Privacy Implications of Biometric Surveillance:
The Destruction of Anonymity

Elizabeth Ann Masiello

Submitted in Partial Fulfillment
of the
Prerequisite for Honors
In Computer Science

April 2003

ACKNOWLEDGEMENTS

To my family,
for their constant love and support.

And to Lyn and Maud,
for their wisdom, patience and guidance.

CONTENTS

1

INTRODUCTION

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual … the right “to be let alone.”
~ ”The Right To Privacy,” Warren and Brandeis, 1890

INTRODUCTION

This document analyzes privacy in the context of emerging biometric-enhanced technologies in the twenty-first century. My thesis is that biometrics serve to destroy expectations of anonymity, and, when used in conjunction with surveillance, infringe on privacy. I have been trained as a computer scientist, not a philosopher, and so will bring this perspective to my work. I believe it is important for those with technical training to pay close attention to the social issues surrounding scientific advancement. Understanding the technical details is critical to fully evaluating almost all issues arising from scientific advancement. Therefore, scientists have a social responsibility to use their expertise in order to assist in the evaluation of related social problems. It is only by social and scientific analysis together that these problems will be resolved. I will therefore include in this discussion a technical analysis of biometrics, though the focus of this work is on philosophical ideas.

I will argue that privacy as we now know it will be lost in the movement to increase security by introducing biometrics into surveillance systems. This argument will involve an analysis of privacy and the technical strength of biometrics as identification technologies. In particular, I will argue that modern means of surveillance, video surveillance for example, are aimed at the psychological control of individuals; it is through surveillance that enforcers are able to exert power over the enforced. This fact, in confluence with the destruction of anonymity by biometrics, serves to create an environment in which the individual has lost control over his own identity and his ability to think and act freely. When analyzed in the context of common theories of privacy, it is clear that these results are the direct consequence of stripping the individual of his anonymity, and therefore his privacy.

The idea that emerging technologies threaten privacy is a claim that has been argued for decades. It is on one level ironic that privacy is under siege by new technology, because it was a technical innovation that first created the phrase "the right to privacy" back in 1890. The proliferation of the camera in everyday life sparked and fueled frustration among individuals that they no longer held control over the private aspects of their life: "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life."[1] Despite the irony, the story has remained unchanged for the last century: advancing technologies continue to reshape perception of our own identity, altering the types of privacy we seek and expect. In the 1920's wiretapping presented a way of exploiting the telephone as a means of eavesdropping. The development of the personal computer and databases further complicated privacy by digitizing our work and aggregating personal histories into data. The internet has most recently called into question how we value privacy by making

[1] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy," *The Harvard Law Review Vol. IV No. 5* (15 December 1890), 193.

available copious amounts of information about any conceivable topic, including our own private lives. And now, just as the camera made possible the publication of private affairs, so will biometrics make possible the identification of seemingly anonymous, and therefore private, behavior.

The problem of biometrics in surveillance systems centers around the conflict between security measures and privacy. In this country biometric technology received increased media attention following the events of September 11, 2001 as a potential means of preventing further terrorist attacks. Americans have witnessed the deployment of face recognition in airport security already, and this is likely the first of many scenarios in which biometrics will become a part of common tasks. In Great Britain a similar string of events occurred: following increased violence between the British and the Irish Republican Army, the British turned to Closed Circuit Television as a means of enforcing the law in public areas and deterring terrorism. What has since taken place in that country may be America's future: Great Britain has now installed an estimated 2.5 million cameras to monitor public street corners and parks, a growing number of which have facial recognition installed as a piece of the system.[2] Interestingly, the goal of these systems is no longer to prevent terrorism but is now to monitor the common criminal.[3]

The central question is how we define private affairs. There is no definitive agreement on whether an action in public is public by default, or if it can in some cases be afforded a certain measure of privacy. If you give a speech to a large crowd in a public arena, then there is little argument that your words are public. On the other hand, if you and a friend are having a conversation as you stroll through an park, it is unclear whether you have an expectation of privacy. One argument is that in public, all expectations of privacy are forfeited, while another view holds that under given circumstances privacy can be expected and maintained in public.

I will not attempt to provide a definitive answer to the above issue. I will however assert that anonymity is an often ignored piece of privacy, regardless of which theory of privacy you use. Ignoring it complicates the issue of privacy, and some attention to the details surrounding identity will help clarify these questions. Within this context I will address the problem of biometrics and surveillance.

There are four main chapters in this work and a conclusion, each of which will address a specific piece of the overall problem of biometrics in surveillance. Chapter 2 discusses privacy. The topic of privacy is huge in its scope and ranges from historical to legal to philosophical content. I will attempt to provide both an etymological and legal history of privacy in this country. While it is possible to analyze privacy over thousands of years, my analysis will focus largely on the last century in America, during which time our understanding of privacy has matured and deepened. I will focus the final pieces of this chapter on the philosophical theories of privacy. This is, I believe, the most important analysis of privacy. Because the term is not well defined but rather vague and ambiguous, it is critical to break the theories down and attempt to understand just what privacy is in a liberal society. I will provide four scenarios which I feel are not well handled by the current theories and explain the holes in the prominent theories in this context.

[2] Jeffrey Rosen, "Being Watched: A Cautionary tale for a New Age of Surveillance," *New York Times Magazine*, 2.

[3] Rosen, "Being Watched: A Cautionary tale for a New Age of Surveillance," 2.

In Chapter 3 I supplement the theories of privacy discussed in Chapter 2 with my own analysis of anonymity. One detail I found lacking in all the work on privacy is the component that involves identity. In many cases, it seems that we tend to assume identification is or is not possible, without analyzing the difference the distinction has on the outcome of the situation. I break identity into concrete terms in an attempt to place anonymity within the leading theories on privacy. In doing so I return to the four scenarios presented in Chapter 2 and show why anonymity is such a critical concept when we discuss privacy.

I then discuss biometrics from a technical perspective in Chapter 4. In saving this discussion for a later point in the work, I hope to provide a context of identity and anonymity within which to put the technology. Understanding the technology is critical to addressing the problems it poses for society, regardless of which emerging technology we deal with. I provide a brief overview of the use of biometrics and their effectiveness and accuracy, and then describe in detail several specific technologies I believe will be valuable in the surveillance industry. In addition, I show that biometrics have potential to be used successfully in access control as a means of verifying identities. Among those biometrics I will address are the face, iris, voice, gait and DNA. I touch on fingerprints as an example of a mature biometric, and very briefly on thermal IR facial recognition as an example of an emerging tool that, if improved upon and deployed, might revolutionize our ability to identify people in various environments.

The final chapter focuses on surveillance. There has been a great amount of work done in recent years on data surveillance, and what work there is on video surveillance or wiretapping is often lumped into this same category. I show why this categorization is inaccurate, and discuss the distinct problems each type of surveillance poses for both identity and privacy. I use a theoretical structure, the Panopticon, to analyze the ways in which surveillance can create power and can coerce behavior among individuals, and show that this coercion is only strengthened by absolute identification as is provided by biometrics.

It is my intent to show that while biometrics can be used in access control[4] successfully, their integration into surveillance systems only serves to further control behavior among the people, destroying what has been called “privacy in public.”[5] I also argue that in fact this integration will not vastly improve the enforcement mechanisms already so strong in video and other forms of surveillance. On such a scale as public surveillance, biometrics are not yet a strong enough form of identification to be relied upon, and therefore the only real enhancement they will provide is in deterrence. It is

[4] Access control refers to the verification of an individual authorization to gain access to a secured area or to secure information.

[5] Helen Nissenbaum, “Protecting Privacy in an Information Age: The Problem of Privacy in Public,” *Law and Philosophy: An International Journal for Jurisprudence and Legal Philosophy*, 17 nos. 5-6 (November 1998): 559.

therefore important to realize that even if the only intended deterrence is from criminal behavior, privacy is invaded and the potential has been created to destroy it altogether.

2

PRIVACY

pri-va-cy n 1.a. The state or condition of being withdrawn from the society of others, or from public interest; seclusion. 1.b. The state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion. 2. Absence or avoidance of publicity or display; a condition approaching to secrecy or concealment.

~ Oxford English Dictionary

PRIVACY

Americans in the twentieth century became enamored with the “right to privacy,” so much so that it is now not uncommon to meet a person who mistakenly believes the United States Constitution guarantees such a right. In fact, the so-called “right to privacy” remains ill-defined and, in the context of continual technological change, has been subject to constant reevaluation since its conception in the late nineteenth century.

The potential of a right to privacy emerged in America in 1890 when the *Harvard Law Review* published an article written by two alumni, Samuel D. Warren, Jr. and Louis D. Brandeis, titled the “Right to Privacy.”[1] In this article, the two men argued for privacy as a “right to be let alone,”[2] an idea that sparked a century of debate over the right of an individual from various intrusions by others. With the proliferation of the photograph came lawsuits over the right to ownership of one’s own image.[3] In the 1930s the advent of electronic surveillance, or wiretapping, presented new questions about the extent to which private conversations are free from intrusion. A great deal of theoretical discussion was prompted by wiretapping in the 1960’s and 1970’s, the decades in which such definitive works as *Privacy and Freedom* by Alan Westin were written. Most often this discussion revolved around an attempt to pin down what exactly the right to privacy entails, if it even exists. Now, thirty years later, at the start of the twenty-first century, America is entrenched in an Information Age that threatens to redefine privacy altogether.

Increasingly, the discussion has moved away from the philosophical underpinnings of privacy to analyses of the ways in which ubiquitous computing and data surveillance threaten this right to privacy. Judith Jarvis Thomson explains in her 1975 article “The Right to Privacy,” that “nobody seems to have any very clear idea what [the right to privacy] is.”[4] If the term was vague in 1975, the problem has only worsened with time. As technological growth has taken place at a faster pace than our legislative process can keep up with, our notions of privacy have become outdated. Thomson presents examples such as domestic quarrels loud enough to be overheard, or the possession of a concealed pornographic picture that can be viewed using an X-ray device.[5] Westin describes technologies that he predicted would threaten privacy in the 1970’s, such as “powerful binoculars, long-range telephoto cameras, and ‘zoomar’-type television cameras” in addition to “wiring a person’s clothing.”[6] Today, however, society

[1] Robert Ellis Smith, *Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet* (United States of America: Robert Ellis Smith, 2000), 121-26.
[2] Warren and Brandeis, 193.
[3] Smith, 138-39.
[4] Judith Jarvis Thomson, “The Right to Privacy,” *Philosophy & Public Affairs* 4 no. 4 (Summer 1975): 295.
[5] Ibid, 300-304.
[6] Alan Westin, *Privacy and Freedom* (New York: The Association of the Bar of the City of New York, 1967), 73-78.

is threatened by far more sophisticated technology. Take, for example, the opening lines of Mark Tunick's essay, "Privacy in the Face of New Technologies of Surveillance," published in the year 2000:

> "The government routinely conducts aerial surveillance, uses infrared thermal imaging devices, and conducts random drug tests involving sophisticated chemical analysis of urine or hair samples, all without search warrants or probable cause. As technologies continue to develop, the capacity to uncover information will continue to expand. People's movements can be monitored through the use of microchip implants; millimeter-wave cameras can detect concealed weapons; a sensor that detects gravity fluctuations may soon provide the ability to reveal contraband in closed containers."[7]

Clearly, the discussion of privacy deserves revisiting, as technologies have been realized that were previously not easily conceived by human imagination.

The issue with which I will concern myself most directly is the use of biometric identification in surveillance systems. However, before dealing with this specific topic, I believe it is critical to examine the background of this "right to privacy" in Western thought over the last several centuries. Although I will be unable to provide an entirely comprehensive survey of the right to privacy, I will attempt to give an overview of the history and philosophy behind the current concept of such a right. I will not attempt to define privacy, but I will provide my own analysis of its complexity, using the earlier works of several philosophers as a starting point. In the following chapters I will show that anonymity is a necessary component of privacy and is threatened by the advancement of biometric technologies in surveillance.

AUTONOMY AND PRIVATE PROPERTY

In order to understand privacy, it is helpful to understand the roots of the word's meaning. This is different from evaluating the history of private life; humans have always kept some aspects of their lives private without necessarily describing general privacy as a natural right. It has been argued that the "modern claim to privacy derives first from man's animal origins and is shared, in quite real terms, by men and women living in primitive societies."[8] However, even if the specific values that compose our modern understanding of privacy are ancient ones, we still need to understand what exactly is meant by privacy in the context of the twenty-first century and how that meaning has developed.

The term "private" is derived from the Latin root "privare," meaning to bereave, deprive, rob, isolate, or make solitary.[9] The root definition appears different from those provided for privacy today: "freedom from interference," the "state of being withdrawn," and "avoidance of publicity."[10] In fact, a link can be drawn between the two definitions, but still a distinct transformation has occurred. In being apart from others, one is isolated and solitary. However, secrecy and anonymity, implied by "the state … of being alone,

[7] Mark Tunick, "Privacy in the Face of New Technologies of Surveillance," *Public Affairs Quarterly Vol. 14 No. 3* July 2000, 1.

[8] Westin, 7.

[9] Patricia Boling, *Privacy and the Politics of Intimate Life* (Ithaca: Cornell University Press, 1996), 44.

[10] Oxford English Dictionary, 2nd ed., (1989), "privacy."

undisturbed, or free from public attention,"[11] are certainly not present in the earliest definition, although included in today's. Privacy now incorporates more than physical isolation or solitude; it has come to include a sense of individual control over decisions, controlling access to personal information, the choice to keep one's life secret if one so desires. The word has also acquired a positive connotation in the last several hundred years, having become associated with "personal" in a positive manner.[12] According to Raymond Williams, the association of private with "withdrawal" and "seclusion" became outdated in the 16th century, when private became associated with "independence" and "intimacy."[13] This transformation reflects the influence of individualism on social values. We will see that the concept of privacy has been affected by the philosophical and political idea of personal autonomy, as well as the development of individualistic societies in the West.

Some of the earliest ideas of a private space came from Aristotle, who saw a very distinct separation between the public sphere of politics, and the private sphere of the home and family life.[14] John Locke later elaborated on the concept, deriving a right of all humanity to private property. His argument rests on the statement that "every Man has a *Property* in his own *Person*. This no Body has any Right to but himself."[15] Based on this idea, Locke argued that a person has sole control over the land on which he exerts labor.[16] Locke's philosophy had a huge impact on Western thought, especially American ideals, as evidenced by the presence of a right to property in the United States Constitution.

John Stuart Mill was among the first philosophers to make a claim for individualism, another idea that had enormous impact on western thought. In his essay "On Liberty" Mill argues, in short: "Over himself, over his own body and mind, the individual is sovereign."[17] Similar to Locke's argument that the individual has sole power over his private property, Mill argues that the individual has sole power over his own thoughts, his own body, in effect over his own private self. The ideas of Mill and Locke seem to have combined in transforming privacy to its current conception, an idea of control over one's self, body, and life.

After the introduction of individual thought and private property to Western society, the modern concept of privacy began to take place. The word privacy, distinct from "privacies" or "private", did not come into common usage until the nineteenth century.[18] During this time, the term came to embody the meanings provided in the definition at the start of this chapter, "condition of being alone, undisturbed, or free from public attention, as a matter of choice or right."[19]

[11] Ibid, "privacy."

[12] Raymond Williams, *Keywords: A Vocabulary of Culture and Society* (New York: Oxford University Press, 1976), 204.

[13] Ibid, 204.

[14] Judith Wanger DeCew, *In Pursuit of Privacy: Law Ethics, and the Rise of Technology* (Ithaca: Cornell University Press, 1997), 10.

[15] John Locke, *Two Treatises of Government*, "The Second Treatise," ed. Peter Laslett (Cambridge: Cambridge University Press, 1988), 287.

[16] Ibid, 287-290.

[17] John Stuart Mill, *On Liberty and Other Writings*, Ed. Stefan Collini, (Cambridge: Cambridge University Press, 1989), 13.

[18] Oxford English Dictionary, 2nd ed., (1989), "privacy."

[19] Ibid, "privacy."

Patricia Boling, in her book *Privacy and the Politics of Intimate Life* , presents a contrast of the terms private and public, and in doing so provides clarification of the concept of privacy. In her analysis of the myriad of definitions of private as provided by the *Oxford English Dictionary*, Boling concludes the following:

> "…we can articulate various dimensions of privateness: lack of (or sometimes freedom from) public or political office, involvement, or significance; intimacy; exclusivity, including the ability to control information about oneself and contact with the world; ownership; and objective impact."[20]

Unfortunately, it is likely that Boling's list cannot come close to enumerating all the dimensions covered by privacy. Privacy is dependent on context, and our understanding of its meaning evolves as conditions change, be they legal, economic or technological.

TWENTIETH CENTURY AMERICAN LAW

Warren and Brandeis drafted their 1890 article in response to what they deemed invasions of individual privacy by the press.[21] In particular, they were spurred by the technological innovation of the photograph. In 1884 the acquisition of photographs was made simpler by the innovation of a handheld camera, and as Robert Ellis Smith points out, this innovation had a "special impact:" "Imagine the realization that for the first time the very essence of your being – your visage – could be captured by someone else – used and controlled by someone else."[22] Smith implies that your image alone carries the power often reserved for one's soul; today, with modern plastic surgery one's image may change while the soul remains constant. Perhaps it would be more accurate to describe one's visage as a representation of the "very essence of a being"[23] rather than the essence itself. Nonetheless, capturing another's image was a novel capability provided by the advent of new technology, and a capability that provoked a great deal of concern among Warren and Brandeis about individual privacy.

"The right to be let alone"[24] was tested and defeated by the courts shortly after its conception. In a landmark case, the New York Court of Appeals denied the existence of a right to privacy, leaving open the avenue by which legislatures could enact laws protecting such infractions as the use of a portrait for "purpose of trade without the written consent."[25] By deeming a right to privacy too broad to be legally protected, the New York Court established a precedent whereby future attempts to secure privacy would protect only specific examples of the concept. Later in the century, Thomson argued that the right to privacy is derived from other, more fundamental rights and is therefore not in and of itself a fundamental right,[26] an argument that seemingly justifies the court's decision not to protect a sweeping right to privacy. However, as I show in the next section, Thomson's argument fails to address many necessary questions related to privacy, and therefore is not a very robust argument.

[20] Boling, 45.
[21] Smith, 124.
[22] Ibid, 124.
[23] Ibid, 124.
[24] Warren and Brandeis, 193.
[25] Smith, 140.
[26] Thomson, 312-314.

A second innovation would again challenge the right to privacy in America's legal system. It has always been difficult to protect the privacy of a conversation between two people. Even if they believe themselves to be alone, it is often possible for an eavesdropper to gain close enough proximity to a conversation to overhear the content, whether it takes place in public or requires trespass onto private property. The invention of the telephone in 1876 introduced a false feeling of increased privacy. Since a phone conversation involved people in two disparate locations, it would be difficult for any traditional eavesdropper to overhear the conversation in its entirety, and thus the content of the conversation was protected. However, it was not long before technology became available to "tap" a phone line, leading to the proliferation of wiretapping as a means of eavesdropping on telephone conversations from afar. It was the case of Roy Olmstead's conviction for illegally trading liquor in 1928 that first raised the question whether secret wiretaps constitute an invasion of privacy.[27] At the time, the Supreme Court decided that electronic seizures were constitutional in *Olmstead vs. United States*.[28] Forty years later the issue resurfaced when a man named Katz entered a phone booth and was subject to wiretapping. Katz was involved in illegal betting, and while making a phone call from a public phone booth was the subject of an FBI wiretap.[29] The question at hand was whether he could expect any sort of privacy while conversing on a public phone line. This question made its way to the Supreme Court, who in 1967 decided *Katz vs. United States.* [30]

The Court ruled in favor of Katz, sticking to Brandeis and Warren's definition of the right to privacy, but still failing to grant privilege to such a broad definition of privacy under United States law. On the subject of public versus private information, however, the Court did lay the following precedent: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment[31] protection, but what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[32] Perhaps, then, privacy is a conditional right granted by the U.S. Constitution, dependent on intent. The Court seems to have determined that it is the intent to keep something private that qualifies its status as a right, not the gravity or quality of the actual thought, action or information in question.

American privacy law now rests on the "reasonable expectation of privacy," a precedent also set by the *Katz* decision. Katz, in fact, had such an expectation, because "one who occupies [a phone booth] is entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[33] That is to say, he had reason to believe no one was listening to his phone conversation. Such a definition is interpretive, and, as such, accomplishes very little in defining a right to privacy. For instance, does an individual have a reasonable expectation of privacy in a private conversation on an

[27] Smith, 147-49.
[28] Ibid, 149.
[29] Ibid,170.
[30] *Katz vs. U.S.,* 373 U.S. 427 (1963).
[31] The Fourth Amendment of the *United States Constitution* reads: "The right of the people to be secure in their persons, houses, 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 place to be searched, and the persons or things to be seized."
[32] *Katz vs U.S.,* 373 U.S. 427 (1963)
[33] Ibid.

isolated park bench?[34] Returning to the question of intent for a moment, such an individual has demonstrated an intent to keep the conversation private by seeking a location isolated from others, believing that he is "[free] from the observation, intrusion, or attention of others," and, by definition, in private and therefore warranted protection by the U.S. Constitution. But would the courts uphold such an argument? Has such an individual, by knowingly allowing the possibility for eavesdropping, given up any expectation of privacy? Or, is it no different than a phone wiretapping case?

Unfortunately, the legal system lacks an enumeration of all possible interpretations of the law, and the U.S. Constitution, in fact, admits in the Ninth Amendment that it is not exhaustive of all inalienable rights. In the case of the isolated park bench, the law is as yet unclear, and although the law continues to evolve, it has yet to entirely clarify privacy. The United States legal system has illuminated the evolution of our ideas about privacy, but is not very helpful in the twenty-first century in analyzing what falls into the category of privacy and what does not.

