THE TECHNOLOGICAL ASSAULT ON ANONYMITY

by

VANCE MICHAEL LOCKTON

B.Math., The University of Waterloo, 2003

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

THE FACULTY OF GRADUATE STUDIES

(Computer Science)

THE UNIVERSITY OF BRITISH COLUMBIA

October 2005

ABSTRACT

Anonymity, the state of being nameless, is a very divisive issue. On the one hand, criminals frequently attempt to hide their identities during the commission of crimes; because this is the use that is best understood, many people view this state as a negative status which needs to be eliminated. Others though, including many lawmakers and psychologists, have recognized that anonymity is a necessary feature of both a democratic society and of general mental well-being. However, regardless of one's opinion of this state, it must be admitted that technological advances are threatening to eliminate one's ability to be anonymous. As closed-circuit television (CCTV) cameras are installed by the thousand, radio frequency identification (RFID) tags are added to both ID cards and merchandise, and virtually all commercial transactions are recorded, very detailed pictures of people's lives are being created, and they may find fewer and fewer locations in which they are not identified. Even in the online world, where identity exploration and free access to knowledge abound, governments are applying pressures on service providers to allow constant access to users' true identities. This thesis will examine these technological threats to anonymity, as well as providing a detailed explanation of the reasons that anonymous action is a vital resource to the public. It will then conclude by surveying and critiquing the various means which have been suggested for the protection of this resource, and provide an explanation as to why legislation and education will provide the only ones which are truly effective.

TABLE OF CONTENTS

Dedications

The following people deserve more than an acknowledgement; they deserve a dedication.

To Richard Rosenberg, for inspiration and guidance.

To Sarah Cormier, for bringing me out of the shadows.

To Steve Wilson, for keeping me active.

To Wendy Foster, for conversation (and the bulking up of Chapter 6).

To (now-defunct) Bullpen 238, for a wonderful introduction to the school.

To the patrons and staff of Koerner's Pub, Little Albert's Nightmares, The Ballwhackers, a good part of the CS student body, etc., for entertainment.

And finally, and most importantly, to my parents, for the stability that has afforded me the confidence to take risks.

I thank you all (certainly for more than the things I've just mentioned), and dedicate this work to you.

Vance M. Lockton

1. Introduction

One cannot fail to notice the revolutionary effects that computer technology has had on society. During the scant 50 years in which the computer went from a multi-million dollar behemoth occupying entire floors of buildings to a microscopic technology incorporated into virtually all consumer electronics, the average person learned to depend on it to guide him or her through his or her daily activities. For example, cellular phones have made mobile, instant communication a reality, and the functionality and miniaturization provided by new chip sets has allowed them to become near-ubiquitous. In Japan, for instance, there are 88 million active cellular phone subscriptions ["Information", 2005] in a population of 127 million; this 69% ratio is small compared to Germany, which has 90% as many cell phones as inhabitants ["Quarterly", 2005], or Sweden, at just over 100% [LaRoche, 2004] (explained by some people having more than one phone). Also, great amounts of information have shed obscurity and become easily found in the massive world wide web; as the 'net grows, so do the number of people accessing it. 68% of the US population are Internet users, and over a billion people will be connected worldwide by the end of 2005. ["Worldwide", 2004] These people have come to know a world of instant gratification, in which the barriers of time and space have become obsolete.

However, there is a price to pay for the ultra-convenience provided by new technologies. Some traditional values have had to be discarded or modified in order to keep pace with such a society; the ethos of the early twentieth century simply has no place there. As such, some fundamental rights have been put at risk; not least among them is privacy. The standard label for modern times is 'The Information Age'; the 'right to be let alone' has become very difficult to ensure. In order to satiate the appetite for instant service, information must be complete and universally available: employers want to know exactly the location of, and have access to, their employees at all times; police agencies don't want to have to physically follow a suspect when a tracking tag can do the task just as well; and neighbourhoods want to know the complete histories of any and all newcomers before they arrive. Additionally, much media coverage has been reduced to 2-minute reports; the threat of terrorism plays much better on such a stage than a defense of privacy ever could. Thus, this right is being lost by the wayside, and the transformation of society continues unabated.

It should not be this way. A right, such as privacy, that has been enshrined in human societies for hundreds of years is there for a reason. If we lose it, we lose a fundamental piece of our freedom, for as it will be shown, privacy does not exist simply to shelter the wrongdoer; it also serves vital roles in physical and mental well-being. If privacy is under attack, it must be defended.

1.1. Purpose of Research

This thesis will examine the current assault on privacy, focusing on a specific sub-area: anonymity. Exact definitions will be given in the next chapter, but in essence, anonymity

is the state of being nameless, or unidentifiable. In most current works examining modern privacy, anonymity is given a passing mention; it seems to be either considered unimportant, or too difficult a notion to defend, as its uses and benefits tend to be poorly defined. Media accounts of new technologies will also often make at least brief mention of the 'potential privacy risks' associated with new technologies, but it is very infrequent that the word 'anonymity' will appear. The ability to choose namelessness, though nowhere sheltered as a 'right', deserves some form of protection, or at the very least, a publicized rationale: it is such a defense that this thesis will undertake.

Through an examination of the works of philosophers, psychologists and privacy analysts, a comprehensive overview of the pros and cons of anonymity will be developed. Coupled with this will be a description of the ways in which anonymity is threatened by modern technology, and of the way in which surveillance creates the largest such threat. A person being observed at all times has very little chance to slip into the shadows; modern surveillance technologies create such a scenario, intentionally or otherwise. Even some innocuous seeming technologies, such as radio-frequency identification, create great risks if used improperly; thus, a detailed overview of the potential abuses of that technology will be given, as an example of the unintentional function creep that can occur. Anonymity on the Internet will also be discussed; it is arguable that a truer form of anonymity can be found online than off, though the digital nature of the web makes it more fragile. Finally, suggestions for the ways in which anonymity can be protected will be examined; some will be discarded as ineffective, some as impractical, but others will be shown to be of vital importance in a successful resistance to the threats previously described.

This section ends with a mild admonition to the reader: please, understand not just the technological threats described, but also the reasons one would want to protect the ability to choose anonymity. Technologies will come and go, but human rights should be constant. Anonymity may not be a right, but as it is so strongly associated with privacy and essential to the functioning of a democracy, it should certainly not be relegated to the status of a privilege, available only to those who can pay for it.

2. Introduction to Anonymity

Anonymity is a very interesting issue to consider, given the polarization of viewpoints about its worth to society. At one end, many people consider it a menace. Physicist and novelist David Brin, for instance, has written that, "Almost by definition, anonymity is the darkness behind which most miscreants ... shelter in order to wreak harm, safe against discovery or redress by those they abuse." [Brin, 1998, p 215] It is certainly true that wrong-doers can, and do, attempt to prevent their identities being known; hence, they are exercising a form of anonymity for evil. At the opposite end of the spectrum, though, is a group that praises the value of namelessness, even in democratic (and thus theoretically accountable) societies. No less power than the Supreme Court of the United States has stated in an opinion that the power to speak anonymously is part of "an honourable tradition of advocacy and of dissent." [McIntyre v. Ohio Elections Commission, 1995] Neither of these opinions is necessarily 'wrong'; in fact, both are quite valid. This thesis, though, will attempt to show that the benefits gained from allowing anonymous interactions in both the on- and offline realms outweigh the dangers inherent in such a practice. However, before such a case has been made, we must describe what precisely is meant by the word 'anonymity', and the related term 'privacy.'

Both Webster's Dictionary and the Greek roots of the word itself define anonymity to be the state of being nameless, or having an unknown name. However, this is not a satisfying definition for our purposes; simple namelessness is not enough. Anonymity is a matter of degree; one need not know a person's name to be able to identify him or her. Features such as manner of speech, physical marks (such as tattoos or scars), IP address, or phone number can be associated with an individual; the name is the most obvious means of indexing a particular person, but it is certainly not the only one. For our purposes, we must consider a more technical definition of the term 'name': i.e. "a word or words by which an entity is designated and distinguished from others." [American Heritage Dictionary, 2000] It is only by being nameless is this technical sense that one can truly feel protected, should it be anonymity that is desired. Thus, the definition of anonymity which shall be used reads as follows: anonymity is the state of being free of unique features that can be traced back to one's person, at least to the extent that the difficulty of such a trace makes it practically impossible. For instance, if Person X was described as 'over 6 feet tall, with brown hair', that person is still anonymous, as tens of thousands of people match that description. However, if Person Y was identified to be "over 6 feet, with brown hair, traveling on Robson Street at 2:30pm, carrying a briefcase", his or her anonymity is highly in question, as it is likely only a handful of people could fit that report. If that person is then seen getting into his or her car, and the license plate number noted, then his or her anonymity is completely violated, even though his or her 'name' (the common usage) is still unknown.

Privacy, too often considered to be nearly synonymous with anonymity, means something entirely different. Privacy can be "the state of being free from unsanctioned intrusion," "the quality or condition of being secluded from the presence or view of others," or simply "the state of being concealed." [American Heritage Dictionary, 2000] Thus, the person in the scenario given above has had his or her privacy violated simply

by the fact of his or her observation; in fact, virtually any time one chooses to interact with the outside world, his or her privacy is compromised, by these definitions. This is not a useful definition for our purposes, as any methods for 'protection of privacy' would in that case involve closing all the doors and curtains in one's home and severing any means of communication. Thus, we will turn to the oft-cited article "The Right to Privacy", published in 1890 by Judges Samuel Warren and Louis Brandeis for our definition. According to them, the right to privacy is simply "the right to be let alone" [Warren & Brandeis, 1890]; a person can be observed, followed, even have his or personal information recorded, but so long as that information is never used in a way that affects the person in question, his or her privacy has not been violated. This is still a contentious definition (for instance, does the near-certain use of collected information mean that the collection itself is a privacy violation?), but as it is widely used in the legal community, as well as within the general public, it will serve as the meaning of the term 'privacy' within this paper.

Thus, we have seen that privacy and anonymity are not the same thing; or, at least are not working towards the same goal. A completely isolated individual is private but not anonymous, whereas a person in Times Square is likely to be exactly the opposite. Furthermore, a person who wishes to expose some corporate wrongdoing will have much more effect if he or she speaks loudly yet anonymously than if he or she were to maintain privacy whilst speaking quietly, or not at all. However, there certainly is an association between the two states; to examine their relationship we turn to Alan Westin's landmark 1967 work, *Privacy and Freedom.*

2.1. The Four States of Privacy

Westin defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." [Westin, 1970] The choice of whether or not to have one's identity known when interacting with others is certainly a large factor in this definition of privacy; thus, clearly for Westin the ability to be anonymous is an important factor in protecting privacy. It is not the only one, though. He identifies four states of privacy, which we shall now examine: solitude, intimacy, anonymity, and reserve. [Westin, 1970]

2.1.1. Solitude

The state of solitude is one in which the individual is completely separated from all potential observers; he or she is completely alone. No other person is present to examine the individual's actions and choices, though neither can he or she affect those of anyone else. Although there is no one else present to disturb the individual's peace of mind, that peace may still not be complete; the person may feel judged by some omnipotent higher power, or be disturbed by usually minor physical irritations, such as cold, heat, or itching. Also, this is the state in which a person will most likely find him- or herself most immersed in internal dialogue with the conscience. However, in spite of these psychic intrusions, this is the most complete form of privacy.

2.1.2. Intimacy

In the state of intimacy, privacy does not encompass the individual; rather, it includes a small group of people. This group is allowed to exercise various exclusionary practices in order to form a 'close, relaxed and frank relationship' between two or more individuals. It is taken for granted that any 'secrets' exposed within this group setting will not be exposed to non-members; in this way, trust is formed. Typical instances of this state include marriage, family and working groups: groups which must share a very detailed knowledge base in order to function effectively. This form of close contact may be relaxed or it may be abrasive, depending on the nature of the individuals involved; however, without being able to form such close bonds of trust, the basic human need for contact could not be fulfilled.

