moor. Toward a theory of Privacy in the Information Age. *Computers and Society*, 27(3): 27–32, 1997. In Robert M. Baird et al., editors, *Cyberethics: Social and Moral Issues in the Computer Age*, pp. 200–212. Prometheus Books, Amherst, NY, 2000.

Adam D. Moore. Intangible Property: Privacy, Power, and Information Control. *American Philosophical Quarterly*, 35(4): 365–378, 1998.

Elizabeth Neill. *Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self*. McGill-Queen's University Press, 2001.

Tod Newcombe. Biometric Breakdown. *Government Technology*, May 2001, p. 036.

Richard E. Norton. Response to Notice of Proposed Rule Making 12 CFR Part 216. Letter of March 29, 2000. www.ibia.org/fedglbcomments32900.htm.

Richard E. Norton. Privacy 1. Letter of March 30, 2001. www.ibia.org/hhsprivacycomments033001.htm.

Parliamentary Office of Science and Technology (POST) (London). Biometrics and Security. *Postnote*, 165, November 2001.

P. Jonathan Phillips, Patrick Grother, Ross J. Michaels, Duane M. Blackburn, Elham Tabassi and Mike Bone. Face Recognition Vendor Test 2002: Overview and Summary. Report by DARPA, National Institute of Standards and Technology,

DoD Counterdrug Technology Development Program Office, NAVSEA Crane Division, 2002.

James Rachels. Why Privacy Is Important. *Philosophy & Public Affairs*, 4(4): 323–333, 1975.

James Rachels. *The Elements of Moral Philosophy*, 3rd edition. McGraw-Hill College, New York, 1999.

Geneva Rinehart. Biometric Payment: The New Age of Currency. *Hospitality Upgrade Magazine*, Spring 2001. Reprinted at www.hotel-online.com/Neo/News/PressReleases 2000_1st/Mar00_BiometricCurrency.

Thomas Scanlon. Thomson on Privacy. *Philosophy & Public Affairs*, 4(4): 315–322, 1975.

Julia Scheeres. When Your Mole Betrays You. *Wired News*, 3/14/2001. www.wired.com/news/politics/0,1283,42353,00.html.

Leslie David Simon. *NetPolicy.Com: Public Agenda for a Digital World*. The Woodrow Wilson Center Press, Washington, DC, 2000.

Judith Jarvis Thomson. The Right to Privacy. *Philosophy & Public Affairs*, 4(4): 295–314, 1975.

Irma van der Ploeg. The Illegal Body: "Eurodac" and the Politics of Biometric Identification. *Ethics and Information Technology*, 1: 295–302, 1999.

Veristar Corporation, 5/10/2001. www.veristarcorp.com/solutions/enrollment.html,

James L. Wayman. Biometric Identification and the Financial Services Industry. Congressional testimony of May 20, 1998. In James L. Wayman, editor, *National Biometric Test Center: Collected Works*, pp. 263–266.

James L. Wayman, editor. *National Biometric Test Center: Collected Works*. www.engr.sjsu.edu/biometrics/nbtccw.pdf.

John D. Woodward Jr. *Superbowl Surveillance: Facing Up to Biometrics*. Rand Arroyo Center, 2001.