PHILOSOPHICAL APPROACHES

In the 1970s there was a proliferation of thought on the topic of privacy as a natural right, most likely the result of recent court cases such as *Katz* and the famous abortion case, *Roe v. Wade*, which argued that a woman's body is private. The common sentiment was one of distress over the ways in which modern technologies were eroding privacy, but validating that argument proved challenging.

The first and foremost challenge for theorists of the time was definitively describing what was meant by privacy. For each the meaning differed slightly, thus altering the argument posed. Alan Westin defined privacy as the ability to "determine for themselves when, how, and to what extent information about them is communicated to others."[35] Westin emphasized the choice each citizen has between participation in public affairs and a solitary lifestyle, noting in particular that for most people a balance is sought that shifts with circumstances. He also established four "basic states" of privacy: solitude, intimacy, anonymity, and reserve.[36] His work was among the most detailed analyses of privacy to surface during the twentieth century, examining the values from the most basic concepts in the animal world to the most complex examples of the time: wiretapping, lie-detector tests and the earliest forms of data surveillance. Westin's work generated ideas that still have relevancy to current problems of privacy: that privacy involves control over personal information, that it is intrinsically linked to autonomy and freedom, and that it involves a choice of when to seek solitude and when to seek publicity.

Shortly after Westin's work was published, Charles Fried published an article, "Privacy [a moral analysis]." Fried made some similar arguments as Westin, namely that "[privacy] is the *control* we have over information about ourselves."[37] Fried also extended this argument to include the idea of intimacy. "But intimacy is the sharing of information about one's actions, beliefs, or emotions which one does not share with all,

[34] Example created by Judith Jarvis Thompson, 298.

[35] Westin, 7.

[36] Ibid, 31.

[37] Charles Fried, "Privacy [a moral analysis]," *Philosophical Dimensions of Privacy: An Anthology*, Ed. Ferdinand Schoeman, 209.

and which one has the right not to share with anyone."[38] By linking control over personal information to relationships with others and intimacy in particular, Fried extended the importance of privacy in a way that would be echoed by later philosophers.

Almost ten years after the publication of Westin's *Privacy and Freedom* and Fried's "Privacy [a moral analysis]," the journal *Philosophy and Public Affairs* published a series of articles on privacy. The first of these was Thomson's work "The Right to Privacy." Thomson, in fact, answers the question she originally posed regarding a conversation held at an isolated park bench. She holds, without question, that should a man hide behind bushes in order to overhear such a conversation, he "violates the right to privacy – fully as much as if he had stayed a hundred yards away and used an amplifying device to listen to us."[39] Later though, Thomson holds that people engaged in a loud domestic argument in the privacy of their home, but with windows open, have no right to privacy against a passerby who might overhear the conversation because "[they] have let him listen" and have therefore waived a "right to not be listened to."[40] Here lies once again the problem of privacy: it seems entirely dependent on circumstance and interpretation. Has the couple in their own home not taken the necessary steps to prevent eavesdropping in their own home, even if a window is open? Why are those who seek privacy in a public location entitled to this right of not being overheard when those who seek privacy in their homes are not? Where is the line drawn? Thomson argues that there is no line, that the right to privacy is in reality not a right in and of itself, but instead justifies her claims based on the fact that one is entitled to other rights: "the right that no one shall torture [one]," "the right to life," "the right to not be looked at," and so on.[41] I find Thomson's treatment of privacy difficult to follow logically, and present it here only as an opposing argument to more relevant works.

Two other works on privacy appeared in that same issue of *Philosophy and Public Affairs*. Thomas Scanlon's piece "Thomson on Privacy" served to refute Thomson's main argument. While agreeing that "the rights whose violation strikes us as invasion of privacy … do not derive from any single overarching right to privacy,"[42] Scanlon argued that these rights do have a common base in preventing intrusions. Scanlon describes social conventions put in place to protect from such intrusions which create a "zone," presumably a zone of privacy. Scanlon does not argue that there is a right to privacy, but instead claims that our social conventions and norms protect privacy regardless of its status as a right or not. His connection between privacy and social conventions is an important one. Take, for example, the proliferation of email and the changing social conventions that have followed. As Justice Brandeis' dissent in *Olmstead* illuminates for us, the idea of rummaging through personal letters 70 years ago was one that defied social conventions; laws were put in place to prevent it. However, as current legal cases have shown, personal letters sent electronically are not private, and social conventions today provide little protection against their search and seizure. Scanlon failed to define privacy but succeeded in linking its existence to social conventions, a link that reflects

[38] Ibid, 211.
[39] Thomson, 298.
[40] Ibid, 306.
[41] Ibid, 304-305.
[42] Thomas Scanlon, "Thomson on Privacy," *Philosophy & Public Affairs* 4 no. 4 (Summer 1975), 315.

the always-changing nature of privacy. This link to social conventions was extended on in the subsequent article by James Rachels.

Rachels followed Scanlon's piece with an analysis of privacy as integral to humans' abilities to form successful social relationships, an argument very similar to that made by Fried. Rachels' approach echoes social psychology in its emphasis on human relations, but nonetheless illustrates the necessity of humans to have a certain level of control over personal information, an idea that Westin had argued but which Scanlon and Thomson failed to explore. It is also a focus that legal analysis fails to account for, but one I feel is critical to any right to privacy. Rachels points out that "a fact about ourselves is someone's business if there is a specific social relationship between us which entitles them to know."[43] This analysis, I believe, accounts for the seemingly contradictory examples Thomson supplied.

Rachels returns to Thomson's example of personal gossip as no violation of privacy, but argues that despite how the personal information may have been obtained (perhaps through innocent and accidental eavesdropping, by Thomson's account no invasion of privacy), a right to privacy is still violated because although the information was obtained innocently, it was obtained without the subject's knowledge or agreement – without his permission. Applying a similar argument to the isolated park bench and the domestic quarrel clarifies the earlier questions I posed. Perhaps the individuals on the park bench accidentally allowed an eavesdropper to gain personal information; this is, as Thomson maintains, a violation of the right to privacy if the eavesdropper makes use of this information. Likewise, if a passerby overhears the domestic quarrel because a window was accidentally left open, he violates the couples' right to privacy if he discloses to another the quarrel he overheard. The example is even more complicated than Thomson initially suggests. What if the eavesdropper accidentally hears the conversation, in either case, and does nothing with the information he obtains? Perhaps he knows the couple in the house, and had thought them a happy couple but now has a changed opinion. Or perhaps he overheard juicy details of a personal conversation between two friends in the park, and suddenly views them in a changed way without ever disclosing this information to others. In either case, is privacy violated? Rachels fails to account for the complexity of the example because he fails to define the means by which we control information about ourselves. It is not clear from his argument whether these two people had attempted to control personal information, or whether they had chosen to make that information publicly available by the choice of location. Rachels does make clear that control over personal information is critical, but fails to clarify how one exerts such control.

One year following the publication of the previously discussed articles, Jeffrey Rieman wrote a piece critical of the earlier theories titled "Privacy, Intimacy, and Personhood." Rieman argued that not only was Thomson wrong in her thesis that the right to privacy is derivative of other rights, but that Scanlon and Rachels "[thought] so for the wrong reasons."[44] Rieman builds his case from the analysis of Stanley Benn who claimed that any unwanted observation is a violation of privacy.[45] While Rieman seems

[43] James Rachels, "Why Privacy is Important," *Philosophy and Public Affairs* 4 no. 4 (Summer 1975), 331.

[44] Jeffrey Rieman, "Privacy, Intimacy, and Personhood," *Philosophy and Public Affairs* 1 (Autumn 1976), 27.

[45] Ibid, 37.

to find this argument compelling, he believes it "gives us too much" by providing no restrictions on one's ability to decide any observation is unwanted.[46] Rieman instead contends that "privacy is a social ritual by means of which an individual's moral title to his existence is conferred."[47] Essentially, Rieman says that privacy is critical to the development of a "self," that realizing one's existence depends on the right to privacy. This argument presents new questions that are outside the scope of this work, such as how we define "self" and "existence." Nevertheless Rieman presents a theory of privacy that implies its classification as a fundamental right.

Many recent theories of privacy have centered around control over personal information, sparked in part by the Information Age and the emergence of data surveillance. As data storage and database manipulation became easier and cheaper in the 1990's, people came to feel that technology was invading privacy in ways that had not previously been experienced, perhaps redefining privacy altogether. Privacy had long been reduced to control over personal information, but, in the wake of data surveillance the idea took on increased gravity and appropriateness. Wade Robison builds on this idea in his construction of a theory of privacy in his 1997 article "Privacy and Personal Identity." Robison focuses on the change in the representation of identity and the resulting change in privacy. He holds that the aggregation of personal data creates a risk that the aggregate information will be taken, an act commonly known today as identity theft, and that "what is taken is someone's identity, and it is taken by means of information over which the person whose identity is taken has little or no control."[48] In connecting the control of information with a broader, more abstract idea like identity, Robison turns the discussion of privacy entirely away from property and to the fundamental questions of liberty. His theory fails to answer questions that were left open by earlier philosophers, such as the example of eavesdropping on conversations in public.

Helen Nissenbaum focused on a problem similarly spurred by the advent of data surveillance, and, in 1998, proposed an argument for "privacy in public," attempting to provide a solution to a problem which had "been explicitly excluded or merely neglected by many … philosophical and legal works on privacy."[49] Nissenbaum was concerned with the way in which privacy was invaded through the collection of large amounts of publicly available data, a situation in which individuals hand out their personal information, giving up any control they may have had over the information, becoming "in some sense, complicit in the violation of their own privacy."[50] Nissenbaum points out that many scholars had dismissed any such right of individuals to the privacy of publicly available information, citing Rieman and Charles Fried in particular.[51] Nevertheless she relies on the theories of other scholars to support her claim that removing information from its original context and aggregating disparate types of data both constitute an invasion on one's privacy. The difference, Nissenbaum points out, between publicly available pieces of data and aggregated data is on the side of the entity observing this data; not only is the "magnitude, detail, thoroughness and scope" of aggregated data

[46] Ibid, 37.
[47] Ibid, 39.
[48] Wade Robison, "Privacy and Personal Identity," *Ethics & Behavior* (Volume 7 No. 3 1997) 204.
[49] Nissenbaum, 560.
[50] Ibid, 565
[51] Ibid, 571-2.

different, but the profiles created by aggregate data are “capable of exposing people quite profoundly” whereas “isolated bits of information are not especially revealing.”[52] Because this argument was absent from earlier works, Nissenbaum’s points are important to note; however she does not attempt to provide a complete theory of privacy and thus, like Robison, leaves many fundamental questions unanswered, like that of the park conversation.

Most recently a pair of scholars have presented ideas which are broad and perhaps pose more questions than answers, but which nonetheless are an interesting and novel approach to privacy. Mark Alfino and Randolph Mayes present a theory of privacy which hinges on the ability of individual to think freely for themselves.[53] It is similar to the argument that privacy and liberty are intrinsically linked, but slightly distinct. The argument here is that “to assert a right to privacy is to assert a right to exercise our rationality without undue interference from others.”[54] These two argue that in fact the act of observation is in and of itself no violation of privacy, that “whatever the potential harms of spying, the act of observation itself cannot be one of them.”[55] In fact the only time that observation becomes an infringement of this right, according to Alfino and Mayes, is when the observed becomes aware that he is the subject of someone’s attention. It is only at this time that the act of observation “interferes with the exercise of rationality.”[56] And, contrary to most other points of view, “knowing personal information does not itself constitute a violation of privacy.”[57] Alfino himself goes into more detail in “Misplacing Privacy,” an article published in the *Journal of Information Ethics*. Although this work is merely the beginning of future research, Alfino goes so far in the short piece to claim that in the traditional scenario of a “peeping Tom” “the crucial loss of privacy occurs not from the peeping, but from my awareness that I am being observed in a way that compromises my ability to think.”[58] This argument is interesting in particular because of the emphasis Alfino places on one’s ability to think; not only does this link privacy with liberty, but implies a theory of privacy through which any form of known surveillance would violate privacy. From this interpretation, I would guess that Alfino’s theory will answer the question of a conversation in a public park differently from those before him. I imagine that under this theory, should two people be aware of the presence of an eavesdropper this would constitute an invasion of privacy. However, should those two people be unaware of the eavesdropper, despite any intentions he may have, this might not constitute an invasion of privacy – it would be quite similar to the case of a Peeping Tom. These views are interesting in their divergence from traditional thinking on privacy, and perhaps reflect a change in our thinking about privacy that may be a result of the increased data surveillance in the last decade.

[52] Ibid, 588-89.

[53] Randolph Mayes and Mark Alfino, “Rationality and the Right to Privacy.” *Today’s Moral Issues*, ed Daniel Bonevac. (Mountain View: Mayfield Publishing, 2001), Retrieved on October 15, 2002 from http://guweb2.gonzaga.edu/faculty/alfino/dossier/Papers/Rationality_and_the_Right_to_Privacy.doc.

[54] Ibid, 4.

[55] Ibid, 5.

[56] Alfino, “Misplacing Privacy,” *Journal of Information Ethics*, (Fall 2001), Retrieved on October 30, 2002 using WilsonSelectPlus, Wellesley College, 2.

[57] Alfino, “Rationality and the Right to Privacy,” 5.

[58] Alfino, “Misplacing Privacy,” 2.

IS A NEW APPROACH NEEDED?

The well-recognized problem with privacy is that it is an ill-defined term. As I have just shown, the most respected philosophers disagree about what exactly privacy is and where we draw the lines of a natural right. The theories vary from a right to control over personal information to a right to uninfluenced thought. In some cases privacy is referenced as a physical zone over which the individual is sovereign, in others as a component of individual development and successful interpersonal relationships. The problem with having such disparate theories is that each attempts to answer different questions; perhaps it would be helpful then to enumerate a set of situations that might illuminate the concept of privacy. While the general idea behind several of these examples has appeared in various literature, I have provided four scenarios and associated variants that I believe cover a wide range of privacy issues. For each of these situations and subsequent variants, it is necessary to try to answer the question: "Has privacy been violated? If so, why? If not, why not?"

1. a. A jogger overhears a conversation between you and a close friend, and stops to stretch his legs nearby so he is within earshot of the conversation. Or, as a variant, he innocently stops to stretch his legs and happens to overhear the conversation as a result.
   b. Instead of a jogger, the eavesdropper is a man creeping through bushes behind the bench so as not to be seen.
   c. You see a man standing nearby, overtly listening to your conversation.
2. a. If Alice and Bob are lovers, and Alice accidentally sends a letter intended for Bob to Carol's address. Carol knows neither Bob nor Alice. Carol opens the letter and realizes immediately that it was intended for Bob, but she continues to read despite this knowledge.
   b. The same situation as above, but in this case Carol is an acquaintance of either Alice or Bob, or both.
3. The neighbor to the left of your home has a habit of sitting on his front porch and inadvertently watching people come and go from your house. The neighbor to the right of your home wants additional security for his home and places a video camera on the front of his house to record the comings and goings of visitors or intruders. He also inadvertently places your front yard under surveillance, monitoring the comings and goings of visitors to your house as well.
4. You have become the subject of an investigation by a corrupt government because of your dissenting political views. Although you are completely ignorant of their actions, government officials are monitoring the purchases made on credit cards, bank withdrawals, when and who you call on the telephone, and maybe even the toll history your electronic fast-pay system records on the local turnpike. It is discovered that you make frequent purchases at a local alcohol store and use the telephone for frequent calls to your teenage niece's house, and that your car often makes the trip between your exit on the turnpike and hers. One weekend, your niece is caught throwing a wild party at which alcohol was served to minors. Based on the circumstantial evidence gathered, you are charged with providing alcohol to minors and a formal investigation is opened into this charge.

These are four situations which I believe would be inadequately handled by the theories present in the literature. In particular, many of these theories fail to support anonymity as an integral piece of privacy, and those that make this claim do so only partially. I will not attempt to compose a definition of privacy, but I will argue in the following chapter that anonymity is a critical piece to any definition or theory of privacy.

These situations are carefully constructed to illustrate that the absence or presence of identity drastically changes the way we think about privacy, a fact that does not receive enough attention in current discussions about privacy. First it will be helpful to examine the weaknesses in the present theories in the context of these examples. I will return to these examples later to further illustrate my argument on identity and anonymity.

The first in the series of examples was initially presented by Judith Jarvis Thomson, although I have expanded it and provided more detail. Thomson holds that in the case of the eavesdropper creeping behind the bench, privacy is violated. The three examples I provide, the creeping eavesdropper, the accidental eavesdropping on the part of a jogger, and the case of an overt eavesdropper, illustrate some questions about the right to privacy. It would not be unreasonable to argue that in all three cases, a right to privacy has been forfeited since the conversation takes place in public. This is especially true of the overt eavesdropper – not only are you conversing in public, but doing so with the knowledge that this man is listening in. But perhaps the secretive eavesdropper violates your privacy by disregarding an obvious, if failed, attempt at seeking privacy. A robust theory of privacy would sufficiently deal with these possibilities, distinguishing between the three situations.

Now take the example of Alice, Bob and Carol and the accidental exchange of a personal letter. Again, one might argue that any right to privacy is forfeited when the letter is mistakenly sent to Carol; if Carol has properly received a letter addressed to, but not intended for herself, she has only acted in an expected manner. The most logical conclusion is that no right to privacy would be violated if Carol were not to read the letter beyond her awareness of its intended recipient. However, if Carol continues to read the letter, is her negligence of Alice's intended privacy a violation of that privacy, or simply an unfortunate consequence of Alice's carelessness? On the one hand, Carol did not make a determined effort at violating Alice's privacy; Carol did nothing more than open her own mail and read the contents. On the other hand, once she recognizes that she was not the intended recipient, it would be respectful of Alice's privacy to discontinue reading. Even then, Alice may feel that her privacy was violated because she has no way of verifying that Carol did stop reading the letter. Does the burden of privacy fall on the victim or the intruder, and at what point does the victim's perception become a defining characteristic of privacy? I will further distinguish between the two variations in the following chapter, answering the question: does it matter whether Alice and Bob are acquaintances of Carol?

The third example illustrates the problem of intent in violations of privacy while additionally introducing the problem of permanent data collection. Here, what may be construed as good intentions actually might have destructive consequences for privacy, whereas intentions potentially sparked by nosiness may be less harmful. The neighbor with a surveillance camera may have innocent, maybe even admirable, intentions; he creates permanent records that could be called upon at a later date to verify or negate human memories. On the other hand, the neighbor who simply sits on his porch does so with unclear intentions – what motivation could he have for watching the comings and goings of neighbors all day other than curiosity? Yet, this neighbor does nothing but watch public actions – he, unlike the other neighbor, creates no permanent record of what he sees. Does the collection of permanent records introduce a new variable to the question of privacy? I would argue that it does. Whereas the human memory is subject to revision with time, a permanent record is just that – permanent. The man on the porch may see his neighbor's mistress enter a house and think nothing of it, letting go of the memory for the future. A permanent record will not make note of current events, but will be available for future recall no matter what the importance. This distinction introduces a new dilemma into the problem of privacy. Does it matter that the surveillance camera, though permanent, is deployed only to provide additional home security while the neighbor on his porch, despite a passing memory, could potentially have an intent only to pry into your personal life? An issue that must be resolved is at what point intent factors into the classification of an action as an invasion of privacy.

The fourth example touches on the issue of social control with respect to privacy. The most recent ideas about privacy suggest that even peeping Toms present no conflict with privacy so long as their presence is unknown. In this example, the actions of the government are unknown to you, and so by this argument no violation of privacy occurs. Your psyche and "ability to think rationally" are unaffected by these actions, and you successfully move about your daily life without interference. However, the evidence gathered presents a suspicious scenario and suddenly you are found the subject of a police investigation. Regardless of whether you are eventually found guilty or innocent, such a fact may alter your reputation among acquaintances, friends and family. I argue that this kind of data collection, despite its secrecy and inability to affect the current psyche, presents a violation of privacy. A person should be able to move about his daily life, coming and going as he pleases, buying what he chooses, without selective surveillance on the part of a government or place of work because such surveillance may subject him to unfair judgment based on partial facts. The man here does not know about the surveillance at the time, but it still could have a deleterious effect on his life. I will show that in this case, anonymity with respect to those doing the surveillance could protect privacy here.

SO THEN, WHAT IS PRIVACY?

In this chapter I have provided a brief history of privacy, legally and philosophically. Though it is hardly complete in its coverage, I have touched on some important ideas about privacy that will relate to the rest of this work. In particular, I have shown that current ideas are still unclear on how to handle scenarios of privacy in public within a working definition of privacy. The most common ideas about privacy stem in large part from Alan Westin's work, *Privacy and Freedom*, and in particular his notion that privacy is largely control over personal information. The idea that Rachels presented, that privacy is critical to our formation of social relationships, is a strong argument for the classification of privacy as a natural right. This link between social interactions and control and the right to privacy is one that is further extended by Charles Fried and that coincides with the link between privacy and freedom. The last point I want to further focus on are the arguments presented by Robison and Alfino. Robison's points about identity and privacy will resurface in my discussion of anonymity as critical points that link the two. Alfino's argument that privacy involves the ability to think freely will also be important later when I discuss surveillance.

3

ANONYMITY

"The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification…"
~Alan Westin, *Privacy and Freedom*

ANONYMITY

In modern American society the act of shopping for groceries is losing the anonymity it had acquired during the middle of the twentieth century. Long before it became an anonymous experience, grocery shopping took place in small general stores where the customer likely knew the clerk personally. As large cities emerged and chain grocery stores became the norm, it became rare for a customer to personally know the clerk from whom he bought his groceries. The old behavior quickly disappeared. In fact, it is possible that, today, with large grocery stores employing tens of clerks, if any one clerk were to track the purchases of any customer it might be construed as a form of stalking. However, as technology advances, a new mode of purchasing grocery items is emerging.