2.1.3. Anonymity

The third state of privacy is anonymity; this is the state which occurs when an individual seeks, and finds, freedom from identification and surveillance when in a public forum, or while performing public acts. This person knows he or she is in public and under the observation of others, but does not expect to be personally identified and thus held to the full rules of behaviour and role that he or she would be otherwise. Garrison Keillor, for instance, has described the pleasure that he felt in visiting New York City as a young man, being able to walk the streets unknown and unnoted by anyone, a very liberating feeling for a man from a small town in which everyone knew everybody else, and thus (through the lines of gossip) also knew every action of every other person. [Brin, 1998] The state of anonymity affords such contentment; as Westin claims, "knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas." [Westin, 1970]

An interesting occurrence that happens in the state of anonymity is the "phenomenon of the stranger," as named by psychologist Georg Simmel. He observed that unknown persons often received "the most surprising openness – confidences which ... would be carefully withheld from a more closely related person." [Westin, 1970] An individual may turn to a stranger for aid during times of psychological crisis for the simple fact that he or she is a stranger, and thus will not continue on in the individual's life. The stranger may provide simply an ear for a person needing to verbally work out solutions to his or her problems, or may be able to provide some measure of objective advice; however, since he or she will be able to exert no authority over the individual, such a confessional session will have few or no repercussions. Thus, the state of anonymity can allow for psychic relief.

2.1.4. Reserve

The final and most subtle state of privacy is reserve: the creation of a psychological barrier against unwanted intrusion. In even the most intimate of relationships, there is the need to hold some part of one's self back as either too personal and sacred, or shameful and profane, for revelation; it is assumed that only an antagonistic person would

aggressively attempt to break down this barrier. This choice to withhold or disclose information is the dynamic aspect of privacy in everyday relations; the ways in which an individual claims reserve and the extent to which it is respected varies greatly from society to society, but remains at the heart of securing meaningful privacy in the modern world. [Westin, 1970]

Most of a person's life is spent not in solitude or anonymity, but in reserve and intimacy. The former pair are states which must be actively sought; to be in solitude one must seek an inviolable sanctuary, a difficult task in the crowded modern world, while to be anonymous a person must seek out either a means of concealing his or her identity or an area in which he or she is not known, potentially a problematic undertaking in a close-knit community for example, and virtually impossible within the home. Reserve and intimacy, though, occur when one is with associates, friends or family members, and relate simply to the amount of disclosure of personal information to others. Most of our lives are spent in situations in which we are known by those around us; it is difficult to keep one's actions private in these circumstances, but one's thoughts and feelings can, and frequently must, be kept internal.

2.2. The Functions of Privacy

Too often statements such as "Giving up privacy will only affect those who have something to hide" are used to justify intrusions into the private lives of individuals. This is simply not true. Privacy does not just hide misdeeds; it also helps to develop and maintain the psychic health of the individual. There are at least four main psychological functions served by privacy: personal autonomy, emotional release, self-evaluation, and limited and protected communication. [Westin, 1970] Before we consider the specific benefits of anonymity, these functions will be examined in order to show the ways in which the four states of privacy can be utilized for psychic well-being.

2.2.1. Personal Autonomy

It is taken for granted in democratic societies that every individual is in some way unique; it is this uniqueness that allots him or her the basic rights and dignities afforded to all members of the human race. This desire for individuality has been attributed to the basic need for autonomy; a desire to avoid being completely controlled or manipulated by some other person or group of people. [Westin, 1970] Thus, an attack on the autonomy of the individual is in essence an attack on his or her innate humanness.

In order to protect against such incursions, various theorists have suggested that individuals tend to interact with others in term of 'zones': protective layers which surround the 'core self.' [Westin, 1970] The outermost zones consist of innocuous information made available during all interactions; items accessible in these zones are considered so harmless to the individual that they can be freely shared. Middle zones are seen by acquaintances; these contain slightly more personal information, but no secrets which can be used against the individual. The innermost layers are saved for intimate secrets, freely given to close companions, family, and in some instances strangers who

hold no power over the individual. The core zone, though, is accessible by no-one, except in times of extraordinary stress during which the individual must give up his or her most personal information in order to achieve relief. The most serious threat to personal autonomy is a breach of the core zone, whether by the application of physical or psychological pressures; once an invader has learned the secrets of a person's core self, he or she is in complete control of that individual. [Westin, 1970] Thus, the adoption of some degree of privacy (in particular, a measure of reserve) in all interactions with others is an absolute necessity; the risks of doing otherwise, particularly to autonomy, are simply too great.

Privacy does not only guard against psychic invasions, though. It is also a key aspect in the development of the individual. Historian Robert MacIver has written that, "Everything that grows does so in the darkness before it sends its shoots out into the light." [Westin, 1970] The human psyche is certainly no exception. Every person lives behind a mask; externally, he or she is a role player, interacting with society in the manner expected of him or her. However, behind the mask is a turmoil of desired traits to be chased and not yet understood aspects with which to be experimented. Unexpected psychological reactions to various situations may make a person question his or her true self, and a drive to succeed may push him or her towards development of self-determined 'better' qualities. However, the fragility of these changes means that the person must maintain the choice of when to reveal his or her new self to the outside world. If the mask is torn off prematurely, the individual will believe him- or herself to be naked in a society of the clothed (masked), and he or she could be destroyed by that level of exposure. Thus, the allowance of anonymous experimentation becomes a key factor in the development of an individual's psyche, and as such his or her distinctiveness and autonomy.

Moments of solitude are also vital to a person's development. Social worker Leontine Young has written, "Without privacy there is no individuality. There are only types. Who can know what he thinks and feels if he never has the opportunity to be alone with his thoughts and feelings?" [Westin, 1970] Periods of reflection allow the individual to break away from what he or she is told to think or feel, and examine what he or she truly believes. This is a very important procedure for a democratic society, in which independent thought, diversity of ideas and non-conformity are (or at least should be) considered desirable. Privacy and solitude allow an individual to critically examine and evaluate his or her notions of society, and fine tune them before making them public. In this way the ideas are made stronger, and a person is allowed to avoid the potential ridicule associated with the espousing of premature thoughts.

2.2.2. Emotional Release

In the fast-paced, high-tension modern world, individuals are often in need of emotional release. Whether this takes the form relaxation from role-playing, the venting of anger, or occasional non-compliance with social norms, a modicum of privacy ensures that this release can be effectively free of consequence.

As will be discussed further in section 6, *Internet Anonymity*, current society expects an individual to play roles; for instance, a single person can be expected to shift from the role of manager to that of father to husband to pub wise-guy, etc, all in the course of a single day. Each group that an individual interacts with is likely to have an expectation about his or her behaviour; it would be emotionally exhausting to always have to shape one's behaviour in a different expected manner depending on the situation. Thus, individuals seek periods of respite from role-playing, be that by immersing one's self in solitude or by utilizing the anonymity provide in a large crowd. Allowing a person periods in which he or she does not have to be 'on' does wonders for his or her physical and psychological health.

Very closely associated with the above idea is the notion that people need some occasional relief from social norms. Following every rule of law and etiquette demands a great amount of mental energy from a person; again, to not be allowed some minor break from this would leave a person drained and weakened. Thus, virtually all societies allow some minor transgressions to pass unnoticed. It is privacy that allows this overlooking of 'permissible' offenses to occur. In solitude or intimacy, a person is allowed to break most social mores; walk around naked, scratch itches, curse – the individual is allowed to 'not care' for a short period. Anonymity allows people to act publicly without considering the consequences: to jay-walk, break speed laws, or even to wear clothes usually considered inappropriate to one's position can be refreshing. However, should every person's actions be monitored at all times, these indiscretions could not be ignored; a record of these events would force either the change of social customs or more likely, the punishment of virtually everyone. The results of such a society can be seen in Orwell's *Nineteen Eighty-Four*, which will be considered in the next chapter.

Finally, every person needs to let off steam at some point. Many psychologists say that pent-up anger is harmful to psychological health; thus, it is good to have some safe form of release. Private moments in which a person can rage against the world are quite therapeutic. The commentaries that may be given are often unfair, biased, frivolous, and libelous, but are not intended to be aired in a public forum. Freedom of speech does not protect such outbursts nearly as well as solitude or intimacy.

2.2.3. Self-Evaluation

The amount of information flowing past a person at nearly all times of the day is frequently over-whelming; it simply cannot all be immediately processed. Alan Bates has written that, "Privacy allows an individual to assess the flood of information received, to consider alternatives and possible consequences so that he may then act as consistently and appropriately as possible." [Westin, 1970, p 36] These periods of reprieve are not used solely for evaluation, however. Studies have shown that most 'non-verbal' (i.e. creative) thought takes place during moments of reflective solitude or while 'daydreaming' in moments of reserve. [Westin, 1970] The presence of others, and the individual's awareness of them, tends to stifle abstract thought, as immediate demands of social custom and fear of the derision of ideas that are not fully formed tend to focus a person on the concrete.

There is also a moral value to moments of self-reflection. An individual will tend to take matters of morality into account when making decisions throughout the day, but it is only during periods of rest that that person is allowed to evaluate the overall moral path down which he or she is traveling. [Westin, 1970] Religions have long recognized this fact and introduced the concept of the 'religious retreat'; a time during which the individual is allowed to scrutinize his or her actions and reconnect with a higher power. Even a non-spiritual person needs time to make peace, be it with their family, the world or themselves. Privacy allows moments of tranquility, in solitude or in public; it is the feeling of observation which makes a person aware of the self, and thus awakes him or her from his or her reverie.

2.2.4. Limited and Protected Communication

The final function of privacy which will be considered is limited and protected communication. In the words of Westin, "The greatest threat to civilized social life would be a situation in which each individual was utterly candid ... saying exactly what he knew or felt at all times." [Westin, 1970] This seems like an obvious statement about a situation which will never occur; the necessity of 'biting one's tongue' on occasion is clear. However, as privacy is eroded, the need to be candid will increase, for one will be more likely to be caught in his or her 'little white lies.' Civilized discourse depends on one's ability to carefully select which thoughts will be voiced, and which dismissed; without some manner of reserve, this is not possible. If a person is led to believe that he or she is under intense surveillance, then he or she has little reason to self-censor, having assumed that the conversational partner can infer his or her thoughts anyway.

Limited communication also serves to establish and maintain hierarchical structures. In work situations, for instance, it is vital that the superior keep a degree of mental distance between him- or herself and his or her subordinates. The power relationship depends on a lack of intimacy between levels. Should a manager open his soul to his or her employee, his or her power is diminished. Should the employee become too intimate, the manager gains influence. Similar distance must be kept between professor and student, parent and child, and in many other relationships. In general, the superior in each situation is allowed an area of solitude, in order to prevent constant surveillance, and the subordinate is afforded a measure of unquestioned mental reserve, in order to facilitate a functional relationship.

The psychological functions described above provide a strong foundation for a defense of the right to privacy; however, there are much more tangible and immediate benefits that are also provided. In the next section, we examine some current and historical uses for anonymity, in hopes that the reader will recognize precisely what freedoms are threatened by the technologies to be described in future chapters.

2.3. Historical Usages of Anonymity

The history of anonymity is very rich with stories of political commentators and satirists who chose to utilize the measure of safety provided by publishing their works anonymously. In 1532, for instance, Francois Rabelais began his political and social satire *Chronicles of the Giant Gargantua*, publishing the first book of the series anonymously; two years later, the second was distributed in the same manner. Though these were criticized by the Sorbonne (the theological department of the University of Paris) as being 'obscene' [Wallace & Green, 1999], it was not until the third book, written in 1546, that he needed the protections afforded him. That book was labeled 'heretical'; Calvin, the Protestant leader, wrote of the book:

> "[These writers are] curs who assume the attitudes of comedy to enjoy greater freedom to vomit their blasphemies. They revel in banquets and they haunt libertine company where, speaking at pleasure, they leave no stone unturned in destroying all fear of God in the minds of their hearers." [Wallace & Green, 1999]

These books are now celebrated in France as brilliant works of comedy; however, had Rabelais associated his name with them at the time, it is unlikely that he would have been allowed (or even left alive) to write past the first volume. He had good reason to be fearful of the consequences of publishing these works: his colleague, Etienne Dolet, was hanged and burned for publishing a dialogue by Plato which questioned the existence of the immortal soul. [Wallace & Green, 1999] However, he saw the necessity of exposing the public to his ideas; thus, he chose the option of anonymity.

Protection of the author was certainly not the only function served by anonymous publication. When Thomas Paine wrote the landmark treatise *Common Sense* in January 1776, denouncing British rule of America, he signed it, simply, "Written by an Englishman." This pamphlet was extraordinarily popular, selling an estimated 600 000 copies to a population of just over 3 million. ["Common Sense", 2005] Naturally, many people began questioning the author's identity. In response, Paine replaced his original by-line with "an admonition to cease worrying about the author's identity and attend to what he had to say." [Wallace & Green, 1999] He explained by saying that the author was unconnected to any party nor under any influence other than that of reason and principle, and thus his name need not be known. It was not that Paine feared that revelation of his identity would cause him harm; rather, he insisted that opponents attack his ideas, rather than their author. Anonymity, in this case, protected intelligent public discourse, by preventing it from dissolving into a series of personal attacks.

Paine's publication sparked a flood of anonymous publications in the United States. At a time of revolution, many people wished their voices to be heard, but many feared speaking up. Again, this was not an unjustified fear: Benjamin Franklin's brother was jailed for insinuating in his newspaper that the government was not doing enough to protect against coastal pirates, and New York Assembleyman Samuel Mulford was expelled for suggesting that other members of the Assembly were corrupt. Loss of life, liberty or property was not uncommon for those expressing unpopular points of view, and as such, anonymous publication became an important means of expression. Perhaps the most famous of these writings was the Federalist Papers, eventually discovered to be the work of Alexander Hamilton, John Jay and James Madison. These Papers were vital to

the formation of the American Constitution; in fact, the Supreme Court has been known to refer to them when trying to interpret the meanings of various Constitutional passages. [Wallace & Green, 1999]

The tradition of publishing anonymous works has not stopped in recent times, as many writers continue to use the practice to publish information with which for some reason or other they do not wish to be associated. The details of the various incidents may differ, but the foundation remains constant: a person who feels the need to publish some unpopular or dangerous idea but (often rightfully) fears the consequences of doing so turns to namelessness for the necessary combination of protection of the self and exposure of the idea.

The written word is not the only thing that needs the protection afforded by anonymity, however. There are many actions which are made easier or safer knowing that one's identity will not be associated with them. For instance, many medical clinics offer anonymous HIV/AIDS testing. This is done by simply giving the patient a reference number to be used to access the results of the test; no identification is ever asked, and confidentiality is assured. With the exception of recognition by a receptionist or doctor, there is no way for that reference number to be associated with the person being tested. This handling of a delicate procedure is very important. In North America, AIDS still carries a stigma; simply being tested can lead to community judgments of a person's lifestyle and raise questions about the safety of being around that person. However, a person who is tested regularly has a higher chance of survival should they contract the disease (as it will be caught in the potentially treatable early phases), as well as know that they must take precautions to avoid infecting others upon a positive test. An anonymous testing centre is far more likely to be used than, say, the clearly labeled 'Sexually Transmitted Disease Clinic" on 12th Avenue (655 W. 12th) in Vancouver. There is much reason to be tested, but also much reason to not want to have one's identity associated with that test. Anonymity provides such an opportunity.

A person may have far more to hide than the fact that they are having medical tests done, though. Victims of crimes, particularly sexual assaults, are frequently so frightened of their attackers that they refuse to report it. If the crime was to be reported, and the accuser's name publicized, that person would be at great danger of a repeat offense until the accused was arrested. Thus, in many countries worldwide victims of sexual assaults have the right to remain anonymous until a formal arrest is made, and at rare occasions even throughout the trial.

In the past, Britain has extended this anonymity even further: to the accused. They recognized that "potentially innocent defendants needed to be protected from the social stigma of a rape allegation, which often remained for life, notwithstanding an acquittal." [Sexual Offenses Bill, 2003] This is particularly true for allegations involving children: it was found that 5-7% of those arrested for child abuse related offenses committed suicide, likely due largely in part to the impossibility of erasing such a charge from one's public reputation. Also, it was noted, providing anonymity for the complainant was likely to lead to an increase in false reports; the devastating nature of the simple accusation of a

sexual crime demands that blatantly untrue allegations should never have names associated with them. [Sexual Offences Bill, 2003] Thus, anonymity for the accused, for the period between the allegation and an actual charge being laid, was seen as a fair compromise between the journalistic need for free reporting, and fairness for those not yet charged with any crime. This provision was adopted in 1976, removed in 1988, and again suggested (but not enacted) by Britain's House of Lords in 2002.

The First Amendment to the US Constitution reads:

> "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; of abridging the freedom of speech, or of the press; or the right of the people to peaceably assemble, and to petition the government for a redress of grievances." [US Bill of Rights, 1791]

There is no better way than the allowance of anonymous action to guarantee that these rights are upheld. A tyrannical government which tried to overturn such rights would have a much more difficult time rounding up resistors if such a group were able to hide their identities; exposed, they would have to attempt to transmit their message before being captured, or killed. Revolutions begin underground; it must be ensured that such an underground can exist.

Anonymity is used by protesters, revolutionaries, those who fear for their reputation, and those who fear for their lives. It has been an extraordinarily vital tool for many individuals throughout history; even the US Supreme Court has recognized this fact, noting in 1960 that, "It is plain that anonymity has sometimes been assumed for the most constructive purposes." [Brin, 1998] Privacy and anonymity are wholly necessary for a democratic society to exist, as well as for the general mental well-being of its citizens. This can be shown to be true in not only every human society, but among some animals as well.

2.4. Privacy and Anonymity: A Modern Concept?

In this author's experience, there are two main objections raised when trying to convince individuals of their need for privacy. The first is the idiomatic "If I've done nothing wrong, I've nothing to hide." As has been previously mentioned, though, privacy provides more than shelter for the guilty; it serves valuable psychological functions, as well as providing protection for those trying to change an unjust situation. The second objection, though, is not countered by these facts. It goes, "Privacy is a modern concept; people in small tribes or villages knew everything about one another. If they can survive without privacy, why can't we?" This is not an easy criticism to answer, but it can be done. We will now show that every civilization employed some form of privacy; perhaps more subtle than our own, but extant nonetheless. It will also be made known that a sense of privacy is not exclusively a human concept, but that it exists in the animal kingdom as well.

2.4.1. Privacy in the Animal Kingdom

Animal studies have shown that virtually all species seeks periods of individual seclusion or small-group intimacy: birds sing and monkeys screech in order to claim a territory as

their own; except during nesting, two robins will never be on the same branch; dairy cattle in the US space themselves to create individual intervals. [Westin, 1970] To violate this sense of privacy can have drastic results. In the mid-1950's, the deer population on an island off the coast of Maryland rose to around 300, a number that was higher than usual, but still wholly sustainable. The deer had more than enough food, and there was no sign of infection in any of the animals. However, between 1958 and 1959, nearly two-thirds of the deer died. The dead animals appeared to be in perfect health, and their diet was easily adequate for their needs: they seemed to have simply passed away. The only possible explanation was that the higher than usual population of the island had had an injurious effect on the animals; in effect, they were suffering from a lack of private space. Studies of the event agreed with this analysis, concluding that the crowding of the island had created metabolic stress in the animals, triggering an endocrine reaction that resulted in a sort of natural selection. Once the population returned to its usual levels, this reaction stopped. [Westin, 1970]

The need for privacy in animals is not as complex as it is for humans. In essence, it can be assumed that contacts with others produces a stress reaction; this reaction is mild, though, and generally has no effect on the animal. However, when the animal is constantly in the presence of others, particularly those not of its immediate herd, this reaction increases, potentially to fatal levels. Many animals are not solitary, and so are never 'alone', but generally there is a sense of those who are its 'intimates': the members of its herd, pack, family, etc. Privacy is thus related to a sense of security; assuming no harm will come from one's intimates, the stress brought on by fear (or aggression) will only occur in the presence of 'outsiders.'

Experiments into animals' need for personal (i.e. private) zones shows us that much higher populations can be sustained in an enclosure if the animals are allowed space to themselves. For instance, one experiment showed that the number of rats that can live in an open, quarter-acre pen is approximately 150, though the test-period would have allowed for the females to produce 50 000 offspring. However, if the rats are allowed individual 2 square foot cages, 5000 can survive. If the cages are 8 square inches, the population stabilizes at about 50 000. Thus, the affording of space to each rat increased the potential population over 300-fold. One cannot push these boundaries too far, though. Should too many rats be crowded into a cage, their social hierarchies are destroyed. Patterns of courting are disrupted, aggression increases, and sexual conduct becomes sadistic. [Westin, 1970] Thus, it seems clear that rats value a sense of private space.

The reactions of these animals should not be surprising. In the human world, it is stressful to be in the constant presence of others, with the possible exception of one's intimates. However, section off areas into 'private zones' and individuals can be calm. This is the principle behind office cubicles, and to some extent apartment buildings. The same number of individuals would be unlikely to be able to live or work together in a completely open environment; humans, much like animals, need time and space to be alone. Again, privacy is not just useful for those with something to hide; the desire to be

alone is a biological one upon which governments and corporations intrude at their own risk.

2.4.2. Privacy in Primitive Societies

In examining the role of privacy in primitive societies, we must be sure not to simply compare its functionality to that seen in developed areas. North American privacy norms, for instance, are certainly not universal. In Margaret Mead's famous study of Samoan culture, for instance, she notes that there are no walls in the houses; rather, sleeping quarters are demarcated by mosquito netting. Adults wear little clothing, beaches are openly used as latrines, and intimate moments such as birth are publicly viewable; she claims, "There is no privacy and no sense of shame." [Westin, 1970] That statement is not entirely accurate, though. What Mead means is that North American standards of privacy do not exist, in that many natural functions do not occur 'behind closed doors.' However, is there still a sense of privacy felt by the Samoans? To answer that question, we will describe two other cultures, and the ways in which they understand privacy.

A paper by Clifford Geertz shows us two possible modes in which privacy can operate within Indonesian culture by comparing homes and openness in Bali and Java. [Westin, 1970] In Bali, privacy is very physical; homes are surrounded by high stone walls, and are entered through a narrow doorway. Except when invited, one never enters another's property; if an outsider wishes to see one of the residents, a child is sent to fetch that person. Inside the walls, one is free from the public eye, as only immediate family will be around one at any time. In Java, however, homes are not considered so sacred. Houses face the street with a clear yard in front; there are no walls, no fences and frequently no doors. People in the house freely enter almost any room at any time, and outsiders can enter freely during the day with only a brief announcement of their presence. Only the bathing enclosure, in which the Javanese change clothes, is considered a 'private' zone, and even that is open below the knees and above the shoulders. There are virtually no physical defenses against intrusion; however, there are many mental barricades. In the home of a Javanese family, relationships are very restrained, and rules of etiquette are enforced at all times; one may feel as if he or she is in a public square, and thus must uphold rules of decorum. Emotional restraint and a lack of candor are constant and immediately noticeable. The openness of the Javanese home does not imply that they do not care for privacy; rather, the social norms of that culture enforce it by psychological rather than physical means. In contrast, inside the very private, walled-off Balinese home, the atmosphere is of "a tremendous warmth, humour and openness." [Westin, 1970] Comforted by the fact that they are surrounded by only those to whom they have permitted access, residents do not feel a need for psychological barriers. However, once a Balinese individual leaves the safety of his or her home, he or she becomes nearly as reserved as the Javanese.

Thus, it is not safe to say that simply because a culture erects few physical barriers that they are willing for their lives to be laid open; psychological barriers are just as important for the preservation of privacy. Many primitive cultures directly recognize this fact by

forbidding the presence of outsiders at sacred rituals. Margaret Mead notes that this is likely because of an understanding that the allowance of spectators at the events would affect the psychological feelings of unity and belonging of the participants. [Westin, 1970] It is important to be able to remove one's mental barriers during these rituals in order to feel the true kinship of the others; outsider surveillance makes this impossible.

2.5. Summary

We have seen that a sense of privacy and anonymity is both a natural phenomenon and a universal one, spanning culture and time. The functions that they serve, both for psychological health and physical (and mental) security, are vital to one's well-being. In this light, the statement, "If you have done nothing wrong, you have nothing to hide" is clearly incorrect. Privacy and anonymity serve roles for all people, and attacks on them should not be tolerated.

In the next chapter, we look at the results of such assaults as foreseen by various authors, and the technological means that they believe are likely to be used by a corporation or government to violate an individual's right to privacy and anonymity.