Today many customers carry with them a discount card that entitles the holder to discounted grocery goods. The catch is that obtaining these cards requires the release of personal information often including one's name and address; if you choose to make purchases via check or credit card some stores will additionally require social security numbers or driver's license numbers.[1] The result is that customers no longer purchase goods entirely anonymously, at least those who use a discount card. Now a list of purchases is tracked with identifiable information, allowing companies to aggregate this data in the creation of a shopper profile. Many stores provide "Privacy Policies" to inform customers of how and to whom information about them will be given,[2] further proof that the linking of identifiable information and purchases is possible. Interestingly, this linking of identity with personal information is obviously not a new idea in the grocery experience, as the general store in its earliest manifestations made anonymity an impossibility.

In recent years, anonymity has become an integral piece of the privacy individuals enjoy in the United States. Our freedom to move about large cities almost entirely unnoticed allows us choices we would not otherwise have. Emerging technologies like the database aggregation used in discount cards continue to threaten what anonymity we now enjoy, a fact which rarely gets the attention it deserves as a driving force behind the loss of privacy experienced at the turn of the twenty-first century. I will show that anonymity can protect privacy and is therefore an aspect of any robust definition of privacy.

ANONYMITY AND IDENTITY

Anonymity is the state of being unidentifiable. In order to evaluate its meaning, it is therefore necessary to understand identity. Identity is generally understood as a

[1] *Privacy Policy: Stop and Shop,* (n.d.), Retrieved April 20, 2003 from http://www.stopandshop.com/card/policy.htm.
[2] Ibid.

representation of an individual. It is defined in the Oxford English Dictionary as "the sameness of a person or thing at all times or in all circumstances; the condition or fact that a person or thing is itself and not something else; individuality, personality."[3] By strict definition then, each person can have only one identity, and to each identity there belongs exactly one person, though in practice people assume false identities. Erving Goffman provided a definition of identity in 1963 that I think is still appropriate: "by personal identity, I have in mind only the first two ideas – positive marks or identity pegs, and the unique combination of life history items that comes to be attached to the individual with the help of these pegs for his identity."[4] Goffman's definition points to a concrete idea, "identity pegs" or "marks," with which to discuss identity. Using concrete examples of identity may help to simplify the very abstract term. Therefore, I want to conceptualize identity as much as possible in concrete terms.

It is often helpful when discussing abstract ideas to note their concrete representations. For example, with respect to citizenship we might refer to the possession of a passport. In the case of identity, there are numerous concrete objects which might represent an identity by serving as a means of recognizing an individual. The most obvious example of a representation of identity is a name - in most Western societies it is a decisive way in which an individual is identified. One's visage could also represent identity, or in some cases an identification number is assigned. In the United States an example of such a number is the Social Security Number; several other countries use mandatory national identification numbers as a form of identification.

Any one of these representations is seemingly useless without one or more of the others. Take the name, for example. In a small enough community each name is unique and therefore only matches to one person. However, in practice the match is made with the use of another form of representation – the visage. A name or number only works as an identifier if it can somehow be linked with the physical being of the person in question. This linking is most often accomplished by a visual image, though today it can also take place through various authentication techniques, biometrics being one of these. Without a linking between a physical body and data, the data is meaningless. An identity could then represented by a visual appearance or a name or series of numbers or even a fingerprint. One other representation of an identity might be the sequence of a person's DNA. In this case, we can imagine moving directly from the DNA sequence to an actual person; unlike the name, a DNA sequence can be directly matched to a physical body much like a visage. In all cases identity is represented by some piece of information: a name, a number, an image, or a sequence of chemicals. Therefore it could be said that anonymity is the lack of such information, or the inability to obtain or recognize this information.

Anonymity is also a relative term. The woman who appears in the televised commercial advertising soup may be anonymous to the vast majority of people who watch the commercial, but to a select few who know her personally she is anything but anonymous.[5] Similarly, I am not anonymous in my small hometown, but if I venture to a different town suddenly I have acquired anonymity with respect to the people I encounter

[3] Oxford English Dictionary, 2nd ed., (1989), "identity."

[4] Erving Goffman, *Stigma: Notes on the Management of Spoiled Identity*, (New York: Simon & Schuster, Inc., 1963), 57.

[5] Example provided by Suzanne Masiello, December 28, 2002.

there. Therefore it is important to discuss anonymity with respect to a person or group of people, as opposed to discussing an absolute classification.

If anonymity is relative, then one cannot have a right to absolute anonymity. This is important because I am claiming that within the "right to privacy" falls an expectation of anonymity, but this expectation is not unqualified. You cannot enter a shopping mall in your hometown and expect that no one will recognize you. Indeed, imagine you lived in California but traveled for a weekend to New York City; you can't claim a right that no one on Fifth Avenue will recognize you, although it is unlikely anyone will. The chances of maintaining anonymity in the second case are much higher than in the first – most of the people you know probably live in California, in order to meet you one would need to make the same trip at the same time that you had. But it is not unlikely that one of many people in your hometown might venture to the central shopping mall on the same day as you. I point this out because I do not mean to assert that we can expect absolute anonymity; in fact there is really no point at which you have any expectation of absolute anonymity. But in today's society there are opportunities to increase the likelihood of maintaining anonymity, and there are times at which you could be said to have a reasonable expectation of anonymity, especially from people whom you have never met before. This reasonable expectation of anonymity, I hold, is critical to what privacy we enjoy today.

A COMPONENT OF PRIVACY

To begin analyzing how anonymity fits into the concept of privacy I will start with those theories that explicitly name anonymity as an integral component. Alan Westin declares anonymity as the third of four "states of privacy," which also include solitude, intimacy and reserve.[6] Westin does not go into great detail in his explanation of why anonymity is included in this list, but he does point out two types of anonymity that are valuable. First Westin describes "anonymous relations" [7] that become unique and important means of uninhibited expression. "In this aspect of anonymity the individual can express himself freely because he knows the stranger will not continue in his life, and that … he is able to exert no authority or restraint over the individual."[8] Jeffrey Rosen, a modern scholar, expanded on this very idea:

> "George Simmel noted … , 'The stranger who moves on,' he observes, 'often receives the most surprising openness – confidences which sometimes have the character of a confessional and which would be carefully withheld from a more closely related person.' This phenomenon of the stranger will be familiar to anyone who has overheard two seatmates thrown together by chance on an airplane or a train loudly sharing intimate disclosures about their most embarrassing secrets. Confessions to strangers are costless, precisely because the social disapproval of strangers can be ignored, unlike the social disapproval of those whom we encounter on a daily basis."[9]

[6] Alan Westin, *Privacy and Freedom*, (New York: The Association of the Bar of the City of New York, 1967), 31.
[7] Ibid, 32.
[8] Ibid, 32.
[9] Jeffrey Rosen, *The Unwanted Gaze: The Destruction of Privacy in America*, (New York: Random House Inc., 2001), 198.

Without explicitly saying it, Rosen is touching on the anonymity that Westin argues is a component of privacy.

Ruth Gavison articulates three components of privacy: anonymity, secrecy and solitude. Gavison describes anonymity as "attention paid to an individual" and relates that a loss of anonymity directly translates to a loss of privacy and may occur in several ways: "Y may follow X, stare at him, listen to him, or observe him in any other way."[10] Despite identifying these three components, anonymity, secrecy and solitude, Gavison opts to work with a complex and imprecise concept of privacy rather than delve into a detailed analysis of what each of those components represents. Her analysis is incomplete and at points faulty. In fact, Gavison says that "being intimate in public is almost a contradiction in terms."[11] This is a conditional statement, and I would argue that intimacy in public is an achievable goal if anonymity is preserved. Indeed a couple in love, perhaps the shining example of people seeking intimacy, may find such closeness in a public realm where they will not be recognized – it is not uncommon to see lovers strolling in a park immersed in their own world. However, famous people, Hollywood stars for example, are known to struggle with finding such intimacy in public, largely because there is a high likelihood such a person will be recognized by someone everywhere. This contrast, I hope, shows a fallacy in Gavison's argument that intimacy in public is unachievable. It also demonstrates a weakness in her argument, illustrating the need to further develop an explicit relationship between anonymity and privacy.

Westin and Gavison are the two scholars who make the most explicit arguments for including anonymity in the scope of privacy, but unfortunately they both do so only superficially. Helen Nissenbaum deals with the issue in a different manner, by discussing "privacy in public." She does an excellent job of explaining why the theories of privacy available have done so little for protecting this form of privacy, but focuses her own argument against data surveillance. Nissenbaum argues that data surveillance destroys one's ability to maintain any privacy in public, but fails to note the impact it has on anonymity and link this impact to a destruction of privacy. In particular, is it possible to have privacy in public without anonymity? I do not believe it is, because if one's actions are public, that is viewable by other people, and identifiable, then those actions cannot be private. I believe her argument would be strengthened by including this concept.

The problem of anonymity must be more adequately dealt with in order to clarify what is meant by privacy. I would like to use my earlier analysis of anonymity and identity to discuss its importance within the context of prominent theories on privacy. One of the most prevalent and indeed most relevant of these theories is the idea of autonomous control of personal information. Anne Branscomb in *Who Owns Information?* argues that personal information should be afforded the same rights as private property.[12] Her work is the most detailed argument for autonomous control over personal information, but the idea also echoes of Westin's work and is similar to the arguments put forth by Robison and Rachels as well. Anonymity is the state of being unidentifiable, when an identity is represented by a visual image of the individual in question or a name or number that is associated with that person. In order to discuss

[10] Ruth Gavison, "Privacy and the Limits of Law," *Philosophical Dimensions of Privacy: An Anthology*. Ed. Ferdinand Schoeman, (Cambridge: Cambridge University Press, 1984), 353-54.

[11] Ibid, 362.

[12] Anne Branscomb, *Who Owns Information?*, (New York: Basic Books, 1994), 181.

anonymity as a form of control over personal information, it is necessary to reconcile whether personal information and any of these representations of identity are one in the same. I argue that they are.

Your name is your personal information - you choose to whom and under what circumstances you will give it out. You also choose, although arguably through a subconscious decision, which visual image of yourself will be made available to the public eye. It may seem that in every case in every culture, presenting one's visual appearance happens by default. However, each individual chooses which variety of his own appearance will be seen by which groups of people, and many individuals in today's society go to great length to change their visual appearance for certain circumstances. A woman attending a formal dinner is unlikely to present the same visual image of herself that she might when she is relaxing at home on a Saturday afternoon. She therefore controls her visual appearance, as she would any personal information. Few would question the classification of DNA as personal information because of its immeasurable power. With a person's DNA, it is presumably possible to ascertain details about medical conditions, information generally considered personal and private. If we consider personal all of these pieces of information – the image, DNA, the name, ID numbers – then we must consider the identity itself personal information. If we do, then anonymity is just another form of privacy – control over personal information, in this case one's identity.

James Rachels links this control over information with a more fundamental piece of existence, "our ability to create and maintain different sorts of social relationships with different people."[13] Charles Fried, in a related argument, holds that privacy is "necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust."[14] In this sense privacy is fundamentally linked to our ability to lead normal lives, to interact with our family and loved ones. Control of identity, the ability to remain anonymous, is a critical facet of this type of privacy. Fried focuses his attentions on the way in which privacy affects our interactions with people we know – how intimacy might be affected if individuals fear invasions of privacy. I think the more important point he illustrates is an unintended side-effect of his theory. Fried says, for example, that

> "If we thought that our every word and deed were public, fear of disapproval or more tangible retaliation might keep us from doing or saying things which we would do or say if we could be sure of keeping them to ourselves or within a circle of those who we know approve or tolerate our tastes."[15]

A key point he assumes in making this statement is that by making one's actions public, these actions and words are somehow linked to one's identity. If in fact such a link never exists, if the person's anonymity is preserved, then the above statement would no longer hold – we would not fear social disproval or intolerance because such judgments would be ephemeral. For instance, if an individual decides one day to dress up as a gorilla and

[13] James Rachels "Why Privacy is Important," *Privacy and Public Affairs Quarterly* 4 no. 4 (Summer 1975), 326.

[14] Charles Fried, "Privacy: A Moral Analysis," *Philosophical Dimensions of Privacy*, Ed. Ferdinand Schoeman, (Cambridge: Cambridge University Press, 1984), 205.

[15] Ibid, 217.

wander a public park, witnesses may judge such a person to be foolish or maybe insane. These judgments, however, would be limited to the moments in which the anonymous gorilla's path crossed with any particular person. In essence, they would be meaningless. On the other hand, if the man removed his mask for a moment and was recognized by a colleague, these judgments might remain with the costumed man for days or weeks to come; at best he faces ridicule from his colleagues, at worst he may lose credibility in his work, never able to live down the label of "lunatic." Fried assumes identity as a piece of information that is always attainable, as something over which we have no control, when in fact this is not always the case.

A more recent approach to privacy clearly illustrates the link between identity and personal information. Wade Robison shows the ways in which data surveillance in the 1990's have taken from us control over our personal information, thereby reducing our identities to meaningless objects. His focus is on identity theft, of which he comments:

> "When we are treated like packets of information, to be appropriated, we have lost control over who we are – how we are perceived in society. To have others appropriate us is to fail to respect us and so fail to respect our choices about how we would like to present ourselves to the world." [16]

Robison is able to show the link between representations of identity and our sense of self, "control over who we are."[17] His discussion is set in a context of data surveillance, an environment in which information about one's residence, credit, business is collected into aggregate databases. Robison's argument is close to the one I hope to make: that control over one's identity is critical to privacy. However, his focus is on protection of identity, almost as though it is a piece of property. I argue that control over representations of identity translates to an ability to remain anonymous in various situations of daily life, and that this ability is an essential component of privacy.

APPLYING ANONYMITY TO EARLIER SCENARIOS

It will be helpful to return now to the scenarios I posed in the previous chapter. Without resolving the particular questions I posed earlier about privacy in general, I would like to articulate how identity and anonymity dramatically change these scenarios in the context of privacy. Anonymity is a critical component of privacy in that it serves as a common means of protecting our privacy, and attention to anonymity will have an effect on these scenarios.

Returning to the public park scenario, recall that a likely argument would be that, at least in the first two cases – the stretching jogger and the jogger hiding in the bushes – no right to privacy has been violated. This is either by Thomson's conclusion that such a right would not be violated because of the public location or by Alfino's argument that the subjects of any eavesdropping are unaware that they are being overheard. In the third case, Alfino might conclude that such overt observation constitutes an invasion of privacy, while many other theories would hold that there can be no expectation of privacy. I believe changing the example slightly to include the variant of identity will help clarify the issue. In any of the three cases, if the two subjects are entirely

[16] Wade Robison, "Privacy and Personal Identity," *Ethics & Behavior* (Volume 7 No. 3 1997) 205.
[17] Ibid, 205.

anonymous to the eavesdropper, it might be argued that no loss of privacy has occurred. Perhaps the jogger overhears one friend "coming out" to another, admitting his or her homosexual preferences. If these two people are anonymous to the eavesdropper this information is interesting but useless, in fact meaningless. However, if the eavesdropper recognizes one or both of the individuals in question, particularly if he recognizes the one making a confession, the issue of privacy becomes more complicated.

By choosing a public space one risks being overheard, but if the burden of privacy is on the invader then perhaps the eavesdropper ought to avoid overhearing details of an obviously private conversation between two acquaintances. Even if we conclude the burden falls on the speaker, does he have an expectation of anonymity that, unless he finds to be false through recognition of surrounding people, ought to protect the privacy of the conversation? Likely the answer is no if he is a famous actor or politician or the like, but an average citizen might indeed expect such anonymity, and therefore such protection. Nevertheless freedom from identification will in fact protect the content of the information exchanged from association with either individual. We could imagine the jogger returning home and recounting the juicy conversation to friends, but unless he could say definitively who was involved, the information is harmless. No privacy has been invaded.

When I dealt with Alice, Bob and Carol earlier I worked under the assumption that Carol knew either Alice or Bob, if not both. But let us imagine that Carol opens the letter and upon seeing the address "Dear Bob" realizes she does not know anyone named Bob. Perhaps she has just moved into a new apartment, previously occupied by Bob, a man whom she never met. Recall that if Carol reads the letter despite her awareness that it was intended for her acquaintance Bob, she neglected Alice and Bob's privacy. I argue that if she does not personally know Alice and Bob no privacy is in question: their anonymity with respect to Carol protects their privacy in such a circumstance. Even if Alice realizes that Bob never received the letter and suspects its interception by an accidental recipient, she would likely wonder who might have received the letter, but would more feel disappointment at the loss of her intended communication with Bob. Alice would be unlikely to stop using the postal system as a means of communication or to alter her communication of private emotions to Bob. Thomson might hold that a right to privacy has been forfeited in this circumstance since Alice did send the letter mistakenly, but I argue that privacy could be protected by anonymity.

Modern internet chat-rooms present a similar example, and people's behavior within these rooms illustrates the protection they feel as a result of anonymous communications. If you have spent time in these chat-rooms, you know that people discuss detailed parts of their lives with multiple anonymous users. You may also have experienced the formation of "private" conversations in these rooms, where two or maybe three people become the sole participants in a string of the conversation while others simply "lurk" and read the information exchanged. People have proven willing to discuss intimate details of their lives in the context of these rooms, and I argue this is largely the result of their anonymity from other users. I might be able to say that "johnny0987" discussed in detail the different recreational drugs he chooses to use, but it would be difficult for me to pin down exactly which human body is associated with "johnny0987," and even if it is possible, "johnny0987' probably is working under the belief that it is unlikely and his anonymity with respect to myself and other members of the chat-room will be preserved. If the room were populated with people who recognized "johnny0987" as their classmate, he might be less likely to divulge the details of his drug use.

With respect to the third example it will be helpful to envision the impact this type of observation has on the occupant of the home versus the impact on a visitor. When discussing the privacy problems introduced by this example I focused on the problem of permanent records, so I will here work within that framework. Let me extend the example some to further illustrate the distinction between occupant and visitor. Perhaps a visitor approaches the house and waits outside for the occupant to join him on the porch. The two have an extensive discussion during which voices are raised and there are clear indications of an angry conflict between the two individuals. Whether the argument is seen by the video camera or the neighbor on his porch is probably of little matter to the occupant – in either case he will be recognized by his neighbors and identified with the argument. And similarly, the problem of permanent records becomes insignificant to the visitor – the neighbor's ability to link him with the argument is limited by his ability to identify the visitor. If the visitor remains equally anonymous to both neighbors, neither is able to invade his privacy. In creating permanent recordings, however, the neighbor to the right creates a potential for invading the privacy of the visitor should he ever come to identify this person. Still, at the time of the argument, it is possible to violate the occupant's privacy and not the visitor's because of anonymity. In this way, the inability to identify the visitor protects his privacy.

The example of the uncle and niece is among the most relevant to problems our society faces today and will lead me into a discussion of surveillance in the next chapter. First, let me illustrate how anonymity in data surveillance could protect privacy in this example. I have argued earlier that while arguments like Alfino's might suggest this scenario does not initially present a threat to privacy, it does indeed violate an individual's ability to come and go as he pleases without concern for repercussions of everyday actions. If the initial surveillance conducted were done with attention to the individual's anonymity, the end result of a police charge would likely not be possible. To clarify let me return to the grocery store example I presented at the start of this chapter. Recall the example of grocery store discount cards. If these customers are anonymous with respect to their purchases, that is to say, if it is impossible to move from a list of purchases to an individual or vice versa, no privacy has been violated. In fact, this type of monitoring is not very different from taking inventory in the store. If, however, it is possible to link purchases to an individual, this might result in situations in which individuals are labeled "suspicious" based on what might be interpreted as irregular or deviant purchases over time. Even though a store may claim to never do such labeling, it is possible if the information falls into the wrong hands, and therefore detrimental consequences like those in the fourth example are possible, resulting in a violation of privacy.

Control over one's identity, or lack thereof, serves to clarify the issues present in these examples dealing with privacy. The reason it provides clarity is that anonymity is indeed an important piece of privacy. Westin pointed out that:

> "every individual lives behind a mask in this manner…indicating both the conscious and expressive presentation of the self to a social audience. If this mask is torn off and the individual's real self bared to a world in which everyone

> else still wears his mask and believes in masked performances, the individual can be seared by the hot light of selective, forced exposure."[18]

Generally we talk about privacy in our actions, words, thoughts, our everyday doings. It is common to argue that if those private doings are made known to a person, we have lost privacy. However if those doings become known without an associated identity, then privacy cannot be infringed upon – whose privacy is at stake? That of the unknown identity?

Anonymity is then a component of privacy. I have defined anonymity as a state of being unidentifiable, which, as I have pointed out, requires control over one's identity. The question then is how we define the personal information that constitutes an identity. In the next chapter I will present an overview of biometrics. These biometrics, I believe, are representations of identity just as a name or number is. Goffman, in his description of identity pegs, provides the following thought:

> "As suggested, the choice of mark is itself quite standard: unchanging biological attributes such as handwriting or photographically attested appearance; permanently recordable items such as birth certificate, name, and serial number. Recently, through the use of computer analysis, experimental progress has been made in using speech and handwriting qualities as identity pegs, thus exploiting a minor expressive feature of behavior much as the specialists do in 'authenticating' paintings."[19]

The attributes Goffman refers to in 1963 are now referred to as biometrics, and as Goffman argues are as strong a representation of personal identity, or "identity pegs," as any.

[18] Westin, 33.
[19] Goffman, 57.

4

BIOMETRICS

“Any high-integrity identifier represents a threat to civil liberties, because it represents the basis for a ubiquitous identification scheme, and such a scheme provides enormous power over the populace. All human behavior would become transparent to the State, and the scope for non-conformism and dissent would be muted to the point envisaged by the anti-utopian novelists.”

~Roger Clarke

BIOMETRICS

Biometrics, defined from its Greek roots "bio" and "metric," mean literally to measure life. Rather than measuring amount of life however, biometrics measure the identity of living beings. Generally, biometrics are measurements of information that represents a unique physical or behavioral characteristic of an individual. In my previous discussion of anonymity I referred to concrete representations of identity like the name or ID number or visage. Biometrics measure aspects of a person's body that are known to be unique, or nearly unique, and use that measurement for identification purposes. If we agree that an identity can be represented by information unique to that identity, it follows naturally that, for example, a fingerprint, which is known to be unique to each person, is also a representation of identity. Biometrics, I would argue, are more accurate representations of identity than the name because they provide a direct, and often absolutely unique, link between an individual body and an identity. In this discussion I will provide a technical overview of emerging tools that will be used to measure identity in novel ways.