3. Previous Examinations of Privacy's Role in Society

3.1. Jeremy Bentham's *Panopticon*

In 1791, philosopher Jeremy Bentham imagined a concept for a highly efficient prison: the Panopticon. Within it, cells would be arranged in a ring, all facing inwards towards a single guard tower. Prisoners could be seen from this tower, but they could not see into it (by elaborate use of Venetian blinds). In this way, the inmates would not know when they were being watched, or even how many guards there were; there could be hundreds, a dozen, or none. The important part is that the prisoners knew that there was a chance that at any time, they might be under observation. Ideally in a prison situation, Bentham believed, a person should be under the eye of his or her keeper at all times; this being impossible, he believed that, "the next thing to be wished for is, that, at every instant, seeing reason to believe [that he or she is being observed], and not being able to satisfy himself to the contrary, he should convince himself to be so." (Bentham, 1995)

This structure, though it was never built, was examined extensively as a theoretical topic in social control. Michel Foucault, in his work *Discipline & Punishment*, used the Panopticon as a metaphor for *all* modern disciplinary societies, including the army, schools, hospitals, and factories. The Panopticon destroyed the traditional seeing/being-seen dyad; the watched could not see, but could be seen, while the opposite was true for the watchers. From this asymmetry came the very essence of power, because, for Foucault, "the power to dominate rests on the differential possession of knowledge." [Foucault, 1983]

The Panoptic structure must be kept in mind when considering technology and anonymity, for that is exactly what is created by a wholly-identified society. When a person has been identified in a situation, he or she can now be watched. Whether anyone is *actually* doing so is irrelevant; the possibility remains. This is particularly true when technology is incorporated into the environment. A person carrying an electronic tag does not know (in fact, almost cannot know) *for certain* that there are no readers in the vicinity. Similarly, one can seldom be comfortable in the knowledge that there are no hidden surveillance systems present, particularly in places that have signs posted reading, "Smile for the camera." The list of situations in which one cannot be sure if another is watching is endless: workplace e-mail filtering, electronically-recorded credit card transactions, GPS cell phone location, etc. Furthermore, one virtually cannot watch the watchers. It is not easy to know who is reviewing surveillance camera footage, for instance, particularly when one is in public spaces where a camera's owner is not even easily determined. The Panopticon may not have had much effect as an architectural design, but the concept lives on with frightening prescience in modern society. The next work that will be examined will show just how much power this structure can create.

3.2. George Orwell's *Nineteen Eighty-Four*

George Orwell's 1949 novel, *Nineteen Eighty-Four*, is a vital piece of work in the study of privacy, even though it is a fictitious account of a future dystopia. Through

comparisons to this well-known work, the privacy fight can be brought to the general public; most people understand the concept of the 'thought police', and virtually everyone recognizes the phrases 'Orwellian' and 'Big Brother.' However, it is not simply its ubiquity that makes the book vital; it was also one of the first widely recognized works on the effects of surveillance and lack of privacy on the populace. Again, it is a work of fiction. However, putting that fact aside momentarily, we will undertake an examination of Orwell's vision of future Britain, and see in just what ways we can utilize it in our discussion of anonymity.

The first thing to recognize about Orwellian London is its panoptic nature. In every room of every building, as well as throughout public areas, are *telescreens*; essentially, televisions with the capability to simultaneously receive as well as broadcast. Every movement, and every sound above a low whisper, is picked up by these monitors. However, what happened with this data wasn't clear to any citizen of Oceania, for a very clear purpose: the ruling Party wanted the people to censor themselves, and in this way clear themselves of even *thought crimes*. Orwell writes:

> "There was of course no way of knowing whether you were being watched at any given moment. How often, or on what system, the Thought Police plugged in on any individual wire was guesswork. It was even conceivable that they watched everybody all the time. But at any rate, they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." [Orwell, 1949]

The telescreens, as well as hidden microphones in areas where the screens were not practical, were the major fear of the Oceanic people. Winston (the protagonist), in particular, noted that it was inadvisable to wear anything but an expression of quiet optimism when facing the screens. Any action or comment that seemed peculiar would draw the attention of the thought police, which was generally considered the worst possible fate for a Londoner [a concept to keep in mind for chapter 4, when Chicago's Intelligent Camera system is discussed.] Because no one knew exactly what actions were being watched for, or when a particular camera feed might be monitored, the Thought Police had power in the city; the Party's dominance (which will be assumed to be an undesirable situation herein) was based on this imbalance of knowledge. By preventing anonymous action through constant surveillance, the Party bred control.

Is this situation so different from modern society? Faceless cameras monitor many public actions, and remote computers record financial transactions. It is true that the aim of modern surveillance is the improvement of life for the citizenry, but will the outcome be any different? This is a question which will be addressed throughout this thesis.

Another question which will be touched upon is the role of the public in government surveillance schemes. There is a common idiom which says "I prefer the devil I know to the devil I don't." This means that in general, a person forced to choose between two negative outcomes will choose the one that he or she understands and knows, rather than a mysterious outcome (which may not be as bad). In relation to surveillance, this can be interpreted as obvious methods being preferable to hidden ones. Networks of cameras, then, are preferable to networks of spies; at least, in this case, one knows not to trust the cameras. The society depicted in *Nineteen Eighty-Four* recognized this distinction.

Those being surveilled recognized that "the amateur spy was the greatest danger of all." [Orwell, 1949] One is always cautious around the telescreens, but might slip up in the company of others. The Party recognized this fact, and enlisted children into 'the Spies' at a young age, teaching them that it was a great crime to be against Big Brother, and that it was their duty to watch for, and report, any strange occurrences, even involving friends or parents. This was simply one further way to obliterate anonymity in society; one will frequently reveal his or her name simply by way of introduction, and take others into confidence. If the practical anonymity of the stranger is taken away by the likelihood of that person being a government agent, then it is likely that conspiratorial whispers will also disappear. Who knows what will be overheard, or directly reported?

Again we must ask, is this world much different from our own? In 2002, the United States Justice Department created the Terrorism Information and Prevention System (TIPS). This project was a means for workers to report suspicious activities in a uniform manner. It would have enrolled truckers, train conductors, letter carriers, utility employees, ship captains, and many other as government informants; instantly, the US hoped to create millions of homeland spies. This project was to pilot in 10 cities; 1 in 24 people in these cities, many who had access to homes (mail carriers, cable installers, etc), would have been trained to recognize "unusual or suspicious activity." [Stanley, 2004] Additionally, the Department of Homeland Security published materials admonishing citizens to stay alert, and to recognize that, for instance, "persons not fitting into the surrounding environment, including any beggar, demonstrator, shoe shiner, fruit or food vendor, street sweeper, or newspaper or flower vendor not previously recognized in the area ... could be a terrorist in disguise." [Stanley, 2004] By creating such a society, a person is forced to identify him- or herself at all times, lest he or she be mistaken for a radical. The government is endorsing fear or the stranger, and by doing so not only removes an individual's ability to be anonymous without attracting overmuch attention, but also stops that individual from not conforming to community standards. A stranger is a person who looks or thinks differently than you; according to Homeland Security, it is your duty to observe, and report on, all this person's actions.

3.3. David Lyon's *Surveillance Society*

Moving from the fictional world of Orwell, we now enter the real. David Lyon's *Surveillance Society: Monitoring Everyday Life* is an interesting book in that he does not outright condemn the concept of universal surveillance; rather, he calls for controls to be puts on the data being collected. He notes, as will be further expanded in chapter 4, that surveillance is not "the product of some capitalist conspiracy or the evil effects of a plutocratic urge." [Lyon, 2001] Instead, it is a product of modern society's overwhelming demands for efficiency and convenience. It is efficient for a government agency to collect all your personal data into a single file, rather than having it scattered (or unavailable); it is also very convenient. Similarly, it can be tremendously convenient for an individual to be recognized by a store he or she is visiting (as items of interest can be brought to his or her attention immediately), or by his or her home (adjusting conditions to match the owner's preferences). There is certainly a caring, enabling aspect

to large-scale surveillance. However, along with that comes the other half of the dyad: control and constraint.

The two faces of surveillance need not be completely disjoint; the same piece of equipment can serve both purposes. Consider, for instance, a downtown CCTV camera. This camera may reassure a person traveling through the neighbourhood at night; the camera's presence allows greater freedom of movement, due to a reduction in the fear of crime. However, that same camera might keep a person away from a protest or stop him or her from doing a silly dance, due to the unwanted attention that such an act might bring. Thus, Lyon would argue, it is not the actual watching to which a person would object; rather, it is the treatment of the information being recorded which is offensive.

What has led us to a situation in which watching is inevitable? Lyon claims that it was the modern 'society of strangers', in which the private sphere emerged from the growth of cities and anonymous, impersonal relations. [Lyon, 2001] In the West, persons fought to become sovereign individuals in order to differentiate themselves from the masses. In order to participate freely and effectively in the new democracies, people distinguished themselves from their family, clan or city; as such, the 'individual' emerged. This action, however, naturally led to the collection of data on these individuals. In the words of Bertrand Russell, society transitioned from knowledge by acquaintance to knowledge by description. [Lyon, 2001] The sheer numbers of people striving for individuality made it near impossible for anyone to personally know all those in whom he or she must lay trust. Thus, descriptors rather than personal knowledge became the basis for many functional relationships, and the more details one had about another person, the more trust could placed on his or her being a responsible citizen. The surveillance society was born.

The initial surveillance society was somewhat tolerable. Recorded events were almost always triggered by the actions or behaviours of the subject. A credit or store loyalty card only ever collected data when the holder chose to use it; medical records would only be updated upon a trip to a physician; even telephone tapping only works when the phone is used. Also, the benefits to the watched were almost always palpable; in some way, most surveillance created added convenience. Because of this, the practice was eventually accepted. Data collection was seen to be necessary, and since a person had at least some degree of control over when at what was collected, and was receiving some tangible benefit from it, surveillance was allowed to be integrated.

However, this is where changes are occurring in the nature of surveillance technology. Society is becoming more and more enmeshed in the 'tyranny of the possible', in which technologies are deployed simply because they are available. [Lyon, 2001] This frequently has to do with fear. Nan Ellis claims that the late twentieth century saw fear generating "divisive architectural policies that turned inward and backward rather than facing the actual social challenges of urban life." [Lyon, 2001] Defensive spaces began to appear, rather than living spaces. Surveillance began to take on an anticipatory nature; people were no longer as concerned about recording what had happened, as they were about predicting what would happen. Thus, it became ludicrous to prevent a technology from being deployed simply because it was unproven; let it flourish or fail in the field, as

one cannot know what events the technology *might* be able to predict, or in what ways it might be used to do so. Further, it became unbeneficial to allow people control over the collection of their data; it was only through constant surveillance that one could be safe. Additionally, the 'palpable benefits' of incessant supervision became singular: the reduction of fear. The reasons for tolerance for this state of society were removed, yet the technologies remained; thus, rather than accepting surveillance as a benefit, people were forced to accept it as an inevitability.

Surveillance is the single greatest threat to anonymity; if no one is listening, shouting your name has no deleterious effects. However, when constantly under some unseen, watchful eye, it is nearly impossible to exist without being identified. David Lyon's surveillance society is one of efficiency and convenience, it is true, but it is also one of social sorting, disembodied citizens, and social orchestration; exactly the society which is crying out for anonymity. One needs to be able to break the chain of surveillance, but to do so (barring outright revolt), he or she must be able to escape the monitors. Even if only for brief periods, there must be a way to namelessly watch the watchers.

3.4. Simson Garfinkel's *Database Nation*

Where David Lyon leaves open the question of the future of surveillance – that is, the potential to control its use – Simson Garfinkel presents a much more definite viewpoint. He claims,

> "The choice that we face is not between pervasive monitoring systems operated by the establishment and monitoring systems that are operated by the establishment *and* all the citizenry. There is a third choice: creating rules that cover the deployment of monitoring systems and the use of captured happenings. We dismiss this third choice at our peril." [Garfinkel, 2000]

The privacy crisis that we are now facing, he notes, certainly does appear to be a matter of trading off personal data for the benefits of modern society. But why should this be? There is no reason that a person should need to surrender his or her shopping habits, address or Social Insurance Number to a database over which he or she has no control simply to be able to use a credit card. However, this is the compromise we are being asked to make.

Interestingly, Garfinkel compares today's battle over privacy protection to the fight in the 1950s and 60s over environmental regulations. At that time, big businesses claimed that poisoned lakes and rivers were the inevitable price of technological development. Without them companies could not flourish and provide economic development, job growth or an improved standard of living. In Garfinkel's words, "Poison was progress: anybody who argued otherwise simply didn't know the facts." By the end of the 1960s the battle for the environment seemed to have been lost; Lake Erie was declared to be dead, and Ohio's Cuyahoga River had caught on fire. However, many environmentalists soldiered on, and by 2000 Lake Erie was again alive, and fish caught in the Cuyahoga could be safely eaten. This is the type of fight that privacy activists may be in for. Modern society is presenting us with a choice: surveillance, or lack of progress. This, according to Garfinkel, is ludicrous. It may not be easy, but privacy protection and progress can proceed hand-in-hand. He goes on describe not only how this can be accomplished, but also why it must.

Perhaps the United States, arguably the least privacy-conscious developed Western nation, will need a privacy crisis much like the 1960's environmental crisis to finally consider effective privacy protection. In fact, much privacy law seems to be reactive. When the US Department of Health, Education, and Welfare developed the Code of Fair Information Practices, virtually every European country created laws based on these principles; many created commissions or commissioners to oversee the application of these laws. Why did it have this effect in Europe, but not the US? In the time of Nazi Germany, Adolf Hitler's secret police used the records of the governments and private organizations in the countries he invaded to identify and capture those who were most threatening to the occupation. Because of this crisis, post-war Europe recognized the danger of allowing extensive, unchecked data collection on individuals, even by well-meaning, democratically accountable governments. [Garfinkel, 2000] Various lesser situations have shown that the US will pass reactionary laws as bad situations arise. The 1988 Video Privacy Protection Act was passed in response to a journalist's accessing Supreme Court nominee Robert Bork's video rental records, looking to find pornographic materials. (The journalist was unsuccessful, though many off-handed remarks at the time ignored this fact.) More recently, a string of data thefts (including hacker's accessing 40 million credit cards numbers through MasterCard's databases, and large-scale security breaches at various data aggregators) led Congress to propose many data privacy changes, including an $11 million fine for not reporting such incidents to affected consumers. [Krebs, 2005] However, even with these changes in place, strong privacy laws do not exist. The PATRIOT Act, for example, gives the FBI the power to demand any tangible item from any company, and prevents them from revealing the request; thus, the mere existence of records can compromise their integrity.

Why is having our personal information recorded and stored such a bad thing? This speaks straight to the heart of Garfinkel's argument. Privacy and anonymity serve vital functions in our society, and to take them away is to limit our liberties. Anonymity is not simply about the person wanting to watch pornography online; it is also about the woman who is afraid to use the Internet to organize a protest about a toxic dump, fearing that the dump's investors will rifle through her past if she becomes a nuisance. Privacy is not just about special prosecutor leaving no stone unturned in his or her search for corruption; it is also vital for the upstanding citizen not wanting his or her life turned into a public event simply because he or she runs for office. And neither privacy or anonymity is about the searches, metal detectors, and inquisitions that have become routine in our daily lives; they are about a society which treats its citizens as potential terrorists, while providing little real protection. [Garfinkel, 2000] We are in a battle against people who desire information for reasons of business, politics, security or simple nosiness, and at stake is our notion of free democratic participation.

When examining new surveillance methods and their effects on society, Garfinkel argues, it must be made clear that technology is *not* privacy neutral. Frequently one will hear the argument, "Technology can be used to invade privacy, or it can be used to protect privacy." [Garfinkel, 2000] Thus, it is neutral; it is the way that the system is used by *people* that creates problems. However, this argument is simply not complete. Yes,

technology can be used to protect privacy, but the overwhelming tendency is to remove it. [Garfinkel, 2000] Privacy protection often necessitates an extra design step; a video camera, for instance, that catches and records everything is easier to create than one that analyses a scene, and only records vital data. Also, while it is simple to create a privacy invasive mechanism, it is near impossible to create one that guarantees that your information is protected. It is possible that one will see some clear signs that your privacy is being violated: increased junk mail, his or her personal information posted online, or finding a video camera in the bedroom. However, how can one know that his or her privacy is not being violated at any particular moment? Unless he or she is completely disconnected from the outside world (including the prevention of wireless transmissions from the home), such knowledge cannot be had.

Furthermore, the public must critically examine the proposed benefits of any surveillance system being considered, particularly when those systems do not have clearly defined limits. Pervasive surveillance has so many negative effects that it must be ensured that they are outweighed by the positives. This can be a very difficult task to undertake, however. For instance, one of the reasons that is frequently cited for the instituting of large scale surveillance systems (government access to all materials purchased, travel, literature read, etc.) is the fight against terror. Such a system would be extremely effective, in some cases, and perhaps easily justified. Michael Froomkin, an American law professor, notes that in cases of terrorism many may feel that even torture of suspects is justified, if it will prevent the detonation of, say, an atomic bomb. [Garfinkel, 2000] It is certainly not a lawful act, but it may be a moral one. Given this, can anyone question the morality of wiretapping, video surveillance, or consumer data recording? These techniques can certainly be used to find those who are planning major chemical or nuclear attacks, perhaps even at the stage of purchasing the necessary materials for a bomb. Thus, since these actions are not only effective, but also arguably moral, are they not completely justified? Clearly, given the context of the previous statement, the answer will be 'no.' However, I would ask the reader to try to see the persuasiveness of the given line of reasoning, before I present a counter argument.

The counter argument to the above relates to the assertion that the surveillance techniques described are effective. The morality argument can also be questioned, but will not be here. The case will hinge on the following statement: some terrorist acts cannot be anticipated. As an example, biological terrorism will be considered. This is particularly difficult to detect ahead of time, because biological agents (such as botulism or anthrax) occur naturally. There are no emissions and virtually no traceable purchases necessary. A single person, having taken one or two basic college microbiology courses, could create a major weapons arsenal with $10 000 of equipment and a 15 square foot basement room. [Garfinkel, 2000] Kathleen Bailey, former assistant director of the US Arms Control and Disarmament Unit, states that "If someone wants to do it, you can't stop them." [Garfinkel, 2000] Even if the Constitution was abolished, and a police state declared which destroyed all privacy laws and permitted any form of surveillance, the bioterrorist threat could not be abolished. An anthrax infected sheep or a tin of rotten meat in which the botulism toxin grew and some know-how is all that is needed to create a massive and very deadly attack. Thus, Garfinkel would agree with the conclusion

reached by the American Civil Liberties Union, and many others: "Mass surveillance threatens freedom more than it threatens terrorists." [Stanley, 2004]

The Database Nation, in which every action is recorded and stored for future use, is not to be feared, so much as controlled. It can provide benefits, such as security and convenience. However, we must ensure that function creep is highly monitored. One of the principles of Fair Information Practices reads, "There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent." This is where safety in databases can be assured; if a) the purpose of information collection is stated and thoroughly investigated and deemed valid by some independent body, and b) the information collected is not used for any other purpose, it is much more likely that the data will be safe. However, this is not the case. Information is routinely bought and sold by various groups, accessed secretly by government agencies, or simply lost. Should these practices continue unchecked, the destructive forces of the Database Nation will continue.

3.5. David Brin's *The Transparent Society*

David Brin approaches the notions of surveillance, privacy and anonymity in a very different manner than the previous two authors. The two quotations with which he opens his book exemplify his ideas quite well:

> "There's no going back, and there's no hiding the information. So let everyone have it."
> "Sacrificing anonymity may be the next generation's price for keeping precious liberty, as prior generations paid in blood." [Brin, 1998]

Hidden actions and identities are detrimental to society, Brin believes, because they allow for an absence of accountability, the single greatest weapon for preventing corruption in a citizen's arsenal. Additionally, he says, we are never going to have true privacy or anonymity, because technological attacks on them will never be thwarted. Cameras will simply get smaller and less detectable, data trails will become un-erasable, and people will come to realize that there are no more secrets. At that time, it will be recognized that those at the 'top' of society have an endless, unstoppably open data flow upwards, and the average person will realize that his or her only recourse is to open the flow of data back down. The creation of a completely transparent society, he argues, is the only realistic means of survival, as it will produce the same level of accountability for the leaders as it does for those being led. To quote the book's editors, "The biggest threat to freedom ... is that surveillance technology will be used by too few people, not by too many." [Brin, 1998]

Countering the flow of information upwards, Brin believes, is counter-intuitive. It both breeds anti-social behaviour and creates distrust in those around us. He asks the reader to consider the following situation: a person is in your neighbourhood, performing some bizarre action; perhaps it is a strange dance, or involves some unrecognized object. In this situation, who would you be more willing to accept as harmless: the stranger in a ski mask, who refuses to reveal his or her name or background, or the person you know, who answers questions readily and whose past quirky incidents are known to be at worst an irritant. Clearly, one of these people is less likely to be tolerated as a mere 'eccentric',

and more likely to be actively feared or persecuted: the anonymous stranger. [Brin, 1998] Citizens are taught to fear the unknown, and nothing is more unknown than the person without an identity. It is important in a person's life that he or she be trusted, whether he or she wants to affect social changes or simply live free of harassment, and the best way to garner trust in others is to be known to them.

Additionally, Brin writes that anonymity creates suspicion in others for good reason: it also harbors ill deeds. Again, he begins his argument with a quotation, this time from philosopher Adam Smith:

> "While a man remains in a country village his conduct may be attended to, and he may be obliged to attend to it himself .... But as soon as he comes to a great city, he is sunk in obscurity and darkness. His conduct is observed and attended to by nobody, and he is therefore likely to neglect it himself, and to abandon himself to every low profligacy and vice." [Brin, 1998]

Paraphrasing Brin's argument in this case can only lessen its impact, as he is adamant on this point. Thus, his statement is here in full:

> "Almost by definition, anonymity is the darkness behind which most miscreants – from mere troublemakers all the way to mass murderers and tyrants – shelter in order to wreak harm, safe against discovery or redress by those they abuse. In fact, it might be hard to name any famous villains – even those standing atop a pinnacle of state power, like Hitler – who did not rely at least in part on anonymity to enhance their own (or their henchmen's) power to destroy. The glare of light can be irritating to the honest, but it is devastating to knaves and despots." [Brin, 1998]

Because anonymity is so frequently used for ill, why have it at all? It is true that it is useful in some cases, he writes, but in general it is simply a way to dehumanize others in order to exert power over them or justify doing them harm, or to hide one's self in order to commit acts that would not be done otherwise. The way to ensure freedom and a habitable society involves light, not darkness.

Would limitless data flow in all directions be abused? Brin claims that it would not. A person would not risk the public censure associated with use of, say, a comprehensive CCTV system for voyeuristic purposes, because it would be entirely likely that he or she was being watched as well. It is this mindset of being under permanent observation that will ensure accountability at all levels. Corporations will fear overusing customers' data because those same customers could turn around and expose the company's misdoings. Governments will not be able to harbour corruption, as a single observant individual will be able bring attention to it. Also, the average person will be forced to act civilly, as the will likely be under the watchful eye of someone at all times. It is in this way that our freedoms will be ensured, and our societies will flourish.

Brin's conception of the functionality of a completely transparent society is not necessarily incorrect so much as it is impractical. It is founded on the belief that accountability will be distributed equally if information is made freely available to all; this is simply not the world in which we live, nor will it ever be. An employee, for instance, who has witnessed his or her employer doing wrong can reveal that information and create an embarrassing situation for the latter; an employer, however, can financially cripple an employee by not only firing them, but also spreading word throughout their field about any wrongdoings, effectively black-listing the employee. Power relationships will not change due to the transparency of information; in fact they will likely worsen, as those in charge seek to leverage any blot on an inferior's record for more control. Short

of extreme corruption, though, there will be little an ordinary person can find in the information flow that will have much effect on a superior. Additionally, the vast nature of the flood of records that would be made available will make it unlikely that important data could be filtered out of the noise, without technological assistance. Who will have access to the necessary computing facilities, and be able to research way of wading though the oceans of info? The powerful, of course. It is clearly true that transparency will increase the accountability of corporations and governments, in that obvious corruptions will be recognized. However, the effects will be felt mainly by those in the lower social strata, as a domineering superior will be able to use any and all past transgressions as a means of control. Even among those on an equal social footing, there are some who have more to lose through complete transparency than others. A person with long forgotten radical political affiliations, or an alternative (i.e. non-heterosexual) lifestyle, or who simply leads an interesting life, will be selected for particular observation by many. Punishment (in the form of additional scrutiny) of non-comforming people is a means for homogenization, not free choice of lifestyle.