Technically speaking, biometrics[1] are understood to be the "automated use of physiological or behavioral characteristics to determine or verify identity."[2] The incorporation of the word "automated" is critical to understanding the goal of this technology. While the technology recognizes the same characteristics that humans rely on to identify people, the use of biometrics implies training a machine to automatically process and identify these characteristics. In this way, biometrics serve to mechanize the determination of identity.

The type of characteristic measured classifies a biometric as physiological or behavioral. Physiological biometrics are "based on direct measurements of the human body,"[3] while behavioral are those biometrics "based on measurements and data derived from an action."[4] Examples of physiological biometrics are the fingerprint, iris, face and hand. Within this classification, some scientists further distinguish between genetic and phenotypic measurements. Facial structure is determined by genetic patterns, while iris patterns, though based on genes, develop distinctive characteristics during early embryonic development.[5] Behavioral biometrics include gait, keystroke, voice and

[1] It is important to note that the plural biometrics refers to the whole of biometric technologies, while the single biometric can refer to either the physical trait being measured, or the technology used to measure it, most often the former.
[2] Samir Nanavati, Michael Thieme and Raj Nanavati, *Biometrics: Identity Verification in a Networked World* (New York: John Wiley & Sons, Inc., 2002), 9.
[3] Ibid, 10.
[4] Ibid, 10.
[5] John Woodward Jr., Nicholas Orlans and Peter Higgins, *Biometrics: Identity Assurance in the Information Age* (Berkeley: McGraw-Hill Companies, 2003), 28-9.

signature. It is theoretically possible to relearn and consciously alter this traits, although many adults struggle with doing so because the behavior has become so ingrained.[6]

A second classification is made based on the intended use of the biometric technology. As defined, biometrics are used both to verify and determine identity. When placing a biometric in context, the distinction between individual and identity becomes critical. An individual could claim multiple identities, one or more of which may indeed be false. Biometrics measure an identity, not an individual; therefore, a biometric match is only as good as the validity of the enrollment identity, which is the identity claimed at enrollment. With this in mind, accurate biometrics can be used to determine the identity of the user, or to verify his identity.[7] In determination, the user does not need to claim an identity, it will be determined by the system. In other cases, biometrics will be used simply to verify that the claimed identity of the user matches his physical or behavioral representation.

I will now provide a technical overview of several biometric technologies: fingerprint, face, iris, voice, gait and DNA. I have chosen to start with a discussion of the fingerprint as a means of identification because it serves as one of the oldest and most widely recognized examples of a biometric. The following discussions focus on biometrics that have a potential of being deployed in surveillance applications. This overview would not be complete without touching on the potential use of DNA as an identification technique, although it has yet to be fully realized as such. Although today it may seem technologically impossible to use DNA as a real-time identifier, it is perhaps the most absolute form of identification and no doubt will present itself as a common biometric in time. Before describing the specific technologies, I will present considerations that need to be taken into account when evaluating the success of biometrics or the appropriateness of their use.

MEASURING APPROPRIATENESS & EFFECTIVENESS

First we must evaluate why biometrics are useful, as well as the considerations we must make when employing the technology. Authenticating identity is a task that occurs several times a day in twenty-first century America. We rely on authentication to use ATMs, to gain access to our computer, or to board mass transportation. These authentication techniques most often rely on alphanumeric Personal Identification Numbers and passwords or identification cards, common representations of identity today. The unfortunate consequence of these means of authentication is that it is always possible for someone other than you to gain access. John Doe may have stolen your identification card and made himself up to look like your picture, or he may have guessed a password or simply found your PIN written on a scrap of paper in the wallet he picked out of your pocket.

Biometrics theoretically eliminate this consequence by relying on identifiable characteristics that are distinct between individuals and difficult to replicate. Mr. Doe may die his hair red to match the image on a stolen ID card, but changing his bone structure to match a biometric face template would prove far more difficult. In addition to the added security, biometrics enhance convenience. Rather than remembering an

[6] Woodward Jr., Orlans and Higgins, 29.

[7] The term “user” will refer to the individual to which the biometric measurement is applied, not the entity in control of the biometric system.

elusive password or carrying around a plastic card, an individual only needs to present his physical being to gain access. However, this convenience carries with it the possibility for biometrics to fail badly. If Mr. Doe is able to successfully steal a biometric template and subsequently match his own identity, he has potentially gained access to the victim's home, bank account, place of work and car all at once. As Bruce Schneier points out, "we don't use the same password on two systems, but biometrics are globally common. You can't easily change which fingerprint you use to login to which system."[8] A possible way of averting such disaster would involve using multiple authentication techniques in unison: several biometrics, a single biometric and a password, and so on.

There are several terms to define before evaluating the effectiveness of any biometric. First, I will discuss the issues around *usability*: how easy a human finds the technology to use. Then I will discuss *physical* versus *logical* access, and finally the issue of *liveness*.

Usability indicates whether or not a biometric is easy for an individual to use. Several biometrics have proven easier to use than others, thus enhancing convenience. For example, current fingerprint recognition systems seem easier to use than iris scan systems, which in turn are immensely easier to use, and more accepted, than retina scan systems. Retina scans are considered among the most accurate biometrics available, but because of the necessity for extreme proximity, about 2 or 3 inches between the eye and the acquisition device, they have not been well accepted by users. [9] Eye biometrics are generally considered relatively invasive, which leads to decreased usability, although specifically developed iris scanning systems can operate at distances of several meters.[10] A biometric such as the fingerprint, however, is non-invasive and easy to use for most people.

Most often, biometrics are used to grant access, either physical or logical. *Logical* access involves access to information, generally files or servers. *Physical* access involves access to buildings or restricted areas. Protecting physical access, or access to secured locations, has often been accomplished through the use of physical keys or ID cards. Biometrics like hand geometry and iris scans are quickly overtaking the market, providing protection against lost keys and picked locks. Information assurance depends on the authentication of logical access, the control of who gains access to information on computers and networks. The alphanumeric passwords have dominated this market for years, but the overhead cost of forgotten passwords has become a burden for strapped Information Technology budgets. In the place of the password companies are turning to fingerprints and voice recognition to facilitate logins to networked computers.

Liveness is an indication of whether the biometric sample belongs to a live human or not. In the context of biometrics, a technology's ability to detect *liveness* indicates its ability to determine whether the specimen being examined is part of a complete, live human being, or whether it is a dead or removed body part, or in some cases a manufactured look-alike. As I will discuss later, the fingerprint systems have proven to be susceptible to manufactured fingers; the fingerprint is a weak biometric for liveness testing. A better biometric has qualities inherent to the trait that allow liveness testing to

[8] Bruce Schneier, "Biometrics: Uses and Abuses," *Communications of the ACM* Vol 42, N8. August 1999, 2.

[9] Woodward Jr., Orlans and Higgins, 95-96.

[10] Ibid, 91.

be easily integrated. For example, voice recognition inherently tests for a spoken voice, which it assumes to be from a live person, and often challenge-response systems can be used to verify this fact. This biometric is still a weaker test for liveness than others, such as those that rely on thermal scans or behavioral characteristics, because the voice can be recorded and replayed as if it were live.[11] Thermal IR face scans or gait are two examples of biometrics that are very hard to imitate or manufacture.

In evaluating any biometric system the primary tradeoff between security and convenience must be considered. Identifying the primary purpose determines whether security or convenience is of more importance. In a system built primarily to keep people out, a CEO's laptop computer for example, we care more that only the CEO can gain access than the ease of his gaining access. But in a system such as a large corporate building, we may care more that the 1,000 employees are able to easily gain access on the first or second try than whether an unauthorized person can gain access. Here the sensitivity of the secured material also becomes important. On the CEO's laptop, one assumes there is a great deal of sensitive corporate material; it could be catastrophic if even one unauthorized person gains access. However, one assumes that a person who gains unauthorized access to the building will be unable to acquire very sensitive information without also gaining access to the necessary servers and client computers. In this scenario then, it might be that physical access to the building is less sensitive than logical access to corporate information, but we could imagine situations in which the reverse were true.

The number of enrolled users is critical to the evaluation of a system. When a user claims an identity, biometrics are discussed in terms of 1:1 verification. If, however, the user is located in a database of enrolled identities, the biometric is discussed in terms of 1:N identification. The size of N impacts the accuracy of the system: as is to be expected, the larger the database, the lower the accuracy. Therefore we tend to think that biometrics working on a 1:N system of a substantial size will be less effective.

The *reliability* of a biometric over time makes it more effective. Irises and fingerprints, for example, are known to be consistent throughout a person's lifetime, barring severe injury. One's face may retain the same bone structure, but with fluctuations in weight and wrinkles brought on by aging may undergo physical change. Reliability is not only affected by natural changes, but the ease of changing biometric characteristics. Putting on a fake mustache or speaking in a high pitch is far easier than effecting a change in the rings of your fingerprint or iris. The ability of environmental changes to effect the outcome of a biometric decision is also important to take into account. Facial recognition is very susceptible to changes in lighting, while an iris scan is fairly immune to nearly all environmental changes.

Accuracy is the final measurement of effectiveness. The accuracy of any given biometric is dependent on the algorithm used, as well as the environmental variables present. With the exception of the iris, there are several algorithms to recognize any biometric, and the details of many of these are corporate secrets. There is a worldwide patent on John Daugman's iris recognition algorithm out of Cambridge University which has proved remarkably accurate. When evaluating accuracy, False Accept Rates (FAR) and False Reject Rates (FRR) are the most commonly used measurements. For high

[11] Ibid, 144.

security systems, the FAR is most important; again, we care most that the select few gain access and no one else. In systems that emphasize convenience, the FRR is generally equally important as the FAR; we do not want John Doe to stand in front of a camera for minutes on end while the system continues to incorrectly reject him. It is also important to know the Failure to Enroll Rate (FTE) for a given biometric. A high FTE can become a cost in systems that serve large numbers of people. The biometric serves little purpose if it refuses to enroll a significant percentage of the target population.

Among the different biometrics, iris recognition and retina recognition are generally considered the most accurate. Fingerprint recognition, depending on the technology, is also respected as an accurate tool. Facial recognition is considered among the least accurate biometric, not necessarily because of the algorithms but because of the environmental variables that lead to false accepts and false rejects.

FINGERPRINT RECOGNITION

Fingerprint recognition is the oldest biometric on the market today. Humans have known that the fingerprint is a unique characteristic for several hundred years. The Chinese were known to use fingerprints in the 14th century as a means of identifying their babies, just as U.S. hospitals do today. Palms and feet were stamped with ink and the patterns were used to create a permanent identification record.[12] Mark Twain's 1893 story *Pudd'nhead Wilson* gives an account of the differences in fingerprints not only between people, but between identical twins and between individual fingerprints.[13] For years criminal investigators used this characteristic to identify criminals and prove guilt beyond reasonable doubt. In the 1970's, the federal government began research on technology that would automatically identify individuals based on fingerprints.[14] From this early work came the Automated Fingerprint Identification System (AFIS).[15] AFIS systems perform identification over a database of fingerprint images, not just biometric templates. Although AFIS has been around for thirty years, smaller more adaptable technologies used to verify identity based on fingerprints have become commonplace in the last ten years. It is these technologies that I will examine in detail here.

There are several reasons that fingerprint recognition has emerged as such a successful biometric over the past twenty years. First, the fingerprint is among the most stable and unique physical identifiers of an individual. The physical characteristics of the fingerprint are determined by the lowest layer of the epidermis, and are distinct between fingers. The only way to effectively "change" one's fingerprint is to remove all the skin on your fingers and replace it with skin from elsewhere on the body; this technique was used by gangsters in the 1930's, but rarely since then.[16] Although there is some evidence that use throughout a lifetime may reduce the quality of images that can be acquired, the patterns are stable throughout an individual's life. The technology is also independent of typical environment changes. Although inclement weather would make acquisition

[12] *Individual Biometrics – Fingerprint*. (n.d.) Retrieved April 18, 2003, from http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html.

[13] Simson Garfinkel, *Database Nation: The Death of Privacy in the 21st Century* (California: O'Reilly & Associates, Inc., 2000), 41.

[14] Nanavati, Thieme and Nanavati, 119.

[15] Ibid, 59.

[16] Garfinkel, 42.

difficult, moderate lighting and temperature variations have an insignificant effect on the acquisition of the print. Additionally, because the print is unique among fingers, the option to enroll multiple fingers for the same individual increases the accuracy of the recognition.

Current fingerprint recognition involves hardware to acquire the image and software to process the image for comparison. Many of the acquisition devices in use today are small and are integrated into larger systems. Some are peripheral devices that attach to a personal computer; many times acquisition devices are integrated into laptops or keyboards to provide logical access to a machine, and even handheld devices are beginning to integrate these devices into the hardware to provide logical access.[17]

Fingerprint technology rests on the recognition of the various ridges and valleys on the pad of the finger. Traditional fingerprinting involves comparing finger's ink prints which highlight the ridges of the fingerprint. The length of the ridges, the location of their endings, the location where a ridge divides into two new ridges, and any other irregularities are all characteristics humans look at when comparing two fingerprints.[18] These same characteristics are looked at by fingerprint recognition technology in the creation of a set of data points referred to as *minutiae*. There is a variety of algorithms available commercially the details of which are corporate secrets, and each proprietary algorithm creates a different set of minutiae for comparison.

There are three main methods used to acquire the image: optical, silicon and ultrasound. Optical technology is most commonly used in fingerprint image acquisition. It is an inexpensive and reliable technology that has been established over time.[19] The drawback to using optical acquisition devices is the relative inability to distinguish between latent and live prints, as shown by the research of Matsumoto, Matsumoto, Yamada and Hoshino at Yokohama National University in Japan. This group of scientists set out to determine if fingerprint recognition systems were vulnerable to attack by artificial fingers. In particular, they constructed gelatin fingers out of molds of actual fingerprint images. Their study found that 67% of optical and capacitive systems accepted the gelatin prints as live, demonstrating a real weakness in the systems.[20]

Silicon technology was introduced in 1998 and is exciting due to its potential for use in small peripheral devices while still providing very good image quality. Because it is such a new technology, however, its accuracy and reliability remain largely untested.[21] Silicon technology will be ideal for logical access because of its size, but is unlikely to be used in place of larger but cheaper systems in physical access.

Ultrasound acquisition devices are rarely used in simple fingerprint recognition systems because the technology requires a large physical device and is relatively expensive. These devices acquire very accurate images because the ultrasound virtually ignores any dirt or sweat on the finger, whereas optical and silicon both are influenced by

[17] Nanavati, Thieme and Nanavati, 48.

[18] Ibid, 51-52.

[19] Ibid, 54.

[20] Tsutomu Matsumoto, Hiroyuki Matsumoto, Koji Yamad and Satoshi Hoshino, "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems," in *The Proceedings of SPIE (The International Society for Optical Engineering) Vol#4677: Optical Security and Counterfeit Deterrence Techniques IV held in San Jose, CA 24-25 January 2002.*, 11.

[21] Nanavati, Thieme and Nanavati, 55.

the presence of these particles. Ultrasound technology is used in AFIS systems, but is ineffective hardware for access control because of its large size and cost.[22]

Processing fingerprint images requires three steps: eliminating gray areas, locating distinctive characteristics, and creating a template. The proprietary algorithms then locate interesting minutiae, and create the template. Template creation is proprietary as well; each vendor decides how to map the minutiae out into a template and how to decide if a particular minutiae is the result of scars, sweat or other external factors. The template then must be matched against a database of identified templates. The correlation between any two templates is never determined using a bit by bit comparison, but is a piece of the vendor's proprietary secret. Thresholds for matching are determined by the goal of the recognition. If the goal is 1:1 verification and providing the utmost security, the threshold must be lower than when convenience and 1:N verification are the desired outcomes.[23]

Fingerprint verification has already permeated our culture as an access control measure. In many cases, fingerprints are being used to provide increased security of financial accounts. The U.S. company Identix Inc. created a solution utilizing fingerprint scans for the Mexican bank, Groupo Financiero Banorte, to increase security and enhance convenience. The solution involves a smart card, which holds a fingerprint template. The bank wanted to allow employees to cash paychecks easily; the card acts as a timekeeper and a cash-dispenser.[24]

The flexibility of the fingerprint as a biometric is shown by its successful deployments not only for increased security, but also for increased convenience. Elementary schools have begun to use the technology to provided added confidentiality of information for the students. In Pennsylvania, lunch purchases are tracked in virtual accounts by way of fingerprint recognition. "The scanners make steal-able lunch money, lose-able swipe cards and the stigma of being known as the free-lunch kid things of the past."[25] Students receiving federal funds for lunch are thus able to remain anonymous; the source of their funds is only known in the virtual account, not to other students waiting in line for lunch. Additionally, school systems are using the technology as a log-in device to school computers.[26] Schools in Stockholm have begun using this technology instead of a password for elementary students. Advocates say it is an improvement over traditional log-ins because small schoolchildren are apt to forget a password, prompting perpetual password reset cycles.

FACE RECOGNITION

Computers can be trained to recognize individual faces in the same way that they have been trained to distinguish fingerprints. Face recognition got its start during the

[22] Ibid, 55.

[23] Ibid, 52-53.

[24] *Identix Delivers ATM/POS Biometric Fingerprint Scanning Application to Reynosa, Mexico*. (n.d.) Referenced April 18, 2003, from http://www.netlinkaccess.com/wsimages/biometric.pdf.

[25] Sascha Segan, "Finger Food: Fingerprint Scans Replace Lunch Money in Pennsylvania," *ABCNews.com*, 18 January 2001.

[26] Ben Miller, "Applications of Biometric Technologies" at the *Biometric Consortium Conference held in Washington D.C. on 23-25 September 2002.*

1980's when Kohonen developed the Eigenfaces approach to facial recognition.[27] The approach creates a template of the face by "approximating the eigenvectors of the face image's auto correlation matrix."[28] Facial recognition is powerful when used in 1:N identification, although it is rarely, if at all, used in 1:1 verification. Situations that call for 1:1 verification often involve access control, and there are more accurate biometrics available for this need. Facial recognition is important for its ability to scan people from a distance. It is noninvasive, which means the user can be entirely uninvolved in the identification process.

Facial recognition is a powerful biometric because it leverages already existing technologies. The technology can be used on static photographs or in video feeds; in either case existing camera equipment is used as a part of the overall system. It is one of the few biometrics that can theoretically operate without any cooperation on the part of the users, neither at enrollment nor at identification.

A machine's ability to successfully recognize a human face depends first and foremost on clear and accurate imagery. This is true for humans, too; we cannot recognize people if we cannot clearly see the characteristics of their face. Therefore, facial recognition technology relies very heavily on consistent and accurate image acquisition. Ideally, a high resolution camera directly facing the user is needed. If the user will not be facing the camera at identification, then multiple angles of the face must be enrolled.

The introduction of environmental and behavioral variables complicates the acquisition of clear images and has thus far restricted the growth of the technology. The user currently needs to be an appropriate distance from the camera to ensure adequate facial size and resolution. Lighting must be consistent enough to reduce variability in the shadowing of facial structures. Improper lighting can also affect the recognition of darker or lighter skinned individuals. Behavioral changes on the part of the user present an additional complication to the problem of recognizing faces; the inconsistent presence of a hat, glasses or facial hair for example completely changes the facial characteristics the computer will be able to recognize.

The most difficult problem yet to be solved is the translation between a three-dimensional image and a two-dimensional image. The computational complexity of this problem has limited the ability of recognition systems to be deployed successfully. There are six degrees of freedom in the human head; the neck allows for up/down motion, left/right motion, and a roll motion when an ear is tipped toward the shoulder. Because of the number of degrees of freedom, there are an infinite number of two-dimensional images that correspond to one three-dimensional head. This presents a problem when two very different images of the same individual are being compared: how does the computer know if each is one of the infinite possible associations of the other? In March of this year two Israeli twins constructed a possible solution to this problem. Their technology "scans and maps the human face as a three-dimensional surface, providing a far more

[27] Alex Pentland and Choudhury Tanzeen, "Personalizing Smart Environments: Face Recognition for Human Interaction" (Cambridge, MA: The Media Laboratory, MIT) January 21, 2000. Retrieved April 18, 2003 from http://vismod.www.media.mit.edu/tech-reports/TR-516/ieee_computer.html.
[28] Ibid.

accurate references for identifying a person than current systems."[29] This system scans the face with light patterns and then measures distances between set locations on the face. The data is stored in a 3D image as a series of straight lines that represent these distances.[30] However, most solutions on the market circumvent the translation problem by establishing limitations on their systems. Most often the user is required to stand facing a camera, in which case the system is useful for physical access control. Once the dimensional translation problem is solved, facial recognition will be powerful beyond just access control.

After an acceptable image is obtained, the first problem faced by the computer is the location of the face within the image. The solution is easiest if all images acquired are of a standard format, but not all systems allow for this. If the system is deployed on video feeds, for example, locating the face within the image can be a difficult problem. Face detection is a pattern-recognition problem; therefore many of the appropriate solutions are based on general pattern recognition approaches. A common solution is to apply an algorithm based on neural nets. One such algorithm proposed by a group at Carnegie Mellon University trained a system to detect faces by looking for the mouth and eyes.[31] The neural net is trained on images in which the eyes and mouth have been manually detected, and learns to detect similar shapes within a small square of pixels. Other approaches remove a consistent background from the image and find the borders of the face, look for clustered areas of skin-colored pixels, or even look for the simultaneous motion of two eyes blinking.[32]

The distinctive characteristics the computer uses to evaluate faces are perhaps not what a human would expect given our own method of facial identification. The bones above the eye sockets, the cheekbones, the area to either side of the mouth, the shape of the nose and the position of these features relative to each other are characteristics often used in identification systems because they are least likely to change over time.