Again, these problems are not all solved by anonymity; but at least it can help. Anonymity has created hundreds of whistle-blowers, who are cheered for exposing corruption, not chided for hiding behind a protective mask. It allows for many identityless police tip lines, used by thousands in order to turn in criminals without fear of reprisal. Sexual assault victims are granted anonymity in order to encourage the reporting of incidents, an act which involves overcoming great fear. In all of these cases, anonymity is required to reverse the power relationship, providing the controlled a means of recourse in case of abuse. It is not simply a shadow in which troublemakers can lurk; it is also an (unfortunately necessary) cover for those in fear. There is certainly more than one reason for which a person may not want to be seen, and while these reasons may not all be righteous, they are also not all evil. A transparent society promotes conformity, whereas the option for privacy allows for diversity. A diverse society will have its conflicts, but it is the only kind in which freedom of choice can truly be exercised.

There is a common thread running through the works of each of the above authors: the important role surveillance technologies play in determining the level of privacy to be expected by an individual. In the next chapter, we will thoroughly examine the potential impacts of surveillance technologies on privacy and anonymity, and discuss the best possible ways to limit the damage done by the systems which have a legitimate function within society.

4. Technologies of Surveillance: Evolution and Future Impact[1]

This chapter will examine the evolution and future impact of surveillance technologies. It will begin by defining the term 'surveillance,' which can mean many different things to different individuals. An overview of the ethical issues associated with surveillance will then be presented. By way of example, the effects of closed-circuit television on society will be examined in detail, as will be the impact of improvements to CCTV's functionality. Other surveillance technologies will then be presented, though in lesser detail. The public's reaction to these technologies will then be considered, as will the increased threat to the public created by the use of data mining. Finally, conclusions will be drawn about the necessity of constant vigilance from the public to ensure the proper institutional use of surveillance technologies.

4.1.1. Defining 'Surveillance'

In its most literal sense, the word 'surveillance' means 'to watch from above.' This definition creates the image of Big Brother looking down at the populace, viewing the world from on high. Some researchers would agree with this rather pessimistic view of surveillance practices; Christian Parenti, for example, says that constant external watching instills discipline by forcing self-regulation. [Parenti, 2003] This is similar to Jeremy Bentham's Panopticon; the mere potential that one could be under the gaze of an authority figure makes him or her behave in a socially-desirable manner. On the other hand, some researchers see surveillance as a rather more mundane practice. David Lyon claims that surveillance is not the product of some vast capitalist conspiracy; rather, it is simply the natural result of modern society's desire for speed, mobility and convenience. [Lyon, 2001] He also provides a very useful definition of 'surveillance', which shall be adopted for this chapter: according to him, surveillance is "any collection and processing of personal data, whether identifiable or not, for the purposes of influencing or managing those whose data have been collected." [Lyon, 2001] Thus, along with the obvious technologies associated with surveillance (CCTV, phone taps, etc.), we have other 'softer' forms of surveillance, such as customer loyalty cards, electronic building access systems, and toll road collection systems. There are two faces of surveillance; one is caring, the other controlling. Unfortunately, as Lyon points out, modern surveillance is increasingly shifting towards the latter. [Lyon, 2003]

4.1.2. The Ethical Issues Associated with Surveillance

While it may not always be intentional, surveillance breeds control. This is the core of each of the ethical issues surrounding its use. Surveillance, it will be shown, can create public discomfort; this is because the public (rightly) does not trust the motives of those exerting this control over them. If each government agency, corporation and individual that chose to install a surveillance system were trusted not to abuse the information being gathered, there would be no discomfort. Similarly, surveillance can be used to control

[1] A version of this chapter has been accepted for publication. Lockton, V. and Rosenberg, R.S. (2005) Technologies Of Surveillance: Evolution and Future Impact. Proceedings of ETHICOMP 2005. Linköping, Sweden.

and silence public dissent. Henry David Thoreau wrote "All men recognize the right of revolution: that is, the right to refuse allegiance to, and to resist, the government, when its tyranny or its inefficiency are great and unendurable." [Thoreau, 1849] The ability to revolt against an unjust controller is a necessity, but unbounded surveillance makes resistance very difficult. There is almost no question that during the 1960's American Civil Rights movement, FBI director J. Edgar Hoover used every surveillance ability within his power to harass activists, unionists and peaceniks [Parenti, 2003]; it is interesting to consider whether or not this movement could have been as effective had Hoover had access to all of today's surveillance tools. As surveillance technologies increase in power and functionality, so does the potential for abuse. If any organization is allowed to gather limitless information about their opponents, they will become a nearly un-resistible force; mass surveillance allows this to happen.

Marginalized groups in any society are a natural target for information gathering. People are frightened of the unknown; thus, minorities are frequently singled out for higher levels of observation. David Lyon notes that this is actually the way that many new surveillance technologies are introduced to society; they begin by being focused on society's weakest, most marginalized groups, and then through 'function creep' make their way into the mainstream. [Lyon, 1994] This is a very oppressive practice, however. When any group is singled out for scrutiny, they will inevitably be found to be in violation of some set of societal norms. Should this group, though, be unaware of (due to cultural differences), unable to achieve (i.e. the homeless), or simply un-accepting of the norms, increased surveillance will only serve to highlight the differences between this group and the majority, and slow acceptance of the group into general society.

Care must be taken not to unintentionally develop a system of total surveillance; as tools combine, we form a 'soft cage.' This may be a worse scenario than the classic Big Brother. Against Big Brother the masses can rebel, but the 'soft cage' is mundane, decentralized, even convenient – and frighteningly thorough. [Parenti, 2003]

Perhaps these statements are the products of paranoid and pessimistic minds; this chapter will examine some of the surveillance tools currently in use, and let the reader judge for him or herself.

4.2. CCTV

For many, the first technology which comes to mind when thinking about surveillance is closed circuit television (CCTV) cameras. This association is not surprising, as the nature of CCTV makes it a very visible technology. Put simply, if you can't see the camera, it can't see you (with the exception of cameras behind one-way glass, etc). Also, CCTV is a tool for crime prevention, rather than detection. In the best case, the cameras are not meant to be used in the prosecution of criminals; rather, their purpose is to stop crime from occurring by their mere presence. Stores will sometimes hang non-functional CCTV cameras hoping that the apparent surveillance will deter crime; on the same theory of prevention, Tasmanian windshield license stickers read, "Smile! Surveillance cameras are everywhere." [Lyon, 2001] David Lyon refers to this as 'social orchestration.' CCTV

is not used for coercion and control, so much as for more subtly influencing behaviour. [Lyon, 2001] The need to have this affect leads to the necessity of CCTV being a very visible technology; thus, there is strong public awareness of the it. This awareness would not be nearly as strong, however, if it weren't for the technology's ubiquity.

4.2.1. CCTV in the United Kingdom

CCTV use has seen huge increases worldwide in the past two decades, but nowhere is this trend more noticeable than in the United Kingdom. In 1986 a small industrial estate outside the small English town of King's Lynn installed 3 surveillance cameras to counter a rash of crime. This technique was successful; no crimes were reported in that area in the next two years. [Nieto et al, 2002] This result did not go unnoticed; by 1994, over 300 jurisdictions in the country had installed some form of CCTV surveillance system. [Nieto et al, 2002] The growth of these networks had certainly not stopped, though; in 1998, the CCTV initiative was set up under the Home Office Crime Reduction Programme, which set aside £170 million in funding for a total of 684 surveillance camera projects. [Gill and Spriggs, 2005] In fact, between 1994 and 2004 £4-5 billion was spent on the installation and maintenance of the UK's CCTV networks. [Norris et al, 2004] All told, this system counts over 4.2 million electronic eyes, or one for every 14 UK citizens. By 1999, it was estimated that the average person in England was being captured on camera 300 times per day. [Norris and Armstrong, 1999]

Explaining the CCTV Usage in Britain

As mentioned above, CCTV usage in Britain began rather slowly. Prior to the King's Lynn system, very few permanent CCTV installations could be found. In general, small temporary set-ups were used against marginalized groups, such as football hooligans. However, in 1985 the first large scale, though again temporary, CCTV network was installed in the small seaside town of Bournemouth, which was hosting the Conservative Party Conference. [Norris et al, 2004] At the previous year's conference, an IRA bomb targeted at then-Prime Minister Margaret Thatcher had killed 5, though it left Thatcher unhurt; this was the first of many systems installed in response to the threat of Irish terrorism. However, the incident which may have solidified the CCTV's role in the fight against crime was the brutal murder of toddler Jamie Bulger. [Norris et al, 2004] Security cameras caught images of his killers leading him away from a mall; these images, replayed endlessly on television news shows, became iconic in the panic about youth crime. By pointing to CCTV's role in the fight against crime and terrorism, proponents of the technology managed to convince the public of its necessity.

The uses claimed by the UK for CCTV also constantly expanded. Initially, the purposes listed were the prevention of hooliganism, burglary and car theft. By 1994, a pamphlet published by the Home Office promoted CCTV as a solution to racial and sexual harassment, public drunkenness, drug use, vandalism, loitering, and a litany of other 'anti-social' behaviours. [Privacy, 1997] Given CCTV's "sexy, powerful" [Privacy, 1997] image, and the availability of large amounts of funding for its installation, regions had few options but to introduce surveillance camera programs, or to look weak on crime.

4.2.2. Does CCTV Increase Public Safety?

Given the high demand for video surveillance as well as the (potentially) limited time funding available for its installation, it should not be surprising that few, if any, districts undertook evaluations of CCTV's effectiveness in reducing crime prior to installing their systems. Once the cameras had gone up, though, many police forces started to report the dramatic effects of the systems, such as 90% reductions in vehicle crime and 75% reductions in assaults and theft. [Privacy, 1995] Statistics such as these only fuelled the rapid adoption of CCTV. However, the evidence being presented could not hold up to examination. It was noted that country-wide reductions in crime were not being taken into account, nor was the possibility that CCTV was simply moving crime into non-monitored areas. Reporting to the Scottish Office in 1995 on the effects of CCTV on crime, the Director of the Scottish Centre for Criminology stated, "All (evaluations and statistics) we have seen so far are wholly unreliable." [Privacy, 1995]

In 2005, Britain's Home Office commissioned a huge study (Home Office Research Study 292) to once and for all ascertain the impact that CCTV had had on crime. Gill and Spriggs undertook this task, and came to numerous conclusions on the effectiveness of CCTV, including:

- The majority of systems did not reduce crime, and where there was a reduction, it was likely not due to CCTV.
- CCTV did not make people feel safer, nor change their behaviour.
- CCTV had been oversold by successive governments as a 'magic bullet' answer for crime problems.
- The objectives of many CCTV systems were undefined, and thus the systems were installed in areas and circumstances in which they were unlikely to have any effect on crime.
- It is a bad idea to put up CCTV simply because funding is available. [Gill and Spriggs, 2005]

Even if the problems of poor planning were solved, it could not be shown that CCTV would have an effect on crime. Surveillance cameras were not having the effects intended; so, what were they causing?

4.2.3. Ethical Problems Caused by CCTV

Public Discomfort

When the public is being told exclusively about CCTV's crime-fighting and anti-terrorism uses, they tend to support the installation of cameras. However, a UK Home Office survey in 1994 came to the conclusion that the public were less likely to unconditionally support CCTV usage once issues, such as intrusion into private spaces, had been were raised and discussed in a group setting. [Privacy, 1997] Once people are made aware of the extensiveness of the camera coverage around them, they become ill at ease. Consider:

- "I don't like being watched. It makes me uncomfortable."
- "I stopped doing silly things. I don't want to portray myself in a certain light."
- "Cameras used for specific suspects and at specific times, that's good law enforcement. But I don't want it part of my permanent record every time I scratch myself on the street." [Carey, 2005]

Now, take this discomfort, and add to it the fact that the city of London has CCTV monitoring 40% of public activity. [Norris et al, 2004] That means that every time a person leaves his or her home or place of business, there is a nearly one in two chance that his or her actions are being monitored. Before any action is taken, a person may need to stop and consider whether or not they want it to be permanently recorded. Does having a conversation with a stranger make one a potential criminal's associate? If one is viewed reading anti-government material, is he or she now a potential traitor? The exact answer to these questions is not as important as the realization that these are considerations which are forced upon the public by blanket CCTV coverage.