Unlike the fingerprint recognition systems that use a single image of the print to verify identity and fail after a given number of attempts, facial identification systems are time dependent. Over a set amount of time the system takes several images of the face and will fail after the time has passed. Many of these systems do not return a match or no-match response, but instead return a list of possible matches. In this case, a human is required to intervene to sort through the given possibilities.

Several processing algorithms have been developed for creating and matching templates of the face. Among the best recognized algorithms are the Eigenface method, developed at MIT, the Local Feature Analysis (LFA) method developed by Visionics Inc. (now Identix Inc.), and the use of neural networks. LFA is probably the most widely used of these three approaches.[33] Visionics claims that their FaceIT product, which uses LFA, is independent of lighting variation, skin color, and even the presence of glasses, or

[29] *3-D Face Scan Distinguishes Twins*, March 10, 2003, 1, Retrieved April 18, 2003 at http://www.wired.com/news/conflict/0,2100,57984,00.html

[30] Ibid, 1.

[31] Henry Rowley, Shumeet Baluja and Takeo Kanade, "Human Face Detection in Visual Scenes," *CMU-CS-95-158R* (November 1995).

[32] *Face Detection Home Page: Techniques*, (n.d.) Retrieved April 18, 2003 from http://home.t-online.de/home/Robert.Frischholz/facedetection/techniques.htm

[33] Nanavati, Thieme and Nanavati, 70.

lack thereof.[34] LFA incorporates features which are described by Visionics as an "irreducible set of building blocks"[35] and uses the type and relationship of these features to distinguish between individuals.

Eigenfaces, also known as Principle Component Analysis (PCA), is the foundation for many facial recognition approaches, including LFA. The Eigenfaces are model faces that each have distinctive characteristics, and are then used in combination to recreate the characteristics of an individual.[36]

Neural networks can be used in facial recognition in addition to detection, but work best when a set of distinctive characteristics can be pulled aside as the "most" distinctive for a given set of individuals. The system then uses the subset as its means of comparison.[37] The learning takes place when false non-matches or matches occur; when in error, the system reassigns weights to given features and in this way stays on top of the "most effective"[38] set of features.

England was the first country to install face recognition in close-circuit television (CCTV) surveillance systems, and has done so in many towns. The borough of Newham, London became the first such town in 1998 when it installed the Mandrake face recognition system, designed by Software Systems International, into its CCTV system.[39] This system searches for convicted criminals on the streets of Newham in an effort to prevent crime. Crime in Newham dropped sixty percent after the installation of just one camera equipped with facial recognition, attesting not to the technology's accuracy but to its deterrent effect.[40] Similar systems have been since been launched in the United States, notably in a small town near Tampa, Florida. Ybor City was the first city in the U.S. to install facial recognition for public surveillance, but was followed in November, 2001 by Virginia Beach.[41] The 2001 Super Bowl in Tampa featured facial recognition, as did the 2002 Winter Olympics in Salt Lake City.

Facial recognition has also been used to track identification cards. In 1998 West Virginia began using a system developed by Polaroid Inc. to "ensure the integrity"[42] of driver's licenses. When a citizen applies for a license or requests a duplicate, his image is searched in the database of current license-holders to remove the possibility of issuing illegal duplicates. The database is created by scanning in the license images of all holders. The technology is being used for a similar purpose in Mexico. FaceIT software

[34] *Facial Recognition Technology,* (n.d.), Retrieved April 18, 2003 from http://www.identix.com/newsroom/lfa.html

[35] Ibid.

[36] Nanavati, Thieme and Nanavati, 69.

[37] Ibid, 71.

[38] Ibid, 71.

[39] "Candid Cameras for Criminals," *BBC News*, (13 October 1998), 1. Retrieved April 18, 2003 from http://news.bbc.co.uk/2/hi/uk_news/191692.stm

[40] Jeffrey Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," *New York Times Magazine*, (7 October 2001), Retrieved February 2, 2003 from http://www.globalpolicy.org/wtc/liberties/surveillance.htm.

[41] Angela Jarvis, "Are Privacy Rights of Citizens Being Eroded Wholesale," Retrieved April 18, 2003 from http://www.forensic-evidence.com/site/ID/facialrecog.html.

[42] "West Virginia Becomes First State to Issue Driver's Licenses Using Facial Recognition," *Polaroid Inc. Press Releases*, (24 March 1998). Retrieved April 18, 2003 from http://www.primarypdc.com/press/98/march/032598a.html.

by Visionics has been licensed in Mexico to prevent voters from registering or voting twice.[43]

A related technology that is emerging on the market is thermal IR facial recognition. This technology involves scanning the face with infrared sensors to observe the vascular and heat properties beneath the skin of the face.[44] The technology will be useful to extend current facial recognition systems such that lighting becomes more of an invariant, since thermograms are unaffected by lighting. A new and evolving technology, facial thermograms have the potential to vastly improve current facial recognition systems.

IRIS RECOGNITION

Iris scans are among the most accurate biometric, but the technology is limited by its usability and by the economic factors surrounding the research. The iris is an internal organ that is positioned in between the cornea and the lens of the eyeball.[45] It is similar to the fingerprint in that it always has a unique phenotype, despite identical genotypes. The characteristics of the iris have been found to be unique between twins and even between the two eyes of the same individual.[46] Because the iris is internal it is not subject to the same environmental hazards as fingers generally are; it is therefore far less susceptible to damage over time and is a more stable biometric than even the fingerprint. Additionally, because the iris has a natural physical reaction to the presence or absence of light, iris scans have the potential to succeed in testing for liveness where other biometrics have failed.[47]

The algorithms for recognizing iris patterns were patented by John Daugman of Cambridge University. Over the course of several million independent tests of these algorithms, there were zero false matches.[48] This level of accuracy is unheard of in biometric identification and verification systems. One might jump to the conclusion that iris scans ought to be employed in any system that could benefit from biometric use, but I will show that the use of iris recognition is difficult and counters the accuracy of the tool. Although magnification of normal photographs can yield an adequate image to work with, monochromatic imaging works best. John Daugman was able to use color photographs to identify the unknown Afghan girl on a National Geographic cover nearly twenty years later, but typical iris recognition systems rely on both infrared and visible light.[49] Using infrared light in addition to visible light allows for a great penetration of the pigmented iris and increases the range of pigments that a system can analyze. The trabecular meshwork is identified by visible light, and is therefore sufficient to recognize many characteristics of an iris. However, the infrared light picks up characteristics of the

[43] Maria Godoy, “Smile, You’re Being Facially Frisked,” *Techlive*, (7 August 2001). http://www.techtv.com/news/culture/story/0,24195,3340850,00.html.

[44] Woodward, Jr., Orlans and Higgins, 77

[45] John Daugman, “Anatomy and Physiology of the Iris,” (n.d.) Retrieved April 18, 2003 from http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html.

[46] Ibid, 1.

[47] Ibid, 1.

[48] John Daugman, “How Iris Recognition Works,” (Cambridge: University of Cambridge, the Computer Laboratory) Retrieved April 18, 2003 from www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf.

[49] John Daugman, “How the Afghan Girl Was Identified by Her Iris Patterns.” Retrieved April 18, 2003 from http://www.cl.cam.ac.uk/users/jdg1000/Afgahn.html

stroma that are missed by visible light, and can therefore reveal more detailed and diverse characteristics than visible light alone.[50]

The first of three automated systems available that identify irises is a large kiosk. The user stands approximately two to three feet from the machine, which locates and obtains an image within a matter of seconds. The camera, using infrared imaging, does nearly all the work. The second system is a small physical access device which involves a mirror. The user is required to be three inches from the camera, while the machine locates the eye in the reflection created by the mirror and obtains a one inch square image of the eye. The third system involves a desktop camera for logical access to a computer. The user in this case is eighteen inches from the camera, and must align his eye with a guidance light. This system has been shown to have poor usability.[51]

The image of the iris is processed by first finding the outer edge of the iris, then locating the black-color border between the iris and the pupil. The trabecular meshwork is the tissue in the iris that accounts for its radial appearance. Within that tissue rings, furrows, freckles, the corona, the stroma and coloration all increase variation between irises and are used to distinguish between individuals.[52] The entire iris is not considered to allow for coverage by eyelids. Often multiple images are required for enrollment to decrease the chance that reflections are being used in the generation of the template. However, after enrollment the system captures a single image of the iris and, most often, performs identification on that image. As opposed to facial recognition, which returns a list of possible matches, iris recognition usually returns a single match.[53]

Iris scan solutions also have an advantage in testing for liveness. Because the iris is an organ, its motion can be measured as a means of testing liveness. Iridian's Sensar product uses this quality in validating the integrity of an iris presented to the camera.[54] The software looks for "hippus movement, the constant shifting and pulse that takes place in the eyes."[55] This is a quality unique to the iris among other biometrics; fingers, faces, and other common biometrics lack a consistent and regular motion that can be relied on to be present in a live person.

If the usability of iris scan systems were improved, they would undoubtedly become the leading biometric due to their high accuracy and stability over time. Unfortunately, under the status quo the systems have proved too difficult for users and rather expensive. The systems have been deployed in a few situations and have proven fairly successful in airport access and prisoner control. However the technology is theoretically suitable for logical access as well as physical, and for both verification and identification purposes.

Airports have been the main customers in the iris scan market. The systems are being used to speed the security check of frequent flyers, who are given the option to enroll in the iris scan program. Amsterdam's Schiphol, New York's JFK, Washington Dulles and London's Heathrow airports have all begun trials using iris scans for frequent

[50] John Daugman, "How Iris Recognition Works."
[51] Nanavati, Thieme and Nanavati, 79.
[52] John Daugman, "Anatomy and Physiology of the Iris."
[53] Nanavati, Thieme and Nanavati, 82.
[54] Dorothy Denning, "Why I Love Biometrics: It is Liveness, Not Secrecy, that Counts," *InfoSecurityMagazine.com*, (January 2001). Retrieved April 18, 2003 from http://www.infosecuritymag.com/articles/january01/columns_logoff.shtml.
[55] Ibid.

flyers.[56] These systems register the iris template onto a smart card, which the user then presents and checks to pass airport security. Prisons have also installed iris scan systems to track the movement of prisoners. In Pennsylvania and Florida over 9,000 prisoners have been enrolled in such systems, and the hope is to eventually enroll and track visitors as well.[57]

VOICE RECOGNITION

The voice falls into a gray area between behavioral and physical biometrics. Although a person can change aspects of his voice by moving the tongue or lips differently, many vocal characteristics are based on physical characteristics. The pitch of one's voice is determined by the length of the vocal cords while the chambers of the throat and nasal cavity mold the sound that comes from the larynx.[58] Voice scan systems share the same benefits as facial scan systems in their ability to leverage existing hardware. Many of these systems can be deployed across a phone line or through microphones already on the market. Analog signals are converted to digital signals before creating a template used in the recognition process.

Voice recognition algorithms focus on a group of characteristics that, when analyzed together, are dissimilar among individuals. The pitch and frequency of the voice, along with the intensity, are examined in conjunction with a group of statistical measurements and are used to distinguish voices. The short-time spectrum of speech, linear prediction coefficients, cepstral coefficients (a measurement of the signal spectrum covered), and spectrograms (which track frequency and energy over time) are examples of these additional measurements.

Templates are created using the method of Hidden Markov Models (HMM). Hidden Markov Models are a way of determining the probability of a given sequence appearing given past sequences. The HMM uses initial voice samples from which the machine can build a data set of probabilistic features. The technology can do 1:1 verification, but has not proven capable of general 1:N identification. Even 1:1 verification can be challenging because of the behavioral aspect of speech. Accuracy is dependent on the user's desire to be verified and willingness to repeat the pass phrase as he did upon enrollment, in addition to stable environmental factors.

Most current voice scan technologies employ a pass phrase, a series of words the user says at enrollment and again at verification. The user must say the exact series of words and may sometimes run into difficulty if he changes the tone of his voice at verification. This problem could arise during everyday conditions; if a user has a cold, for example, and the nasal cavity is congested, often his voice will change as a result. However "more advanced voice-scan systems are designed to accommodate the normal range of changes in individual vocal aspect."[59]

[56] "Schiphol Backs Eye Scan Security," *CNN.com*, (27 March 2001). Retrieved April 18, 2003 from http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/index.html.

[57] *Iris Recognition in Action*, (n.d.), Retrieved April 18, 2003 from http://www.iris-scan.com/iris_recognition_applications.htm.

[58] *Ask Discover: What Makes Each Human Voice Distinct?*, Retrieved April 18, 2003 from http://www.discover.com/ask/main25.html.

[59] Nanavati, Thieme and Nanavati, 96.

In the case of voice technologies, ambient noise can have a large impact on the quality of signal received. Over telephone lines, the problem of ambient noise is minimized, but when cellular phones or small microphones are the means of acquisition, ambient noise can severely affect the accuracy of the system. In the same way that facial recognition depends on the acquisition of a clear image, voice recognition depends on the acquisition of a clear sound signal. Humans often have difficulty understanding speech in a loud restaurant or bar, so it is to be expected that a computer will as well. This problem is solved by filtering out background noise, focusing on the frequencies into which the human voice does fall, and by cropping the spoken phrase from a long recording with dead noise at either end.

To date, many of the successful deployments of voice recognition scans have been in physical access devices, such as door locks. Simson Garfinkel, in his book *Database Nation*, says having a voice print lock on his front door "gave him freedom and power."[60] With a voice lock users are not required to carry a key, only their voice. But, Garfinkel also noted the challenges of having a voice print lock:

> "After a few months, I discovered that I could not enter my house if a jet was flying overhead, or during a particularly loud rainstorm. I also discovered that biometrics are not democratic. Certain individuals could not be reliably identified by the system, while others were always identified on their first try. As a result, I eventually created "voiceless codes" that would let people in without requiring that they first speak a pass-phrase."[61]

Garfinkel's experience abandoning voice recognition for more traditional access control highlights the weaknesses and strengths of voice recognition: its susceptibility to external noise perhaps outweighs the convenience of the service.

Vocent Solutions Inc., out of Mountain View, CA, has just this year released a product to allow for secure, automated password resets over the phone.[62] Their product Voice Secure™ - Password Reset 2.0 uses voice verification to authenticate a user. By automating password resets, companies that deploy this technology are able to cut down on overhead by eliminating employees whose sole purpose is responding to password reset requests. Vocent has this year partnered with Visa International to work toward providing a voice authentication tool to be used with Visa credit cards.[63] Veritel Corporation, based out of Chicago, has a product they call VoiceCheck Web that allows for voice verification over the internet.[64] The product requires users to have specific hardware for their machine, but adds security to online financial transactions.

This technology has also been implemented to ensure that offenders are meeting sentenced house arrest detentions. Washington County in Oregon is one authority that uses voice verification over the phone to ensure that offenders are home at scheduled

[60] Garfinkel, 59-60.

[61] Ibid, 60.

[62] Vocent Press Release, 9 December 2002, Retrieved April 18, 2003 from http://www.vocent.com/pr0018.html.

[63] Paul Roberts, "Visa Gets Behind Voice Recognition," *PCWorld.com*, (21 October 2002), Retrieved April 18, 2003 from http://www.pcworld.com/news/article/0,aid,106142,00.asp.

[64] Randy Scasny, "Veritel Introduces Voice Security Verification," *Internet News.com*, (15 November 2000), Retrieved April 18, 2003 from http://www.internetnews.com/bus-news/article.php/5401_512471.

times.[65] Random phone calls are placed to the user's home and his voice is then verified; in the case that the voice print does not match up, county workers are notified and proceed to investigate.

The systems are unlikely to return a false positive, which makes them very secure; however, false rejections are common and affect usability. If voice recognition were the lock on the front door of a house, and prevented the owner from entering his home half of the time, the technology would hardly be making life any more convenient. However, many false rejections can be attributed to ambient noise; if a viable solution to this problem were found usability might be improved immensely. Additionally, systems that do use a constant pass phrase are susceptible to playback attacks, whereby the perpetrator simply uses a recording of the user saying the pass phrase to gain access.

GAIT RECOGNITION

In our everyday interactions we use a person's gait, their way of walking, as an additional means of identification. Gait is especially helpful to us at dusk or in darkened rooms, when inadequate lighting may cast doubt on our identification of faces or other features. It should not be surprising then that attempts have been made to train computers to recognize individual gaits as well. Trevor Darrell from the MIT Artificial Intelligence laboratory told the *MIT Technology Review* that "we really don't know yet how discriminative a person's gait is," a reality that has hindered gait from becoming a pervasive biometric.[66]

If perfected, the ability to identify people based on their gait alone would be a very powerful biometric because the required user interaction is minimal. However, it is unlikely that gait recognition will reach this technical capacity in the very near future. Like face recognition, gait recognition has the advantage of leveraging already existing technologies but faces difficult environmental challenges. It is likely that gait recognition would be done in conjunction with CCTV surveillance systems. Gait recognition would be less dependent on lighting conditions than facial recognition and similarly dependent on angle. The angle the initial enrollment imagery of a person's gait was taken at may be dramatically different from the angle achieved in subsequent attempts at recognition, leading to increased false reject rates. Watching a person walk toward you is a very different experience from watching a person walk perpendicular to your line of sight; training a computer to identify these differences and overcome them will be a challenging technical problem.

Additionally, gait recognition faces the problem of changed behavior on the part of the user. Many behavioral biometrics are consistent over time: the way you type your password for example, or your signature on official documents. But gait is easily changed, especially if the user makes a conscious attempt to do so. But imagine how often his gait changes subconsciously throughout the day. It is dependent on mood: if he is hurried and anxious, he is walking more quickly with perhaps a longer stride, but if he is taking a relaxing stroll through a park then his stride probably shortens, maybe he puts a bounce in his step and walks slowly. Gait changes depending on the shoes one wears:

[65] John Hartner, *Washington County: Oregon: Residential Services*, (25 July 2002), Retrieved April 18, 2003 from http://www.co.washington.or.us/deptmts/comm_cor/resident.htm.

[66] David Cameron, "Walk This Way," *MIT Technology Review*, April 23, 2002, Retrieved April 18, 2003 from http://www.technologyreview.com/articles/print_version/wo_cameron042302.asp.

imagine a woman leaving her apartment to go to the gym in sneakers, and again later that morning in her heels to go to work. Her gait is going to be very different when she is wearing the heels than sneakers. Clothing also impacts the way one walks: wearing bulky sweat pants will give a different impression of one's gait than wearing shorts or nylon stockings. There are other environmental and behavioral factors that are perhaps less likely to occur: injury to one of the legs or changed weight. All these factors make gait recognition an incredibly challenging problem.

Gait has not been successfully used as a commercial product yet, but is being tackled largely in the research setting. Much of the research is funded with the intent of using the technology in surveillance, as gait would serve little purpose in access control. One can imagine that, if perfected, gait could be used to recognize an authorized person as he walked down a hallway approaching a secure location, already authorizing and opening the location for this individual as he arrives. Though imagining this use is possible, it is most likely that gait recognition will be used to identify people walking through a recorded scene.

DARPA, the Defense Advanced Research Projects Agency, has funded research in the area of gait recognition as a part of its "Human ID at a Distance" program.[67] Researchers at Georgia Institute of Technology are among those funded by DARPA and are using two different approaches to the problem of gait recognition. Like many in the field, the Georgia Tech team is working on an approach using computer vision.[68] The use of computer vision analyzes the movement of body parts in two dimensions over a span of time, and is a common approach being used by researchers at various other institutions, including MIT[69] and Carnegie Mellon University.[70] The computer vision approach uses activity-specific static biometric, a technique that measures static properties, such as the length of a person's leg, in a single frame.[71] The Georgia Tech team is also using a radar system, which they claim is a novel approach, to solve the problem of gait recognition. This system "focuses on the gait cycle formed by the movements of a person's various body parts over time."[72] Neither approach is mature yet, but both are aimed at "detect[ing], classify[ing], and identify[ing] humans at distances up to 500 feet away under day or night, all-weather conditions,"[73] which would certainly be quite an accomplishment

The reliability of gait recognition has yet to be shown because the technology is so new and still under development. Certainly if it were possible to develop a robust recognition system based on gait, the tool would be very useful; one can imagine numerous scenarios: to detect suspicious persons in crowds or approaching a building, or maybe to grant access to secure hallways. In any case, gait recognition could be a

[67] *Human ID at a Distance (HumanID)*, (n.d.), Retrieved April 21, 2003 from http://www.darpa.mil/iao/HID.htm.

[68] *Walk the Walk: Gait Recognition Technology Could Identify Humans at a Distance*, (11 October 2000), Retrieved April 18, 2003 from gtresearchnews.gatech.edu/newsrelease/GAIT.htm

[69] *Human ID @ MIT AI Lab*, (n.d.), Retrieved April 21, 2003 from http://www.ai.mit.edu/people/llee/HID/intro.htm.

[70] *Human ID at CMU*, (n.d.), Retrieved April 21, 2003 from http://www.hid.ri.cmu.edu.

[71] *Walk the Walk: Gait Recognition Technology Could Identify Humans at a Distance*, (11 October 2000), Retrieved April 18, 2003 from gtresearchnews.gatech.edu/newsrelease/GAIT.htm

[72] Ibid.

[73] Ibid.

promising biomteric for future use, if research is able to overcome the environmental and behavioral obstacles associated with the technology.

GENETIC RECOGNITION

Since 1953 DNA has been recognized as the chemical material that determines in large part our physical characteristics. DNA is known to be unique between individuals, except in the case of identical twins, a fact that makes DNA a very attractive means of absolute identification. DNA is now commonly used and widely respected as a means of identification in criminal investigations, to verify parenthood, or to identify cadavers. For example, in the case of a rape or murder, investigators often try to match the DNA in semen, blood or hair found at the scene of the crime to the DNA to provide incriminating evidence. In the case of bodies that have decayed or been burned beyond recognition DNA is used to verify identity and provide loved ones closure. Following the events of September 11, DNA was widely used in order to determine the identities of perished individuals[74] because the bodies and teeth were too charred to recognize.

DNA is present in every cell of the human body and is comprised of approximately 30,000 to 40,000 distinct genes.[75] These genes only account for about 1% of the approximately three billion nucleotides in an individual's DNA; the other 99% of these are not involved in protein creation or have no known purpose. Between individuals DNA only varies by .1%, and even less among related individuals.[76] Variations occur in two ways: through Single Nucleotide Polymorphisms (SNPs) and large regions that are deleted or inserted.[77] The first of these variations, SNPs, is generally used in the study of disease and genetic engineering to identify differences that may lead to small changes in protein production. The larger deletions and insertions tend to occur in the non-encoding regions of the DNA and are, because of their size, more useful in identification purposes.

The most noticeable difference between DNA and the other biometrics discussed in this chapter is the level of intrusion required. DNA cannot be sampled without acquiring human cells. Unlike the fingerprint, the signature of which is left behind on external objects, or the face which is visible to the human eye, DNA cannot be measured or evaluated without sophisticated biotechnology. First, a DNA sample must be made available. This could be a hair, a blood sample, a fingernail or biological tissue. In any case, an actual sample must be obtained and analyzed. Once there is possession of a sample, a technique called DNA typing, or fingerprinting or profiling, is performed. DNA typing looks for molecular markers in the nucleotide sequence; a common type of marker is a tandem repeat.[78] Based on a comparison between the markers in two samples, a "maybe" or "no" is returned as the result of the match.[79] Thus far, DNA typing has been used more often to prove that two sequences do not match than to prove their match.

[74] *9/11 NYC Services Center: DNA Collection Information*, (n.d.), Retrieved April 19, 2003 from http://home.nyc.gov/portal/index.jsp?pageID=wtc_subpage&catID=1787&cc=1787&rc=1782&ndi=1.

[75] Paul Billings and Sophia Koliopoulos, "What is the Human Genome?" *The Human Genome* (Germany: Council of Europe, June 2001), 20.

[76] Ibid, 21.

[77] Ibid, 21.

[78] Tandem repeats occur when identical segments of DNA are arranged in tandem and in a head-to-tail fasion.

[79] Peter J. Russell, *Genetics,* (San Francisco: Pearson Education, Inc., 2002), 208

Proving a match only returns a "maybe" and a probability or confidence score. It cannot prove that because the markers match, the sequences must be from the same source – the technique can only prove that they could possibly from the same source. A probability calculation is then determined. This type of confidence-based answer is not unlike the returns from other biometrics; all those discussed here have an error rate associated with them that indicates the possibility the result might be inaccurate. However, unlike these other biometrics, DNA currently does require a physical sample to be taken, an act that is generally considered more intrusive than the other biometric techniques. It is imaginable that less intrusive measures could be used, but today's technology does not have any such capability.

Despite the level of intrusion required, DNA data banks are proliferating, both in governments and private industry. The United States Army was among the first organizations to set up a DNA databank. In 1992 the army began requesting the DNA of soldiers to help with identification purposes.[80] The modern dog-tag was followed by a similar program to the IAFIS systems described earlier this chapter. In 1994 the Congress passed the "DNA Identification Act of 1994," authorizing the FBI to set up a databank of DNA.[81] In 1998 the Combined DNA Index System was activated with the DNA of 250,000 convicted criminals and 4,600 unidentified samples collected in criminal investigations.[82] This system uses regions of DNA between two and seven base-pairs in length known as "short tandem repeats." England has had a similar DNA database up and running since 1995.[83] Additional databases are run by biotechnology firms racing to cure genetic diseases. These companies tend to request DNA from individuals voluntarily, and in many cases these individuals are informed that though their DNA may eventually lead to corporate profit, the individual will not benefit.

Knowledge of a DNA sequence lends unique insight into the health of the individual. Ted Peters in 1998 catalogued several of the diseases that are linked to specific genes:

> "Already we know that the gene predisposing one to cystic fibrosis is found on chromosome 7 and Huntington's chorea on chromosome 4. Alzheimer's disease is probably due to a defective gene on two chromosomes, and colon cancer to one on chromosome 2. The recently discovered predisposition to inherited breast cancer is located on chromosome 17 and a second on 11, where we also find type one diabetes. Predisposition to muscular dystrophy, sickle-cell anemia, Tay-Sachs disease, certain cancers, and numerous other diseases have locatable genetic origins."[84]

Therefore by knowing a person's DNA, it may be possible to predict what diseases he is likely to suffer from and perhaps what he will die from. This sort of information could become stigmatizing; for example, if a health insurance company were to be informed that the 55 year old individual they were insuring carried the gene for Alzheimer's and

[80] "DNA dog tag or genetic ID?", (n.d.) *Time* (22 June 1992), v139, n25, 35, Accessed through Expanded Academic ASAP April 18, 2003.

[81] Woodward Jr., Orlans and Higgins, 121.

[82] Kluger, Jeffery, "DNA Detectives: Genetic fingerprinting is already being used to identify criminals. Can the rest of us be far behind?", *Time* (11 January 1999), v153, 62.

[83] Ibid, 62.

[84] Ted Peters, *Genetics: Issues of Social Justice* (Cleveland, The Pilgrim Press, 1998), 3.

would later require extensive health care, the insurance company may feel compelled to stop insuring this individual. If the information were made even more public, one could imagine its influence on mating procedures. Perhaps a couple in love avoids having children together because one is a carrier of the gene that has been linked to a rare form of cancer, a fact they would have otherwise been ignorant of.

Because the information contained in DNA can have an enormous impact on health care, and because acquisition of DNA is so difficult and unavailable to the general public, the issue of ownership over the data is a very interesting one. Simson Garfinkel discusses the topic in depth in *Database Nation*, initially posing the following question: "After all, your DNA pattern is uniquely yours. It determines your eye and hair color, the shape of your face, your sex, your race, and countless other characteristics that have come together in a unique pattern – you. How could you *not* own your own genetic pattern?"[85] It does seem logical that one's DNA ought to belong to each individual given the amount of medical and identifying information contained in the sequence of nucleotides. If DNA were to become a viable biometric, the question of how to protect the property interests associated with DNA would be among the first society would have to answer. Allowing any company or government agency access to a full DNA sequence and the associated identity could create a conflict of interests. If it were a government agency, for example, might they choose to test all sequences for the presence of a gene linked to breast cancer in the interest of public health? Or if it were a company, might they choose to sell the sequences or perform internal research to determine the rate of a genetic mutation linked to nicotine addiction in the general public? If such tests were performed, would the individuals be notified of the results? What if they had no interest in knowing the outcome? This problem of DNA ownership must be answered before it can even be considered as a real-time biometric tool.

CONCLUSION

I have provided an overview of how some common and emerging biometrics work and where they are being used today. This discussion I hope provoked additional thought about identity and anonymity. If one has anonymity, no one has access to identifiable information about that person. In the twentieth century world, this was a common occurrence. The clerk at your local department store had no access to identifiable information about you unless you provided it to him. Imagine now if your biometric information was scanned at the counter as you handed over cash to the clerk. Might he now see a name to associate with the individual in front of him, and be able to then associate an identity with you? Had you intentionally forfeited your anonymity by walking in the store? Will biometrics lead to a loss of control altogether over our identity?

The danger with these tools is that they attempt to ascertain an identity directly from physical or behavioral characteristics, which the user may or may not have chosen to have measured. Ideally these tools could identify any physical body entering a building, or at least measure the identity of a person even if that person remains nameless. This last point presents an interesting question which is as of now left unanswered: does it matter that a facial recognition tool, for example, is only searching

[85] Garfinkel, 184.

for ten known individuals in its database? What if a biometric template of each person who walks through is kept for later comparison? Because, as I have argued, biometrics are in fact representations of an identity as is a name or ID number, it should not matter if you are “Marybeth Jones,” or “F345IMO,” or “Template #9730.” All these representations in fact strip identity from the individual, disallowing anonymity. So long as “Marybeth Jones,” “F345IMO,” or “Template #9730” has a way of being linked to a physical body, anonymity is impossible. Furthermore, because “Template #9730” can, using some technologies, be garnered without permission of the individual, it is in some ways a more egregious destruction of anonymity, and therefore infringement of privacy, than the name or ID number that are usually only accessed via the individual’s voluntary disclosure.

The last point that should be clear after reading this chapter is that none of these tools are perfect just yet. Each has a drawback, be it usability, accuracy, convenience or technical maturity. Within the next few years any deployments of these technology will unlikely be able to associate a unique template with each person. However, the promise of these technologies is great, and the potential for each of them to mature cannot be ignored. Especially with current concerns over security, it is likely that more and more dollars will be invested in the improvement of these techniques. When deployed in surveillance, these technologies present far more questions about privacy than when simply used in access control. The next chapter will focus on the concept of surveillance from a theoretical perspective, while discussing actual implementations of surveillance alone and in combination with biometric tools.

5

SURVEILLANCE

"Only those who can sustain an absolute commitment to the
ideal of perfection can survive total surveillance. This is not
the condition of men in ordinary society."
~Alan Westin, *Privacy and Freedom*

SURVEILLANCE

DATA SURVEILLANCE

In the 1990's the rise of the Internet and the proliferation of computer databases prompted increased publicity of the problem of privacy in an electronic age. Books on the erosion of privacy in the new digital age surfaced all around us, the topic of "cookies" no longer included baking recipes but instead directions on how to secure internet privacy, and lawsuits were being defended with the use of recovered emails. The concept of information security has become a hot topic on everyone's minds, and since September 11, 2001, information security as it pertains to surveillance has gained publicity as a means to prevent terrorism. In April, 2003, MIT's *Technology Review* ran a cover story titled "Surveillance Nation" which detailed the numerous ways surveillance will come to transform our lives. Video surveillance, a focus of this chapter, was cited as accounting for less than 1% of all surveillance.[1] The rest consists of surveillance of actions and people via digital signatures and electronic records. I hope to explore the reasons why real-time[2] video and audio surveillance will entirely alter what expectations of privacy we now have, but first I want to briefly examine this other, more prevalent form of observation: dataveillance.

Dataveillance, according to Reg Whitaker's book *The End of Privacy: How Total Surveillance is Becoming Reality*, is a word coined "to describe the surveillance practices that the massive collection and storage of vast quantities of personal data have facilitated."[3] In other words, dataveillance is the act of monitoring a data trail left by an individual's actions. Several examples of this kind of information surveillance were listed in "Surveillance Nation:"

> By 2006, for instance, law will require that every U.S. cell phone be designed to report its precise location during a 911 call; wireless carriers plan to use the same technology to offer 24-hour location-based services, including tracking of people and vehicles…More than a third of all large corporations electronically review the computer files used by their employees, according to a recent American Management Association Survey. Seven of the 10 biggest supermarket chains use discount cards to monitor customers' shopping habits: tailoring product offerings to customers' wishes is key to survival in that brutally competitive business. And, as part of a new, federally mandated tracking system, the three major U.S. automobile manufacturers plan to put special radio transponders known as radio frequency identification tags in

[1] Dan Farmer and Charles C. Mann, "Surveillance Nation," *Technology Review: MIT's Magazine of Innovation* 106 no. 3 (April 2003): 36.

[2] When discussing what I call here "real-time" surveillance, I intend to reference the observation of actions and conversations in public locations as they unfold.

[3] Reg Whitaker, The End Of Privacy: How Total Surveillance is Becoming a Reality, (New York: The New Press, 1999), 125.

> every tire sold in the nation…the tags can be read on vehicles going as fast as 160 kilometers per hour from a distance of 4.5 meters.[4]

It is not immediately clear why these types of observance are cause for concern, yet many books have been dedicated to exactly this topic. Most often, the privacy worries surrounding dataveillance deal with the problem of information ownership. Simson Garfinkel addresses this question in his book *Database Nation*, in a section he labels: "Who Owns Your Information?"[5] Garfinkel examines the argument that personal information should be treated as property in order to afford it protection under the law and thereby insure privacy. He presents cases in which DNA or even a person's name can be used as a means of privacy violation despite classifying this information as property. The name, however, is generally not considered a sturdy identifier in macro-situations because it is not unique. Imagine trying to track down "Adam Smith" in this country if that was your sole piece of information. The United States does not in fact have a mandated, unique identifier for every individual, but unique identification is still possible by combinations of information: for instance, a name and complete address. There is one number, however, that has become as close to a mandatory identification number as one can get: the Social Security Number.

The Social Security Number has in many ways become the default national identifier, but its original dedicated purpose is "to track benefits under a retirement and disability insurance system that does not even encompass the whole population."[6] Nevertheless, today people are generally willing to hand out their SSN on credit card applications, college applications or even medical records. In fact, these actions have become commonplace in everyday lives. The SSN is even used by some states as the driver's license number.[7] David Brin describes the SSN as "*the* symbolic threat to modern privacy,"[8] but what threat exactly does it symbolize? How can one nine digit number pose such an enormous threat to a concept that, as I've shown, is so ill-defined?

Garfinkel's discussion of ownership over information gets at the crux of the problem. With expanded database technologies, our ability to control our personal information has been stripped from us. "Not only do we not know how much of this information is out there, or who has it, but we also have only a very slim chance of being able to assure that it is accurate and almost no control over who might have access to it...."[9] The focus of this problem has been on control over the information, often in the form of ownership. I would argue that it is not the control over information that strikes us as so troubling, but the control over an identity. Recall the example of electronic discount cards used by grocery store as an illustration of this point. Although this example is often cited as a way corporations are instituting surveillance on the masses, it is in fact a form of surveillance which most Americans happily succumb to, feeling little, if any violation of privacy. The common belief is that surveillance is performed with a focus on market research. If this is the case, the focus is on mass behavior, so no single identity should be reduced to data and tracked. The SSN,

[4] Ibid, 37-8.

[5] Garfinkel, 177.

[6] David Brin, *The Transparent Society,* (United States of America: Perseus Books, 1998), 234.

[7] Ibid, 235.

[8] Ibid, 235

[9] Charles Sykes, *The End of Privacy*. (New York: St. Martins Press, 1999), 29.

however, is a substitute for the identity. In nine digits the SSN nails down an individual, removing the need for any further representation of identity.

It is the loss of control over not only ownership of one's identity, but also the reduction of identity to a number, that troubles the American people so deeply. Brin claims that the reason the SSN poses such a pervasive threat to privacy is that it is used as a password, a means to verify identity.[10] I disagree. While the use of the SSN may create data vulnerably, it is not the use alone that causes concern. It is simply the fact that within nine digits is a life. Recall Goffman's powerful description of identity: personal marks associated with a life history.[11] What is troubling then is the fact that the SSN, because it is unique, represents our identity on its own. It is this appropriation of identity into a digital medium that raises concern about dataveillance in general.

REAL-TIME SURVEILLANCE

There exists another type of surveillance, which I will refer to here as real-time surveillance. This involves not the monitoring of a data trail, but the monitoring of actual actions by individuals as they take place in real time. The most obvious example of this is video surveillance. While you are wandering the stores at your local shopping mall, it is likely that cameras are watching ever step you take and feeding the information to human monitors who observe your actions as they unfold.

Other types of real-time surveillance have been used for years, and it is likely technology will continue to perfect and advance these means. Phone tapping has been in use since the early twentieth century and is among the oldest technological aids to real-time surveillance. In this country phone tapping is only legal under certain circumstances, particularly when a warrant is obtained. However, unqualified phone tapping was ruled unconstitutional by the Supreme Court in 1967 in the *Katz* decision.[12] Another example of real-time surveillance is the use of global positioning systems (GPS) to track movement in real time. GPS is a tricky example because it in fact tracks the movement of a device, usually some type of electronic tag, and not intrinsically the movement of a human. For the sake of simplicity, I will include it as an example of real-time surveillance. I am most interested here in the proliferation of video surveillance in public locations.

Great Britain has led the world in the area of video surveillance, installing an estimated 300,000 cameras by 1998 in public locations.[13] The benefits of video surveillance as a form of security was realized in 1994 when a four year old boy was murdered by children six and seven years his senior. Despite their inability to prevent the crime, shopping mall cameras provided evidence to help convict the two older boys of murder. The use of CCTV cameras exploded in the next five years, mainly out of fear of terrorism.[14] From 1994 to 1998 the number of cities employing CCTV in public locations grew from 79 to 440.[15] Many of these towns reported that the cameras were successful in deterring crime; the crime

[10] Brin, 237.

[11] Erving Goffman, *Stigma: Notes on the Management of Spoiled Identity*, (New York: Simon & Schuster, Inc., 1963), 57.

[12] Katz vs U.S., 373 U.S. 427 (1963).

[13] Brin, 5.

[14] Jeffrey Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," *New York Times Magazine*, 2.

[15] Ibid, 2.

rate in King Lynn, the first town to install cameras in public locations, fell to one-seventieth its former rate after the installation of only sixty cameras.[16] In 2001, Jeffrey Rosen reported that there were so many cameras throughout Great Britain that an exact count was impossible, but that an estimated 2.5 million surveillance cameras were employed in Great Britain at the time.[17]

Great Britain has served as an example, but is not the only country to be running video surveillance programs. Several countries in Asia, as well as the United States, have started such initiatives.[18] Baltimore in 1996 was among the first cities in the United States to install CCTV systems to monitor public locations.[19] New York City followed suit in 1997 and installed cameras in Central Park to allow for 'round-the-clock surveillance of the park.[20] Cameras also have been installed in Boston,[21] as well as many small towns throughout the country. The International Association of Police Chiefs reports that over 200 law enforcement agencies in this country use some form of video surveillance.[22]

The Baltimore case demonstrates the gap between actual and professed use. Simson Garfinkel concluded that in fact the cameras installed in Baltimore were "uninspired" and not installed to cause a decrease in crime; rather, their purpose was to "make people feel good" by adding extra security.[23] As I will discuss at length later, the installation of these cameras is often for psychological effect, as was the case in Baltimore. The cameras were installed downtown, while the majority of the city's crime occurred in residential neighborhoods. Here lay the dilemma: install cameras that would observe private property, or install cameras in an ineffective location simply for the sake of affecting the psyches of the citizens. To avoid potentially illegal observation of private property, the latter choice seems appropriate. However, it does seem to defeat the purpose of criminal enforcement, calling into question the use of these video cameras in surveillance.

The potential to expand on current uses of real-time surveillance is great, as is the potential to build new devices to monitor actions in real time. One such purpose that has already been realized, but could be built on, is the use of video surveillance in the home to observe child caretakers. Called "nannycams," couples use the camera to ensure the safety of their children. This example illustrates the principles of social control, which becomes a very real concern in surveillance scenarios. If a nanny intended to hurt a child, the fact is that a nannycam would probably be useless in the direct prevention of that crime; only in bringing the nanny to justice would evidence gathered on tape be useful. However, the knowledge that the child's parents would have access to such evidence instills a fear in the nanny so that "she would discipline herself to behave exactly as required, to internalize the employer's rules."[24]

[16] Brin, 5.
[17] Rosen, "Being Watched: A Cautionary tale for a New Age of Surveillance," 2.
[18] Brin, 5.
[19] Garfinkel, 106.
[20] Brin, 5.
[21] Garfinkel, 107.
[22] Steve Irsay, "Surveillance Cameras Play increasing Role as Investigation Tool," *CNN.com*, (21 September 2002), Retrieved April 10, 2003 from http://www.cnn.com/2002/LAW/10/21/ctv.cameras/.
[23] Garfinkel, 106.
[24] Whitaker, 81

An interesting development that could make even more pervasive the reach of video surveillance is the commercialization of formerly classified satellite imaging technology.[25] Mark Monmonier refers to this type of surveillance as “remote sensing” and traces its development to military importance during the Cold War.[26] Among these technologies is the global positioning system, or GPS. Monmonier points out the privacy dilemma currently raised by GPS:

> Equally adept at tracking vehicles, employees, adolescents, and convicted criminals, GPS is very much a surveillance technology, with credible threats to personal privacy. Just ask the former clients of Acme Rent-a-Car, a Connecticut firm that tracked its vehicles by satellite and fined customers for exceeding 79 MPH.[27]

Again, in the example of the rental car company, the same problem occurs as with video surveillance as a crime deterrent. There is no direct prevention of speeding, only indirect prevention through induced fear. The satellite technology already available currently serves as an effective means of real-time surveillance; in time it will only be improved upon such that even more detail can be observed from up in the sky.

THE PANOPTICON

Jeremy Bentham in the nineteenth century created a theoretical architecture for a prison system, which he called the Panopticon. According to Michael Foucault, Bentham called the architecture “*the* great innovation needed for the easy and effective exercise of power.”[28] The Panopticon, then, is a mechanism for social control. The idea of the Panopticon rests on a central monitor capable of viewing all cells at any time. The architecture consists of a central tower from which a monitor could watch the cells, and several stories of cells encircling that tower. The cells each had a window facing the tower and a window facing the outside; in this way no matter where the prisoner stood in his cells, either he or his shadow was visible to the monitor. Prisoners see the central tower and know someone might be watching, but never know at which point in time they are free from observation and at which point they are under surveillance. Foucault has discussed the Panopticon in detail and perhaps provided the most powerful analysis of its power.

> In each of [the Panopticon’s] applications, it makes it possible to perfect the exercise of power. It does this in several ways: because it can reduce the number of those who exercise it, while increasing the number of those on whom it is exercised. Because it is possible to intervene at any moment and because the constant pressure acts even before the offences, mistakes or crimes have been committed. Because, in these conditions, its strength is that it never intervenes, it is exercised spontaneously and without noise, it constitutes a mechanism whose effects follow from one another. Because, without any physical instrument other than architecture and geometry, it acts directly on individuals; it gives ‘power of mind over mind’. [29]

[25] Ibid, 86.

[26] Mark Monmonier, *Spying with Maps: Surveillance Technologies and The Future of Privacy*, (Chicago: The University of Chicago Press, 2002), 10.

[27] Ibid, 13.

[28] Michael Foucault, *Power/Knowledge: Selected Interviews & Other Writings*, Ed. Colin Gordon, (New York: 148.