The Silencing of Public Dissent

Columnist Jacob Sullum points out that "knowing that you are being watched by armed government agents tends to put a damper on things. You don't want to offend them or otherwise call attention to yourself." [ACLU, 2002] This is especially true for countries with weak democratic traditions, where anti-government protests frequently end in violence. Consider for instance China, whose Golden Shield project would place 200 000 surveillance cameras throughout Shanghai by 2010. The government envisions "a database-driven remote surveillance system, offering immediate access to registration records on every citizen in China, while linking to vast networks of cameras designed to cut police reaction time to demonstrations." [Walton, 2001] It is certainly not unreasonable to believe that this system would be an attack on all forms of public dissent. A person will certainly think twice about joining a demonstration knowing that he or she will be seen, identified, and quickly met with a police presence. In the United States, one might believe that an identified protester needs to fear a permanent government record on their activities. In China, though, the same identified protester might reasonably fear death. A person in fear of his or her life will certainly not make his or her voice heard over small matters; in this way, surveillance aids in the silencing of public dissent.

4.2.4. Additional Issues Created by Extensions to CCTV

Facial Recognition

Adding facial recognition technology to CCTV is a very natural step. It is also a very frightening prospect. As it exists now, images must either be monitored by a human, or recorded for future viewing. This allows for some small level of potential privacy. If the images are simply stored, they are unlikely to be viewed unless some unusual incident makes this viewing necessary. Thus, everyday activities aren't likely to be observed. Similarly, if a human is monitoring camera feeds, it has been shown that his or her

attention level falls far below acceptable levels within 20 minutes [Green, 1999]; also, humans are generally poor at facial recognition under pressure. [Introna and Wood, 2004] Thus, most people passing through a camera's gaze will not be noticed. However, once computers are able to perform reasonably accurate facial recognition, any privacy provided by practical obscurity will disappear. A person passing by a camera becomes a data point, consisting of the time and location of the identification, which can now be indexed, compared and combined. Painting a picture of a person's movements based on CCTV data will become significantly easier; privacy in public spaces will become a non-existent concept.

Further, the algorithms currently in use are better at finding African-Americans, Asians, dark skinned persons and the elderly within crowds of people. [Introna and Wood, 2004] Because of this, it is likely that more 'alarms' (recognitions of a person of interest) will be caused by members of these already marginalized groups. These identifications will seldom be classed as 'false positives' by already potentially-biased operators, thus placing greater scrutiny on the actions of minority groups.

Chicago's "Intelligent Camera" System

The American city of Chicago recently announced that it will be expanding its CCTV network to over 2200 cameras. This was not a particular notable development; however, the system to which these cameras will be connected is both novel and disturbing. The city has proposed that all camera input be fed into a computer system, which will search the images for 'suspicious behaviours', including wandering aimlessly in circles, lingering outside of public buildings, leaving packages and walking away, and many others. If these behaviours are detected, the footage will immediately be brought to the attention of a human operator, who can dispatch police as needed. [Kinzer, 2004]

This practice raises questions: What behaviours are considered 'suspicious', and who makes this determination? And in times of unrest, can carrying 'un-American' literature or being of a certain ethnicity be considered 'suspicious'? The answer to these questions is simply that we cannot know. Whatever prejudices the programmers of the system happen to incorporate, intentionally or otherwise, into the evaluation software will be seen in the end product. It is then left up to the operator to decide what does or does not need to be scrutinized further; if the operator implicitly trusts the judgments of the system, a situation of massive scrutiny of minorities and the homeless could quickly come to pass, as they are the groups most likely to violate 'social norms' and draw the attention of the computer.

4.3. Other Privacy-Threatening Technologies

CCTV is certainly not the only technology for which current increases in functionality and saturation create threats to privacy. Space limitations prevent an in-depth exploration of any item in the following (certainly non-comprehensive) group of surveillance technologies, but mention will be made of some troubling scenarios which may soon need to be faced. Recall, though, that these scenarios are not mutually exclusive; in fact,

the largest threat to privacy will be through the combination of multiple surveillance tools.

4.3.1. Radio Frequency Identification

Within the next two decades, it is very possible that every item ever manufactured will have an RFID tag affixed to it. RFID is a simple technology, which consists of a chip and antenna that broadcasts a unique identification number when queried by a reader. This broadcast can happen over a distance of a few inches, or many feet, depending on the technology used. Currently, though the main utilization of RFID still occurs within inventory tracking systems, use of the tags is expanding into the everyday world. The U.S. government is planning to incorporate RFID tags into their passports by the end of 2005, though it was only in April 2005 that they gave in to massive pressure to protect the data on these tags using various encryption measures. Had the passports made it to the public without these security measures, anyone with a reader would have been able to read all the information contained on the current printed passport. Similarly, the EVI Management Group has proposed to develop the 'e-Plate', a car license plate which would contain an RFID chip. This system might find great support in the British government, who are currently proposing a road tax based on distance driven, with more traveled roads having a higher cost. The 'e-Plate' would allow a government to monitor exactly the routes driven by each of its citizens, storing this information ostensibly for 'urban planning' or taxation purposes. However, there is absolutely no reason to believe that this data could not be used for more sinister citizen tracking purposes. These are but two of a plethora of potential abuses of RFID technology. With the cost of each tag soon to drop below 5¢, we can only expect the number of scenarios to increase as tags are affixed to anything (or anyone) whose location may be of interest. The uses and impact of this technology will be examined in-depth in the next chapter.

4.3.2. The Global Positioning System

GPS has become a standard add-on for many other technologies. Cell phones carry the units in order to locate their callers in case of an emergency (i.e. a 911 call), and vehicles carry GPS to allow display of local maps on onboard computers, track stolen cars and provide usage data to car rental agencies. However, it should be noted that the ability to locate a device, such as a cell phone or a vehicle, is akin to being able to locate its owner. In the United States, more and more often law enforcement agencies are taking advantage of this feature. Due to a Patriot Act provision, it is legal for any service provider to turn over locational data on their customers in times of 'emergency.' Albert Gidari, a Seattle-based lawyer whose clients include AT&T Wireless, Cingular Wireless and Nextel, has stated that the companies he represents receive 20-25 calls a day requesting the location of various cell phones, based on an 'emergency' such as a missing person. [Gidari, 2005] No proof of this emergency is asked nor given, and no record of the request is ever made, but the requested data is always turned over. No company's executive would want to see the headline "Jane Doe found dead due to Company X's reluctance to give information," but this is exactly the implied threat for refusal. This currently occurring scenario,

combined with the fact that cell phones are becoming near ubiquitous, means that many people are now carrying homing beacons accessible to any law enforcement agency.

Choosing not to carry a GPS unit (be it in one's cell phone, in a car safety system (OnStar), etc) is certainly no way to guarantee that one is not being tracked; surreptitious GPS surveillance has become an acceptable practice for police. It nearly wasn't: in 2003, the Washington Supreme Court ruled that GPS required the same authorization as any other form of targeted surveillance – a warrant issued in a court of law. ["Landmark", 2003] This decision was heralded by the ACLU among others as a great victory for the privacy of the individual. However, in 2005, a federal judge made this decision moot, by determining that New York detectives did not need a warrant to place a GPS unit on the underbelly of a car belonging to a suspected member of the Hell's Angels. Showing a complete lack of interest in the implications of the changes technology makes in the nature of law enforcement, he wrote, "[the suspect] had no expectation of privacy in the whereabouts of his vehicle on a public roadway." [Lyons, 2005] Since police would not have needed to obtain a warrant to physically follow him, they should not need one to use a technology which makes the job simpler, he believed.

A lack of understanding about the impact of using technologies to compile information previously done by humans is a major hurdle in the privacy battle. In this case, this author contends that police were initially given free ability to trail a suspect based on the difficulty of the task. At best, one officer can track a single person; thus, the tracking capabilities of the entire force are limited. This is another instance of privacy by obscurity; information is so difficult to collect that essentially, it can be considered private. However, in the age of technology, this form of privacy is destroyed. A single police officer is now able to monitor the locations of hundreds or thousands of suspects; a moderately sized force now has the ability to track the entirety of a town or city's population. All persons of interest could certainly have their movements recorded; this is a frightening prospect at a time when secret 'No-Fly' lists are quickly reducing the criteria for becoming 'of interest' to the government. Comparing a technological task to the same job performed manually, and assigning each the same level of complexity, is not only ludicrous, it is also dangerous.

4.3.3. Electronic Transaction Monitoring

A final piece of the surveillance picture is electronic transaction monitoring. Every time a person uses a credit, debit, or store loyalty card that information is recorded. This amounts to a huge volume of data; by its own estimate, Wal-Mart has over 460 terabytes of data stored on various servers, a number that is twice as large as the estimated amount of data on the entire Internet. [Hays, 2004] This allows the store to compile a picture of its nearly 100 million daily customers, from individual Social Security numbers to an area's general proclivity for potato chip purchase. If transaction records were stored simply as "These x items were purchased at this time", there would be few privacy problems. But when you append to this statement "by person y", you begin to create not only a profile of their buying habits, but also have now added yet another node to massive amount of locational data being gathered about that person. To purchase at store

x at time y, a person must be present at store x at time y. Further, it is not difficult to extract a person's likely income, marital status, number of kids, and potentially even political persuasion from a series of purchases. By doing this, targeted marketing can take place, as can (potentially) discrimination of customers based on buying power. The monitoring and recording of all electronic transactions is something that most people have simply come to accept; perhaps it is time to look at exactly what is being done with this recorded data.

4.4. Public Reaction to Surveillance

All of the surveillance possibilities presented above are of little consequence if it can be shown that the public doesn't mind being watched. Conversely, if the public is shown to be either clearly uncomfortable with or opposed to high-tech surveillance systems, perhaps agencies should think twice before installing them. Unfortunately, determining the public's opinions on surveillance is not a simple task.

Public reaction to surveillance tends to depend highly on the question asked. A 2003 Harris survey shows this fact well. [Harris, 2003] First, respondents were asked whether or not they were in favour of the increase of various surveillance measures, in response to the threat of terrorism; in general, they were. 69% of people were in favour of closer monitoring of banking and credit card transactions, 62% favoured increased camera surveillance in streets and public places, and 79.5% supported the use facial recognition technology. However, these numbers may be somewhat deceiving, because respondents to the same survey also highly valued their privacy. 96.5% of people felt it was important to be in control of who could get information about them. 91.2% said it was important to not have someone watch/listen to them without permission. Also, 77.6% of people responded that it was important to be able to go around in public without always being identified. Thus, we can conclude that people are in favour of surveillance – for everyone but themselves.

As has been previously mentioned, a 1994 UK Home Office study showed that people are less likely to unconditionally support CCTV once issues about the technology are discussed in a group. [Privacy, 1997] This and the Harris survey seem to confirm the theory, then, that the public doesn't tend to consider civil rights issues associated with a technology until those issues are explained to them. Thus, it is very dangerous to assume that just because the installation of a surveillance technology is supported in opinion polls, that the public has thoroughly weighed the pros and cons of this new system. It is very possible that their opinions are based on a combination of fear (of crime or terrorism) and a lack of information about possible consequences.

If the public's reaction to surveillance can't be easily measured before installation of the systems, can we look at how they feel once they have had time to experience the systems' effects? Perhaps this is a more telling set of opinions. In 2001, the USA PATRIOT Act afforded American law enforcement powers of surveillance unprecedented in that country. In 2004, a Harris poll set out to determine the public's fears, if any, about this increase in police and FBI authority. [Harris, 2004] It was found that 76.3% of

respondents were concerned about the possibility that non-violent critics of the government would have their communications monitored, and 73.7% feared broad profiling, searching and surveillance of people based on their nationality, race or religion, exactly the possibilities that are created by increased use of modern surveillance technology. In this case, three years went by since the United States government introduced radical new surveillance measures and it had still not been able to convince the electorate that the technologies would not be put to un-Constitutional use. In general, once surveillance has been experienced, public support for it tends to decrease; this, rather than *a priori* support for technology, is what must be made clear to policy makers.

4.5. The Increased Threat Created by Data Mining

The central tenet of many current governments and corporations is 'Knowledge is power." Standing out as a striking example of this theory is the U.S. Pentagon's now-defunct (at least in name) Total Information Awareness (TIA) project. The aim of this project was to examine the realm of all electronically available information about each American citizen, in an attempt to determine a 'terrorist signature.' To accomplish this task, government agents set out to compile dossiers on every individual that would encompass areas such as political activities, library records, musical preferences, sexual orientation, credit card usage history, neighbours, acquaintances, and so on. [Stanley, 2004] This project met with such huge public outcry that its funding had to be cancelled, though its functionality likely still exists in many secretive 'black budget' projects. However, the fact that such a project is not an unrealistic possibility raises possibly the largest issue created by the evolution of surveillance technologies: the fact that they do not exist apart from one another. Each technology, by itself, can be justified as necessary or beneficial; however, the society created by their combination is very frightening.