[29] Michael Foucault, Discipline & Punish: The Birth of the Prison. Trans. Alan Sheridan. (New York: Random House, Inc., 1978), 207.

The Panopticon then is a psychological exercise: it acts by instilling fear in the prisoners. Foucault also discussed the limitless possibilities for this architecture; it could be used in hospitals, in school-rooms, and in places of employment.[30] Briefly, I want to introduce again anonymity in the context of this arrangement. Note that it must be that each prisoner is identifiable while in his cell to the monitor; if a prisoner for one second believed the monitor could not identify who acted out he may embolden against his fear and the Panoptic power instilled in the monitor would lessen.

Bentham’s Panopticon was engineered with an eye towards exercising power over inmates. A prerequisite of the Panopticon individuals are stripped of privacy as a forfeited right, but this is not in fact the focus. In the Panopticon the individual is forcibly placed under surveillance, and can never predict when observation will take place. The focus of the Panopticon is exertion of power over the individual by eliminating his ability to choose when and under what circumstances his actions, thoughts, and words will become public.

Many authors compare data surveillance to the concept of the Panopticon as presented by Jeremy Bentham, a comparison I believe is imprecise. In real-time video and audio surveillance a more accurate realization of the Panopticon takes place. Rather than observing data trails, these types of surveillance threaten to directly monitor individual thoughts and actions in the everyday life. Whereas dataveillance is unable to see or hear the conversation you and your friend had in the park after school one day, the real-time surveillance systems created in particular by closed circuit television systems are able to monitor these seemingly insignificant actions. These types of surveillance threaten to expand on the digital Panopticon by creating an actual “gaze” of which to be wary.

I will first discuss the problem of real-time surveillance in public, and will then introduce a biometric enhanced surveillance system as an emerging means of observation. In this discussion, I would like to show that while typical real-time surveillance systems already create a Panoptic gaze, adding biometrics further strengthens the gaze by stripping one’s anonymity and therefore an aspect of privacy.

Dataveillance does not exert the same singular gaze that the Panopticon stresses. The primary concern with dataveillance is not that individuals lose power over their lives, but more specifically that one's identity may be stolen. In particular, the current means of dataveillance provide the individual choices: choices over when to succumb to observation, or at the very least knowledge of when observation takes place. The reason Brin refers to the SSN as “*the* symbolic threat to modern privacy” is because it bundles an identity into a single datum that can easily be manipulated and misused, stripping the individual of power to even be himself. The power that is lost here is far different from that lost in a Panoptic gaze. Indeed, the two types could potentially overlap, as might happen if biometrics were implemented in real-time surveillance. It is an important distinction to note, however, that in fact dataveillance fails to exert the psychological power of a true Panoptic gaze, and that in fact the analogy of dataveillance and Panopticism is a rather weak one.

There is yet another important distinction between dataveillance and real-time surveillance that will be important in illustrating that one is of a Panoptic type while the other is not. As has been discussed, in a real-time surveillance system, particularly those in public, an individual loses choice over the time observation will occur, and he becomes unaware of when the system is paying attention to him. He is now not providing an identifying number

[30] Ibid, 203.

to a store clerk but is walking his dog in the park. Whereas he chose to provide the number to the clerk and knows exactly when he does so, he does not make the same conscious choice to provide his image and voice to a surveillance system in a public park and is certainly unsure of when exactly he is monitored; he is left to wonder if he might be monitored at any time he is in the park. It is the case that often individuals are ignorant of exactly when and how identification numbers are used and tracked, but often this ignorance is fueled by laziness. Navigating the data web requires reading the fine print, and securing one's identity might require making tough decisions. It might be that rather than make a convenient online purchase from a department store, an individual chooses to withhold credit card information and physically visit the store to make the purchase. In forfeiting convenience he secures his credit card information. Note the motivation here: people succumb to dataveillance in order to increase convenience in their lives. This, we will see, is not so true of real-time surveillance.

Whereas a primary goal of most dataveillance is to increase convenience for the individual, the primary goal of most real-time surveillance is to increase security for the individuals and provide additional enforcement mechanisms. There is little increase in convenience for the individual walking his dog, but there may be an indirect increase in security. I say indirect here because although justice may be measurably improved through video or audio surveillance by obtaining evidence of a crime occurring, it is difficult to measure prevention. If a monitor notices on surveillance video that a man is approaching a woman in a park with a gun in his hand, there is little the monitor can do at that point in time to prevent the man from shooting the woman, if that is his intent. After the fact, it will be easy to bring the man to justice: could any jury deny video evidence that showed a man in the act of murder? The main goal of these systems is psychologically enforced prevention: "Criminal attacks are less likely in spaces under constant watch, and activity that degrades neighborhoods, such as drug dealing and prostitution will tend to withdraw from areas of active surveillance."[31] No single crime is prevented as a direct result of the surveillance, but in general criminals fear justice and are thus less likely to break the law.

However, this type of surveillance does have a direct negative effect for the individual. As Ruth Gavison points out, "even casual observation has an inhibitive effect on most individuals that makes them more formal and uneasy."[32] The fact that physical observation affects our thoughts and actions is critical. Milan Kundera reflected on the human result of surveillance in a powerful piece of writing in *Testaments Betrayed.* Kundera describes a Russian figure who had become the subject of real-time surveillance, whose private conversations had been recorded and subsequently broadcast on the radio.

> …instantly Prochazka *was* discredited: because in private, a person says all sorts of things, slurs friends, uses coarse language, acts silly, tells dirty jokes, repeats himself, makes a companion laugh by shocking him with outrageous talk, floats heretical ideas he'd never admit in public, and so forth. Of course, we all act like Prochazka, in private we bad-mouth our friends and use coarse language; that we act different in private than in public is everyone's most conspicuous experience, it is the very

[31] Whitaker, 141.

[32] Ruth Gavison, "Privacy and the Limits of the Law," *Philosophical Dimensions of Privacy: An Anthology,* Ed. Ferdinand Schoeman, (Cambridge: Cambridge University Press, 1984), 363.

> ground of the life of the individual; curiously…it is rarely understood to be the value one must defend beyond all others.[33]

Kundera's account of surveillance is among the most powerful descriptions of why public observation seems such an invasive and improper action. It is because we fear similar repercussions for our observed actions that the Panopticon can theoretically exercise so much power over the individual. Real-time surveillance makes even our most benign actions and words available to anyone, even those we cannot see, deceiving us in our ability to act as we would in private.

In September 2001, Madelyne Toogood was videotaped in a Kohl's department store parking lot beating her four-year-old daughter in the back of her car. She "scanned the Kohl's parking lot to see if anyone was looking"[34] before beginning to slap her daughters' face and tug her hair. The entire event was caught on videotape and broadcast nationally as police searched for the unidentified woman. Toogood eventually turned herself in, faced felony charges of battery and lost custody of her daughter.[35] Toogood served as an example of how surveillance cameras might bring greater justice and security to society. It also shows the ways in which surveillance alters our behavior.

It is likely that Toogood, and other mothers, act unkindly in the home, perhaps in a similar manner to that described above. Many parents spank their children as a form of punishment, an action that is entirely legal in this country. They carry out these forms of punishment most often in the privacy of their own home. If a parent felt compelled to act in such a manner in public, likely they would examine their surroundings to determine how much privacy to expect, much like Toogood did. But under real-time surveillance scenarios one is often unable to determine who is watching – the cameras may be hidden, lenses invisible to the eye. Are we then to go through our lives assuming at all times that we might be watched, unless we are in the privacy of our own home? This is in fact the goal of the Panopticon, to alter our behavior through psychological exercise, thereby increasing security, discipline and social behavior. It is this exact relationship that likens real-time surveillance to Bentham's Panopticon.

BIOMETRIC-ENHANCED SURVEILLANCE

At the 2001 Superbowl the use of facial recognition to identify suspected terrorists received public attention.[36] Facial recognition is one of several biometrics discussed in the previous chapter that are being deployed in real-time surveillance systems to aid in the identification of individuals. Great Britain was the world leader in adopting facial recognition to use in surveillance of public areas. In the United States the idea seems to have taken off following the events of September 11, 2001. Among the leaders in the field, Visionics' C.E.O. Joseph Atick hopes to put his facial recognition technology to use in America's

[33] Milan Kundera, *Testaments Betrayed: An Essay in Nine Parts*, Trans. Linda Asher, (New York: Harper Collins Publishers, 1995), 261.

[34] Steve Irsay, "Surveillance Cameras Play increasing Role as Investigation Tool," *CNN.com,* (21 September 2002), Retrieved April 10, 2003 from http://www.cnn.com/2002/LAW/10/21/ctv.cameras/.

[35] "Mom: No Excuse for Striking Child," *CNN.com* (n.d.), (23 September 2002), Retrieved 10 April 2003 form http://www.cnn.com/2002/US/Midwest/09/23/tuchman.toogood.cnna/.

[36] Declan McCullagh, "Cal It Super Bowl Face Scan," *WiredNews* (2 February 2001), Retrieved April 21, 2003 from http://www.wired.com/news/politics/0,1283,41571,00.html.

airports to increase security.[37] In New York City one hundred cameras were placed in Times Square following the attacks, each enabled with biometric technology.[38] Similar cameras have been installed in high crime districts in U.S. cities like Tampa, and, as mentioned, they were used at the 2001 Superbowl.[39] In Illinois the technology has hit the Department of Motor Vehicle records, where facial recognition is used to ensure that duplicate drivers' licenses are not issued inappropriately.[40] One can envision drivers' license photographs being leveraged for the implementation of facial recognition in surveillance cameras in the city of Chicago.

While neither has received as much attention as the face, voice recognition and gait recognition are also primed to invade the surveillance market. Currently voice recognition is most commonly used as an authentication technique in access control. However, leveraging telephone lines or cellular communication is an ideal means for voice recognition to gain a foothold in the surveillance market. It is also logical for voice recognition to be deployed in CCTV systems; install a few microphones, and along with the visual image of individuals a recording of voices can be made. Gait recognition may receive increased attention in the future as a part of DARPA's "Human ID at a Distance" program.[41] The technology in this case is not yet robust enough to be deployed in real-time systems, but the goal of current research is "to detect, recognize and identify humans at great distances."[42] Iris recognition, presumably the most accurate of these biometrics, also has the potential for use in surveillance. Garfinkel reports that "British Telecom … has developed a high-speed iris scanner that can capture the iris print of a person in a car driving at 50 miles per hour."[43] Although Garfinkel later expressed doubt over the validity of this information,[44] the idea is not a ludicrous one and may in fact be a research goal of companies and governments.

Real-time surveillance has the effect of imposing a Panoptic structure to our public lives. In the United States and elsewhere, video surveillance in particular has become an everyday occurrence, something we expect and are accustomed to. On average a person in Great Britain is seen by 300 different cameras a day.[45] A similar statistic is hard to come by for the United States, as we have not yet reached the per capita numbers of cameras that Great Britain has, but in New York City the average person is recorded between 73 and 75 times a day.[46] Obviously the Panoptic structure pervasive in the videotapes society is of little import to the British; they are able to go about their daily lives without much worry. However, the introduction of these biometric devices into real-time surveillance is cause for more serious concern. To demonstrate this, I need to return for a moment to an earlier discussion of identity and anonymity.

[37] Jeffrey Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," 1.

[38] Ibid, 1

[39] Phillip Agre, "Your Face is Not a Bar Code: Arguments Against Face Recognition in Public Places," (Version of 2 June 2002). Retrieved March 10, 2003 from http://dlis.gseis.ucla.edu/people/pagre/bar-code.html.

[40] Thomas Colatosti, "Viisage Deploying Face Recognition System for Illinois," (7 May, 1999), Retrieved April 19, 2003 from http://www.viisage.com/May7_1999.htm.

[41] *Human ID at a Distance (HumanID)*, (n.d.), Retrieved April 21, 2003 from http://www.darpa.mil/iao/HID.htm.

[42] Ibid.

[43] Garfinkel, 56

[44] Garfinkel, (Personal Communication, 26 July 2002).

[45] Jeffrey Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," 2.

[46] Dean E. Murphy, "As Security Cameras Sprout, Someone's Always Watching," *The New York Times*, (29 September 2002), 33.

In Chapter 3, I commented on the various representations of identity: a name, a number, a visual image, even a chemical sequence. I argued that although all these pieces of information do indeed represent identity, the most practical representations translate directly to a body. Without the associated body, a name is just a name, a number a number. I also claimed that anonymity, or lack of identifying information, alters the conditions under which privacy is violated, thereby changing the level of violation that occurs. Here I have discussed the ways in which surveillance can affect a person's psyche, altering their behavior by creating a Panoptic environment. It is my claim that the destruction of anonymity is a critical component of a Panoptic structure, and that such destruction can take place when biometric technologies are deployed in real-time surveillance.

Bentham's Panopticon worked on the assumption that all the inmates were identifiable. Indeed, in a prison structure there is a controlled set of inmates, all of whom are assigned a specific cell. One can imagine that if the cells were unmarked and indistinguishable, the Monitor in the tower would be powerless to enforce any rules or act on any infringements – how would he decide in which of the many cells the inmate was located? It is necessary, therefore, that the Monitor be able to identify those he observes. If the inmates at any point believed themselves to be anonymous to the Monitor, especially if they in fact were, the power created by the Panopticon would be leveled. The key is not only that the inmates believe they are being watched, but that they also believe the Monitor will identify and punish those responsible. Whitaker states that "the prisoners, incarcerated in their individual cells, are also incarcerated in their bodies."[47] In actuality, the prisoners are incarcerated in their identities. A prisoner in the Panopticon cannot wander the yard anonymously as would an average citizen in a public park – indeed "the very reason the subjects of the Panopticon are there to be watched and trained is because they are prisoners deprived of civil liberty and personal choice."[48]

Therefore destroying anonymity is necessary to utilize the Panopticon. Rosen claims that "Britain, at the moment, is not quite the Panopticon, because its various camera networks aren't linked and there aren't enough operators to watch all the cameras."[49] The connection of these systems is not far off in the distance, according to Rosen, but still Great Britain will be shy of a total Panopticon. Only when those systems are connected to each other and to a centralized biometric system will the Panopticon be fully realized. Without biometrics, individuals feel they are just another person to the Monitor behind the cameras, that they will easily be overlooked. But when biometrics like facial recognition are in use, it is unclear if the Monitor will be selective in who he watches, since the Monitor will be a computer system "watching" those in its database. London has in fact considered populating facial recognition databases not only with known terrorists, but also with the images of those individuals who have registered with the driver's license bureau.[50] In this case, an individual might not be able to feel that he is just another person to the Monitor, but instead may fear that the Monitor could identify him. Anonymity, or at least the illusion of anonymity, will be removed when biometrics are universally introduced into surveillance. This will mark the full realization of the Panopticon in Great Britain, and eventually elsewhere, reducing the individual to a prisoner of the surveillance system.

[47] Whitaker, 34

[48] Ibid, 35.

[49] Jeffrey Rosen, "Being Watched: A Cautionary Tale for a New Age of Surveillance," 5.

[50] Ibid, 3.

6

CONCLUSION

“Ultimately, surveillance will become
so ubiquitous, networked, and searchable
that unmonitored public space will
effectively cease to exist.”
~ “Surveillance Nation”
MIT Technology Review

CONCLUSION

What I have presented in the previous four chapters leads me to the conclusion that the use of biometrics in surveillance systems infringe on privacy in order to successfully realize the Panopticon these systems aim to construct. This argument rests on three main points: anonymity falls under the umbrella of privacy; biometrics present a novel way to identify humans, but one that puts at risk the ability to remain anonymous; real-time surveillance aims and nearly succeeds at constructing a Panoptic architecture with the intent of controlling social behavior. I will approach the argument by first reviewing why anonymity is essential to privacy, and then showing that biometrics make anonymity impossible in a way that is new and distinct from more traditional means of identification. I will then show that in order for real-time surveillance to achieve its goal of increasing security, the systems must strip individuals of privacy, and therefore must strip them of the ability to be anonymous. Because biometrics achieve the necessary end of stripping individuals of anonymity, their use in surveillance has the potential to invade privacy.

Although it is often treated superficially in the literature on privacy, anonymity is a necessary component of privacy. The ability to be anonymous relies on the control over one's own identity. There are many practical representations of an identity: a name, a number, a visage, and variations on these. Control over this information is identical to control over personal information, which is the foundation of many theories on privacy. Those theories that do not rest on control over information rely on the relationship between privacy, relationships, and intimacy. I argued that anonymity provides protection against invasions that could affect relationships or intimacy, thus protecting privacy. Recall the example of a couple in love strolling through a park: though they are in public, their anonymity with respect to those around them allows them intimacy and further maintains the privacy of their relationship. If the couple hopes to maintain secrecy in their relationship, it would not matter that strangers observe their actions in the park; only when their identities become available to those strangers, when they lose anonymity, do they lose privacy. In this way, anonymity is a vital piece of any definition of privacy.

Biometrics inherently eliminate anonymity, and therefore have the potential of infringing on privacy. Biometrics present a novel way of representing identity by relying not just on a piece of data, a name or number, but also on the physical body. Some of the higher-profile biometrics recognize irises, faces, fingerprints, or even gaits. All of these are treated as representations of an identity, as personal information. They all also rely on unique physical characteristics of the human body as opposed to more traditional means of identification that rely solely on non-body information. Therefore, individuals lose control over identity because it is hard to control access to one's physical body if one is to be present at a given location. We are able to find anonymity when our physical appearance is unidentifiable to our surroundings, and we withhold other identifying information over which we have control. However, we cannot easily withhold our physical representation, so if a biometric system can identify that, we have lost the ability to remain anonymous.

In most cases biometrics have been used for access control. In these settings, though an individual has lost the ability to remain anonymous with respect to the system involved, his privacy is not invaded because he chose at some point to enroll in the system, forfeiting his anonymity to that system. These cases are no different than a student who introduces himself to a room full of classmates: he has forever forfeited his anonymity to those students. However, if individual biometric databases were aggregated or forfeited to a central authority, this could present a larger privacy concern. In that case, an individual might not choose to forfeit anonymity to the central authority, but that choice has been made for him. In this way, biometrics might present the same privacy concerns that arise from dataveillance today: aggregation of identifying information, and loss of individual control over that information.

The larger point I have addressed is the issue of deploying biometrics in surveillance. This issue is extremely relevant today because of a push in America to increase security after the attacks of September 11, 2001. Surveillance is an ideal mechanism to enforce the law, and as such is receiving a lot of attention as a potential solution to current security holes. In its most basic form, real-time surveillance falls short of fully realizing this goal. However, by including biometric technologies it just might succeed.

Most real-time surveillance systems have been installed with one purpose: enforcement and deterrence of crime. Therefore, the intent of real-time surveillance is in line with that of the Panopticon: social control. Recall that real-time surveillance disallows individuals choice over when and where they will be monitored, and by whom. This is the defining characteristic of the Panoptic structure: that individuals are constantly aware of the potential for observation, but never fully informed about actual observation. So it is logical to conclude that real-time surveillance not only aims to construct Panoptic control over individuals, but nearly achieves that end. Any system that effectively enforces social behavior must destroy privacy within the system. In other words, if real-time surveillance in a public park aims to deter criminal behavior, it will only be effective if it successfully destroys privacy within the park. From my discussion of privacy, recall that many theorists focus privacy on control over personal information. Many also indicate that privacy is necessary to the construction of "self" and that ownership of one's identity is critical to that construction. There are several who also agree that privacy, or lack thereof, plays a critical role in our behavior. All these concepts are torn apart by the Panopticon. Prisoners no longer control their personal information; instead the Monitor has control over identifying information and could pass it out at will to visitors. A prisoner is furthermore not expected to construct a "self" or to own his identity. Quite the contrary, prisoners are seen as individuals who have lost their freedoms, or, as Foucault suggested, are the subjects of social experimentation. The loss of control over identifying information and the ignorance as to whom might be in the tower, aware of each prisoner's identity, and the ignorance as to when they might be watching, strips individual privacy from the prisoners. This loss of privacy is critical to the functioning of the Panopticon. If a prisoner has no privacy, he cannot think and act freely as he might in his own home. His behavior will change as a result – it will conform to social norms, achieving the end of the Panoptic structure.

In order to fully destroy privacy, the Panoptic structure must also make anonymity an impossibility. If it does not, an individual can find privacy in the protection of anonymous behavior. To clarify this point let us work with the example of a bank robber. The traditional bank robber is the perfect criminal: he is able to walk into a bank full of people, ask the teller for money, and escape in time to avoid capture. Even if he gets away, a confident robber always takes a risk that he will be identified later by the people in the bank. How does the robber alleviate this risk? The common image of a modern robber is a man wearing a black ski mask. The reason should appear obvious: wearing a mask makes identification based on appearance nearly impossible, so if he is able to escape there is a good chance he is free from identification at a later point. The bank robber relates to the prisoner in the Panopticon. If a prisoner could find a way to make himself unidentifiable to the Monitor, he would be fearless in his actions. The Monitor's power relies on his ability to identify each and every prisoner at any point in time; if this is ever not the case, or the prisoners believe it to not be the case, the deterrence effect of the Panopticon would be minimized.

The Panopticon therefore relies on identification, and therefore requires that anonymity be impossible within its structure. Recall that if a person is anonymous, identifying information about him is unavailable and his identity is therefore unavailable. Then it is necessary that at least one or many representations of identity are available to the Monitor at all times. The most logical scenario is that the monitor links cell numbers with names, and can presumably discern the cell numbers from his perch in the tower. In this way he can access the identity of any prisoner at any time by controlling identifying information about the prisoners. This makes possible the absolute destruction of privacy within the Panopticon.

If modern real-time surveillance systems do indeed aim to control social behavior – to prevent crime – then they lack one key ability the Panoptic structure relies on: the destruction of anonymity. Currently people control, for the most part, when and where they are anonymous. Unless I tell another person my name, he has only his memory of my visual appearance to identify me with in the future, and he lacks a way of gaining more information about me. I am anonymous to him, and my actions in his presence are therefore fleeting. Even when using biometrics for access control, the individual decides to enroll in the system in order to gain a privilege. He is therefore aware that he has become identifiable to that system. And even when closed-circuit television is watching me, I believe myself to be anonymous barring any criminal behavior. In fact, even if I commit a crime, the current system requires authorities to play back a tape and run my image against available driver's license photographs, and sometimes to publicize the information in hopes that someone else might recognize my image. Biometrics, however, could change this.

Imagine a biometric surveillance system that was flawless – it could identify everyone in its database without fail and could do so without anyone's cooperation. Then imagine deploying this system in a public park. Now, if I begin a conversation with a stranger and never identify myself to him, there is a good chance I am still anonymous to him – unless he has access to a surveillance system. Can I ever be sure who might be a "Monitor" and who is not? And even if I remain anonymous to this stranger, there likely is someone watching me to whom I am not anonymous because of the new system. Now, if I commit a crime I will be identified without fail. I might not even have to act criminally, perhaps I just behave in a socially deviant manner. Now the Monitor can associate my identity with a socially deviant individual. In this scenario, I have lost anonymity, certainly with respect to authorities, and potentially with respect to individuals around me. This system would complete a Panoptic architecture by closing the hole present in current real-time surveillance: the possibility of anonymity.

I have pointed that there currently does not exist a flawless biometric system, let alone a flawless biometric surveillance system. However, the potential to create a reliable and accurate system does exist. One of the technologies that looks most promising in this regard is the thermal infrared facial scan. Thermal IR corrects many of the problems faced by traditional facial recognition by eliminating the variables introduced by lighting. If the technology is developed further in conjunction with facial recognition, it could potentially create a system capable of identifying faces independent of the environment. If gait recognition is used in conjunction with thermal IR facial recognition, the result could be powerful, but the technology behind gait recognition still requires development. Another technology that may develop towards use in surveillance is iris recognition. The algorithm for iris recognition is excellent and makes this biometric among the most accurate. The hardware is the one component of iris recognition that makes it difficult for surveillance use: it currently requires proximity. It is conceivable, however, that in time the hardware acquisition devices will improve to allow for greater distance between the iris and the camera. If any of these technologies are improved enough to be near flawless, their ability to destroy anonymity would certainly complete a Panoptic structure in surveillance.

What if biometrics are not improved upon? In their current state, I believe biometrics could still be installed in surveillance to achieve a Panoptic structure. The critical detail about the Panopticon is not that the Monitor is watching the prisoners at all times, it is that the prisoners *believe* the Monitor *might* be watching them at any time. It would be enough, then, to deploy biometrics in real-time surveillance so long as the masses *believed* the tools worked flawlessly. It would even be enough if each individual believed the system was *good enough* to identify him. Therefore, even though I showed that biometrics today are technologically unsophisticated enough to actually destroy anonymity, the use of these tools in surveillance would convince people that anonymity *might* be destroyed, thereby increasing the likelihood that individuals would behave as it if were. This would complete the Panopticon without even asserting absolute control – the façade that absolute control exists is enough to alter behavior and exert social control.

I began this work by asserting that understanding the technical details was crucial to successfully evaluating any problem. Indeed, any scientist will understand the failings of biometric systems in their current form. It seems logical then that criminals might understand these failings as well, and be unconvinced by the façade of absolute identification. Conceivably then the Panoptic power would not be as effective over these criminals, and the surveillance system might fail to deter criminal activity. It is likely that if biometrics in their current form were installed in surveillance systems, the full Panoptic power would not be realized because any initial façade that might be created would be quickly broken by those who understand the technical details. Before long, the public would learn that the system was not as smart as they were lead to believe, and would no longer fear the loss of anonymity. In this way, the technical details do play an important role in the social analysis.

I have shown that not only do biometrics destroy anonymity and therefore have the potential to invade privacy, but that when deployed in surveillance they serve to complete a near-perfect Panopticon. It is likely that the spread of real-time surveillance cannot be stopped at this point, and it is likely that the deployment of biometrics in these systems is unavoidable. The first and foremost concern for policy-makers ought to be the prevention of aggregation in the biometric community. That is to say, it ought to be impossible for any entity to share biometric templates of its users to any other entity. This needs to include both corporate and government organizations, and organizations that use biometrics in either surveillance or access control. Additionally, while biometric standards are helpful, the standardization of any algorithm or tool should be minimized. If a universal fingerprint recognition system were accepted, for example, aggregation of fingerprint templates across organizations would be eased. Therefore, universal systems need to be discouraged, if not outright disallowed. Aggregation across data types should also be outlawed. In other words, linking of a database solely containing biometric data and a credit database is unnecessary and only opens opportunities for the continuation of dataveillance. A system established to recognize known criminals need not access a database of credit histories, or any other database for that matter. This kind of cross-database access may facilitate the ability to track suspected criminals over a range of locations and circumstances, but will also encourage discriminatory behavior on the part of the authority.

Leveraging data such as driver's licenses is unnecessary and should be limited, if not disallowed altogether. If biometrics are to be used in surveillance, there is no reason for an innocent individual to fear his inclusion in the database. The only reason he might fear inclusion is out of suspicion that his image, for example, had been leveraged from publicly available data. We need to require authorities to justify the database they use; this could involve obtaining a warrant to include particular individuals as a means of proving the individuals in question were of a real threat.

If possible, the use of biometric surveillance in public locations should be limited to uses for which a very strong case of necessity can be made. For instance, if the systems in Baltimore were indeed installed in an area where crime was not prevalent, they should be removed. Perhaps we should require authorities to obtain a warrant, or some equivalent documentation, to install a biometric surveillance system in public. Limiting these systems is probably the most important policy goal, but will be the most difficult to attain.

In particular, Americans should be cautious of installing biometric systems as a means of preventing future terrorism. These systems will be successful at establishing social control over the common individual - at creating a modern Panopticon. However, terrorism is not a common crime, and terrorists are not common criminals. As evidenced by the rash of suicide bombings in Palestine and Israel in the past years, as well as by the nature of the 9/11 attacks, modern terrorists are fearless. Those people who seek to carry out terrorist acts against the United States do so with the intent of martyrdom. If an individual plans on ending his own life in an effort to harm the lives of others, is social control really going to be successful at convincing him of doing otherwise? Probably not. Even in a Panoptic setting, such an individual is faced with two possible outcomes: he dies in a successful terrorist strike, or he is caught in an attempted terrorist strike and faces a life in jail, or possibly death. If he is intent on causing harm to other people, the first option is probably a more attractive one to him. So a Panopticon is useless against terrorists, and should not be constructed under the guise of providing protection against future terrorism. Indeed, such a ploy would probably serve only to demolish privacy in this country while doing little to prevent terrorism.

We should above all be wary of the current trend to increase security. Today it may seem that biometric surveillance is an answer to terrorism and criminal behavior, but we may find in ten years that we have regained security through other means and have lost privacy along the way, and therefore lost freedoms. A critical balance must be found between this eagerness to secure the nation’s buildings and public arenas and the drive to preserve privacy as one of our civil liberties. In some cases, the move to install biometrics in surveillance may be driven by corporate agendas, which ought to make us even more wary. As a society we should decide for ourselves if a biometric surveillance system will have a markedly distinct affect on safety, or whether it will just create the image of increased surveillance.

WORKS CITED

3-D Face Scan Distinguishes Twins, March 10, 2003, 1, Retrieved April 18, 2003 at http://www.wired.com/news/conflict/0,2100,57984,00.html

9/11 NYC Services Center: DNA Collection Information, (n.d.), Retrieved April 19, 2003 from http://home.nyc.gov/portal/index.jsp?pageID=wtc_subpage&catID=1787&cc=1787&rc=1782&ndi=1.

Agre, Phillip E.. "Your Face is Not a Bar Code: Arguments Against Automatic Face Recognition in Public Places." (Version of 2 June 2002). Retrieved March 10, 2003 from http://dlis.gseis.ucla.edu/people/pagre/bar-code.html.

Alfino, Mark. "Misplacing Privacy." *Journal of Information Ethics*. (Fall 2001): 5-9. Retrieved on October 30, 2002 using WilsonSelectPlus, Wellesley College.

Alfino, Mark and Randy Mayes. "Rationality and the Right to Privacy." *Today's Moral Issues,* ed Daniel Bonevac. (Mountain View: Mayfield Publishing, 2001): 307-312.

Ask Discover: What Makes Each Human Voice Distinct?, Retrieved April 18, 2003 from http://www.discover.com/ask/main25.html.

Benn, Stanley. "Privacy, Freedom and Respect for Persons." *Philosophical Dimensions of Privacy: An Anthology*. Ed. Ferdinand Schoeman. (Cambridge: Cambridge University Press, 1984).

Billings, Paul. and Sophia Koliopoulos. "What is the Human Genome?" *The Human Genome.* (Germany: Council of Europe, June 2001).

Boling, Patricia. *Privacy and the Politics of Intimate Life.* (Ithaca: Cornell University Press, 1996).

Branscomb, Anne Wells. *Who Owns Information?* (New York: Basic Books, 1994).

Brin, David. *The Transparent Society.* (United States of America: Perseus Books, 1998).

Cameron, David. "Walk this Way." *Technology Review: MIT's Magazine of Innovation.* (23 April 2002). Retrieved February 5, 2003 from http://www.technologyreview.com/articles/wo_cameron042302.asp.

"Candid Cameras for Criminals." *BBC News*, (13 October 1998), 1. Retrieved April 18, 2003 from http://news.bbc.co.uk/2/hi/uk_news/191692.stm.

Colatosti, Thomas. "Viisage Deploying Face Recognition System for Illinois." (7 May, 1999) Retrieved April 19, 2003 from http://www.viisage.com/May7_1999.htm.

Daugman, John. "Anatomy and Physiology of the Iris." (n.d.) Retrieved April 18, 2003 from http://www.cl.cam.ac.uk/users/jgd1000/anatomy.html.

Daugman, John. "How Iris Recognition Works." (Cambridge: University of Cambridge, the Computer Laboratory) Retrieved April 18, 2003 from www.cl.cam.ac.uk/users/jgd1000/irisrecog.pdf.

Daugman, John. "How the Afghan Girl Was Identified by Her Iris Pattern." Retrieved April

18, 2003 from http://www.cl.cam.ac.uk/users/jdg1000/Afghan.html.

DeCew, Judith Wagner. *In Pursuit of Privacy: Law, Ethics and the Rise of Technology.* (Ithaca: Cornell University Press, 1997).

Denning, Dorothy. “Why I Love Biometrics: It is Liveness, Not Secrecy, that Counts.” *InfoSecurityMagazine.com,* (January 2001). Retrieved April 18, 2003 from http://www.infosecuritymag.com/articles/january01/columns_logoff.shtml.

“DNA dog tag or genetic ID?”, (n.d.) *Time* (22 June 1992), v139, n25, 35, Accessed through Expanded Academic ASAP April 18, 2003.

Duggan, Timothy. “The Privacy of Experience.” *Philosophical Quarterly* 13 Issue 51 (April 1963): 134-142.

Dyson, Esther. *Release 2.1: A Design for Living in the Digital Age.* (New York: Broadway Books, a division of Bantam Doubleday Dell Publishing Group, Inc., 1998).

Etzioni, Amitai. *The Limits of Privacy*. (New York: Basic Books, 1999).

Face Detection Home Page: Techniques, (n.d.) Retrieved April 18, 2003 from http://home.t-online.de/home/Robert.Frischholz/facedetection/techniques.htm

Facial Recognition Technology, (n.d.), Retrieved April 18, 2003 from http://www.identix.com/newsroom/lfa.html

Farmer, Dan and Charles C. Mann. “Surveillance Nation.” *Technology Review: MIT’s Magazine of Innovation.* 106 no. 3 (April 2003): 36-43.

Foucault, Michael. *Discipline & Punish: The Birth of the Prison.* Trans. Alan Sheridan. (New York: Random House, Inc., 1978).

Foucault, Michael. *Management and Organization Theory*. Ed. Alan McKinlay and Ken Starkey. (London: SAGE Publications Ltd., 1998).

Foucault, Michael. *Power and Knowledge: Selected Interviews and Other Writings.* Ed. Colin Gordon. (New York: Random House Inc., 1972).

Fried, Charles. *An Anatomy of Values: Problems of Personal and Social Choice.* (Cambridge, MA: Harvard University Press, 1970).

Fried, Charles. “Privacy [a legal analysis].” *Philosophical Dimensions of Privacy: An Anthology*. Ed. Ferdinand Schoeman. (Cambridge: Cambridge University Press, 1984).

Gandy, Oscar H. Jr.. “Exploring Identity and Identification in Cyberspace.” *Notre Dame Journal of Law, Ethics, & Public Policy* 14 no. 2 (2000): 1085-111.

Gandy, Oscar H. Jr.. *The Panoptic Sort: A Political Economy of Personal Information.* (Boulder: Westview Press Inc., 1993).

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

Gavison, Ruth. “Privacy and the Limits of the Law.” *Philosophical Dimensions of Privacy: An Anthology*. Ed. Ferdinand Schoeman. (Cambridge: Cambridge University Press, 1984). 346-402.

Godoy, Maria. “Smile, You’re Being Facially Frisked.” *Techlive,* (7 August 2001). http://www.techtv.com/news/culture/story/0,24195,3340850,00.html.

Goffman, Erving. *Stigma: Notes on the Management of Spoiled Identity.* (New York: Simon & Schuster, Inc., 1963).

Hartner, John. *Washington County: Oregon: Residential Services.* (25 July 2002) Retrieved April 18, 2003 from http://www.co.washington.or.us/deptmts/comm_cor/resident.htm.

Human ID at CMU, (n.d.), Retrieved April 21, 2003 from http://www.hid.ri.cmu.edu.

Human ID at a Distance (HumanID), (n.d.), Retrieved April 21, 2003 from http://www.darpa.mil/iao/HID.htm.

Human ID @ MIT AI Lab, (n.d.), Retrieved April 21, 2003 from http://www.ai.mit.edu/people/llee/HID/intro.htm.

Identix Delivers ATM/POS Biometric Fingerprint Scanning Application to Reynosa, Mexico. (n.d.) Referenced April 18, 2003, from http://www.netlinkaccess.com/wsimages/biometric.pdf.

Individual Biometrics – Fingerprint. (n.d.) Retrieved April 18, 2003, from http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html.

Iris Recognition in Action, (n.d.), Retrieved April 18, 2003 from http://www.iris-scan.com/iris_recognition_applications.htm.

Irsay, Steve. “Surveillance Cameras Play Increasing Role as Investigation Tool.” *CNN.com*. 2.

Jarvis, Angela. “Are Privacy Rights of Citizens Being Eroded Wholesale.” Retrieved April 18, 2003 from http://www.forensic-evidence.com/site/ID/facialrecog.html.

Jennings, Charles and Lori Fena. *The Hundredth Window*. (New York: The Free Press, A division of Simon & Schuster, Inc., 2000).

Katz vs. U.S., 373 U.S. 427 (1963).

Kluger, Jeffery, “DNA Detectives: Genetic fingerprinting is already being used to identify criminals. Can the rest of us be far behind?”, *Time* (11 January 1999), v153, 62.

Kundera, Milan. *Testaments Betrayed: An Essay in Nine Parts*. Trans. Linda Asher. (New York: Harper Collins Publishers, 1995).

Locke, John. *Two Treatises of Government.* Ed. Peter Laslett. (Cambridge: Cambridge University Press, 1988).

Matsumoto, Tsutomu, Hiroyuki Matsumoto, Koji Yamad and Satoshi Hoshino. “Impact of Artificial ‘Gummy’ Fingers on Fingerprint Systems.” *The Proceedings of SPIE (The International Society for Optical Engineering) Vol#4677: Optical Security and Counterfeit Deterrence Techniques IV held in San Jose, CA 24-25 January 2002*., 11.

McCullagh, Declan. “Cal It Super Bowl Face Scan.” *WiredNews* (2 February 2001), Retrieved April 21, 2003 from http://www.wired.com/news/politics/0,1283,41571,00.html.

Mill, John Stuart. *On Liberty and Other Writings*. Ed. Stefan Collini. (Cambridge: Cambridge University Press, 1989).

Miller, Ben. “Applications of Biometric Technologies” at the *Biometric Consortium Conference held in Washington D.C. on 23-25 September 2002.*

“Mom: No Excuse for Striking Child,” *CNN.com* (n.d.), (23 September 2002), Retrieved 10 April 2003 form http://www.cnn.com/2002/US/Midwest/09/23/tuchman.toogood.cnna/.

Monmonier, Mark. *Spying with Maps: Surveillance Technologies and The Future of Privacy*. (Chicago: The University of Chicago Press, 2002).

Murphy, Dean E.. “As Security Cameras Sprout, Someone’s Always Watching.” *The New York Times* (29 September 2002) 33.

Nanavati, Samir, Michael Thieme and Raj Nanavati. *Biometrics: Identity Verification in a Networked World*. (New York: John Wiley & Sons Inc., 2002).

Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy: An International Journal for Jurisprudence and Legal Philosophy.* 17 nos. 5-6 (November 1998): 559-596.

Oxford English Dictionary, 2nd ed., (1989).

Pentland, Alex and Choudhury Tanzeen. "Personalizing Smart Environments: Face Recognition for Human Interaction." (Cambridge, MA: The Media Laboratory, MIT) January 21, 2000. Retrieved April 18, 2003 from h ttp://vismod.www.media.mit.edu/tech-reports/TR-516/ieee_computer.html.

Peters, Ted. *Genetics: Issues of Social Justice.* (Cleveland, The Pilgrim Press, 1998).

Privacy Policy: Stop and Shop. (n.d.). Retrieved April 20, 2003 from http://www.stopandshop.com/card/policy.htm.

Rachels, James. "Why Privacy is Important." *Philosophy & Public Affairs Quarterly* 4 no. 4 (Summer 1975): 323-333.

Rieman, Jeffrey H.. "Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future." *Santa Clara Computer and High Technology Law Journal*. 11 (March 1995): 27-43.

Rieman, Jeffrey H.. "Privacy, Intimacy and Personhood." *Philosophy and Public Affairs* 6 Issue 1 (Autumn, 1976): 26-44.

Roberts, Paul. "Visa Gets Behind Voice Recognition." PCWorld.com. (21 October 2002) Retrieved April 18, 2003 from http://www.pcworld.com/news/article/0,aid,106142,00.asp.

Robison, Wade. "Privacy and Personal Identity." *Ethics and Bevahior*7(3) (1997): 195-205.

Rosen, Jeffrey. "Being Watched: A Cautionary Tale for a New Age of Surveillance." *New York Times Magazine.* (7 October 2001). Retrieved February 2, 2003 from http://www.globalpolicy.org/wtc/liberties/surveillance.htm.

Rosen, Jeffrey. *The Unwanted Gaze: The Destruction of Privacy in America.* (New York: Random House, Inc., 2001).

Rowley, Henry, Shumeet Baluja and Takeo Kanade. "Human Face Detection in Visual Scenes." *CMU-CS-95-158R* (November 1995).

Russel, Peter J.. *Genetics*. (San Francisco: Pearson Education, Inc., 2002).

Scanlon, Thomas. "Thomson on Privacy." *Philosophy & Public Affairs Quarterly* 4 no. 4 (Summer 1975): 315-322.

Scasny, Randy. "Veritel Introduces Voice Security Verification." *Internet News.com.* (15 November 2000) Retrieved April 18, 2003 from http://www.internetnews.com/bus-news/article.php/5401_512471.

"Schiphol Backs Eye Scan Security," *CNN.com*, (27 March 2001). Retrieved April 18, 2003 from http://www.cnn.com/2002/WORLD/europe/03/27/schiphol.security/index.html.

Schneier, Bruce. "Biometrics: Uses and Abuses." *Communications of the ACM* Vol 42, N8. August 1999.

Segan, Sascha. "Finger Food: Fingerprint Scans Replace Lunch Money in Pennsylvania." *ABCNews.com*. 18 January 2001.

Smith, Robert Ellis. *Ben Franklin's Web Site: Privacy and Curiosity from Plymouth*

Rock to the Internet. (United States of America: Sheridan Books, 2000).

Sykes, Charles J.. *The End of Privacy*. (New York: St. Martins Press, 1999).

Thomson, Judith Jarvis. "The Right to Privacy." *Philosophy & Public Affairs* 4 no. 4 (Summer 1975): 295-314.

Tunick, Mark. "Privacy in the Face of New Technologies of Surveillance." *Public Affairs Quarterly* 14 no.3 (July 2000): 259-277.

Vocent Press Release, 9 December 2002, Retrieved April 18, 2003 from http://www.vocent.com/pr0018.html.

Walk the Walk: Gait Recognition Technology Could Identify Humans at a Distance, (11 October 2000), Retrieved April 18, 2003 from gtresearchnews.gatech.edu/newsrelease/GAIT.htm

Warren, Samuel D., and Louis D. Brandeis. "The Right to Privacy." *The Harvard Law Review* 4 no.5 (15 December 1890): 192-200.

"West Virginia Becomes First State to Issue Driver's Licenses Using Facial Recognition," *Polaroid Inc. Press Releases*, (24 March 1998). Retrieved April 1 8, 2003 from http://www.primarypdc.com/press/98/march/032598a.html.

Westin, Alan. *Privacy and Freedom*. (New York: The Association of the Bar of the City of New York, 1967).

Whitaker, Reg. *The End Of Privacy: How Total Surveillance is Becoming a Reality*. (New York: The New Press, 1999).

Williams, Raymond. *Keywords: A Vocabulary of Culture and Society*. (New York: Oxford University Press, 1976).

Woodward, John D.. "Searching the FBI's Civil Files: Public Safety v. Civil Liberty. *Privacy and Security Law* 1 no. 35 (2 September 2002): 1042-1051.

Woodward, John D., Nicholas M. Orlans and Peter T. Higgins. *Biometrics: Identity Assurance in the Information Age*. (Berkeley: McGraw-Hill Companies, 2003).