Modern surveillance equipment is increasingly based in a digital world. Consider such technologies as GPS, point-of-sale transactions, RFID, CCTV, facial recognition; any information generated by these technologies is either digital or easily digitized. Thus, every observation made by one of these systems can quickly become a piece of data in some massive, TIA-style dossier. Is it unreasonable to think that this could happen? While the 1974 U.S. Privacy Act prohibited American government agencies from aggregating data on any citizen who is not the target of investigation, they are allowed to purchase information collected by private companies. Data trading is a multi-billion dollar industry in the United States; companies such as Axciom and ChoicePoint exist with no function other than the collection and sale of personal information. Anything that is publicly available will be collected by these companies, packaged as a dossier and sold to any organization willing to pay for it: ChoicePoint, for example, claims to have 35 contracts to provide various government agencies with data on Americans. [Stanley, 2004] Finally, should a company refuse to voluntarily provide, or sell, the information stored in their database, a law enforcement agency can use its Patriot Act powers to subpoena the required data. Massive data aggregation is no longer a matter of 'if'; it is a matter of 'when.'

Consider the amount of detail that could be developed about a person by collecting all available electronic information about him or her. Tracking his or her car with GPS or an 'e-Plate' provides major changes in location, and facial recognition, combined with CCTV footage, cell phone tracking and information garnered from RFID-tags on one's person fill in the details of his or her movements. Transaction records provide lifestyle information. Online logs and library records track intellectual interests, and monitoring, via CCTV or otherwise, of attendance at rallies, lectures and events can provide information about the passions of a person, such as political or religious leanings. The list of information which can be collected goes on and on. The government of the United States, supposedly a country which prides itself on its freedoms, proved during the 1950s and 60s civil rights movements that it is willing to use all means at its disposal to gather information about, and harass, dissidents [Parenti, 2003]; is there any reason to think that the situation has changed, excepting that more tools are now available?

4.6. Conclusions

Harvard psychology professor Daniel Wegner stated that "In a very deep sense, you don't have a self unless you have a secret." [Carey, 2005] Unfortunately, modern surveillance is making it more and more difficult to keep one's actions away from watchful eyes; those without protection from the system will all be forced to live under public scrutiny. Surveillance is becoming more and more sinister; for instance, the city of Gotham, New York has begun to move towards hidden or disguised surveillance cameras. [Parenti, 2003] People will no longer know if they are under the city's watchful eye, and thus will have to be permanently in line with social norms (an exhausting prospect) and also not know where they can travel 'safely' under the watchful eye of a camera. Further, political responses to civil liberties questions are becoming more hostile. Ex-New York City mayor Rudolph Giuliani responded to an ACLU study of surveillance in that city by brushing them away, stating "They raise questions about everything." [Parenti, 2003] Chicago mayor Richard Daley answered critics of his city's intelligent CCTV monitoring by saying "The city owns the sidewalks. We own the streets and we own the alleys." [Kinzer, 2004] This implies that the citizenry be damned, the city can do as it chooses. This is exactly what must be feared. Surveillance technologies exist, and will forever continue to evolve. The only thing that keeps society from a state of total surveillance is the goodwill of those in control of the systems. Surveillance is not inherently malevolent; in the proper hands, it can be a very enabling tool. The issue should not be *that* we are being watched; it should *how* we are being watched. It is said that the price of freedom is eternal vigilance. This statement is as true in this context as any other; to ensure our freedoms, we must constantly watch the watchers.

5. RFID: The Next Serious Threat to Privacy[2]

In this chapter, we examine the threats which can be posed by function creep. RFID itself is not a particularly threatening technology; it is only when it is over-used that risks to the privacy and anonymity of individuals begin to appear.

Radio Frequency Identification, or RFID, is an old technology, dating back to the Second World War. It was developed when the United Kingdom found that while radar could recognize the presence of incoming aircraft, it could not determine the planes' nationalities. In order to make this determination, 'identification friend or foe' (IFF) radio transponders were added to Allied planes, which allowed them to show up with distinctive 'blips' on the radar screen. ["RFID", 2005] In this way, RFID was born. In 1948, however, it was stated in the first academic paper on RFID that "... considerable research and development work has to be done before the remaining problems in reflected-power communication are solved, and before the field of useful applications is explored." ["RFID", 2005] In the present day, that research is well underway. RFID's usage is currently undergoing a revolution, being incorporated into everything from automobile keys to inventory control systems to passports. With this deployment, though, have come great concerns about the technology's effect on the privacy. This chapter will explore the recent history of RFID and examine the privacy issues arising from its use, as well as addressing potential means of handling those issues. Finally, the author's views on the most effective solutions to the privacy problems created by RFID will be presented.

5.1. RFID As It Is Now

5.1.1. Technology

The technology behind current RFID is rather uncomplicated. In its simplest form, it consists of a tag (microchip) and a reader. The tag consists of an electronic circuit which stores data and an antenna which broadcasts this data by radio wave in response to a query signal from a nearby reader. The reader also contains an antenna which receives the radio signal, and also has a demodulator which transforms the analog radio data into digital data suitable for any computer processing which will then be done. 'Active' RFID tags include a battery, allowing them to constantly transmit the data stored on the circuit, whereas 'passive' tags contain no energy source, instead receiving their power from the reader's initial query. Passive tags are thus less expensive, smaller, and have a longer lifespan (no battery means that the integrity of the hardware alone determines functionality) than their active counterparts, and are the standard form of tag being adopted for commercial use. These tags can be read at distances of up to 10m, though for high security applications this range can be limited to as low as 10cm. Active tags have a larger broadcast range (up to 100m), and are generally used when the location of the tag

[2] A version of this chapter has been published. Lockton, V. and Rosenberg, R.S. (2005) RFID: The Next Serious Threat to Privacy. Proceedings of the Sixth International Conference of Computer Ethics: Philosophical Enquiry (CEPE2005), P Brey, F Grodzinsky and L Introna (eds), Enschede, The Netherlands, 269-281.

is more important than the data stored on it; for instance, a slight variation on these tags is used in bracelets given to young visitors to Denmark's Legoland amusement park, so that lost children can quickly be located.

A standard RFID tag stores a simple identification number, usually either 96 or 128 bits long, and contains few or no security measures to protect that data. However, by incorporating a more advanced microchip onto the tag, variations on RFID technology such as 'smart cards' are created, which can contain from 512 bits to 72Kbytes of memory, various data protection and encryption schemes, and a limited read range. This form of contact-less information transfer is used when privacy is deemed to be vital, such as in electronic payment or identification cards.

5.1.2. Current (innocuous) Uses of RFID

Though it has not emerged as a privacy issue until recently, the use of RFID technology has been widespread for some time. Tens of millions of pets worldwide have been 'chipped' in order to facilitate their identification at animal shelters. It is estimated that in the United States alone, 6000 animals were reunited with their owners due to their RFID tags every month in 2003. [Hines, 2004] Animal tagging is also being done in an attempt to prevent the spread of disease; at least 20 million livestock have been tagged in order to track outbreaks of Mad Cow and other diseases, and Portuguese legislators have ordered that the nearly two million dogs in that country be chipped and registered in a national database in an effort to control the spread of rabies. It is certainly not just animals which are being tagged, however. According to Texas Instruments vice-president David Slinger, the revolution in RFID usage began in 1993 with an effort to deter auto theft. A chip was added to the ignition key of vehicles, and a transponder was incorporated into the steering column; if the wrong key (or no key) were used to start the car, it would be immobilized. 7 of 10 cars now have this feature, and Ford is reporting that theft rates on their oft-targeted Mustang line are down 75%.

Nearly 40 million Americans already carry RFID tags [Garfinkel, 2004], whether they are embedded in car keys, building access devices, or speed payment fobs. However, the RFID industry did not reach its current level of prominence until an order was given by the largest, most powerful retailer in the world, WalMart.

5.1.3. The WalMart mandate

In June 2003, Arkansas-based retailer WalMart made an announcement which changed the world of RFID. It was a mandate that by January 1st, 2005, each of the store's top 100 suppliers would have to add an RFID tag to all shipping crates and pallets sent to any WalMart distribution centre. In addition, the next 200 largest suppliers would have to comply with this mandate by the same date in 2006. Demand for RFID tags skyrocketed, as it was estimated that the top 100 suppliers alone will require at least 1 billion tags per year to comply with this order. [Williams, 2004] In fact, by mid-2004, it seemed as if this mandate was too demanding to be accomplished; not for the suppliers, but for the RFID manufacturers. Demand was so high that many wondered whether it was possible

to produce enough tags to meet it. However, each of the top hundred have agreed to tag at least a portion of their shipments; in all, by the end of January 2005, 65% of pallets and cases shipped to WalMart contained an RFID tag. [Bednarz, 2004]

The WalMart mandate will likely provide two benefits to the RFID industry in addition to instantly creating a huge market. First, a standard for RFID technology can be created; rather than develop many different, incompatible tags and readers, it is more sensible for companies to use the retailer's preferred style of tags. Secondly, due to the massive demand for them, manufacturers will be able to drastically reduce the price of each tag, from a range of 25 to 50 cents to 5 to 10 cents each. This will allow for the technology to be adopted by smaller companies, and used in more applications. RFID's day in the sun has arrived, as a direct result of a demonstration of the power of the mightiest retailer in the world.

5.1.4. Why RFID?

WalMart's insistence on RFID tagging was no whim. By allowing pallets of products to be 'seen' without needing a direct line of sight, RFID can solve many of the storage problems encountered by retailers. It has been estimated by the Retail Industry Leaders Association that of the $3 trillion spent throughout the worldwide retail supply chain, 6-10% is lost due to poor visibility. [RILA, 2004] They believe that proper RFID usage can reduce theft and shrinkage in the supply chain, increase sales by decreasing out-of-stock merchandise, and more accurately predict stock replenishment needs. Through visibility improvements, the decrease in warehouse personnel needed, and other benefits, WalMart alone expects to save $407 million annually. [McHugh, 2004]

Clearly, the RFID industry is here to stay. However, as with any technology, with the benefits provided come risks. RFID is an excellent supply chain solution, to name just one of its innocuous uses, but what will happen when the technology inevitably sheds its current unobtrusive role and becomes prominent within the general public?

5.2. Dangers of RFID's Potential Uses

5.2.1. Item-level Tagging

If the tagging of merchandise had been limited to the pallet-level, very few comments would be made on the issue by privacy advocates. At that level, it is highly unlikely that any consumer would ever come into possession of a tag, as the tags would end their time of service in the warehouse. However, this limiting of RFID's use will almost certainly not occur; as the costs for both the tags themselves and the infrastructure needed to support them decline, we will see an increase in item-level tagging. That is, there may come a time when nearly every product manufactured has an RFID tag attached.

The reason for this level of tagging is, again, inventory control. Currently, retail products carry a Universal Product Code (UPC, or bar code). The UPC has two main limitations: it can only identify the type of product rather than details about it, and it

needs line-of-sight to be read. A product carrying an RFID tag containing an Electronic Product Code (EPC) could solve both of these problems. The latter problem, visibility, is trivially solved by the RFID tag's remote readability. The former is solved by the 96-bit EPC, long enough to uniquely identify every product ever made. Using the EPC as an index, an object-name server can be queried and the product's size and weight, best-before date, place of manufacture, shipping details, or any other information can be retrieved. This system will further increase the yearly savings provided to retailers by RFID technology. WalMart, which expects to save $407 million annually with pallet-level tagging, would likely see that amount increase to $7.6 billion under item-level tagging. [McHugh, 2004]

Most industry experts agree that item-level tagging is at least a decade away. Why, then, are so many privacy advocates already up-in-arms about the practice? There are two main reasons. First, the initial monetary outlay on infrastructure improvements necessary to incorporate item-level tagging into the supply chain is large enough that a company is likely to take full advantage of any applications the system provides, ethical or not. It is unlikely that responsibility will come after adoption; it must be guide the design phase. Secondly, the fact that widespread adoption is years away does not mean that there are not disturbing tests of the technology being conducted on an unwitting public. There have been two separate instances, one in the US [Wolinsky, 2003] and one in the UK [Jha, 2003], in which RFID-enabled packaging, combined with so-called 'smart shelves,' allowed for a disturbing level of customer surveillance. In the former instance, tagged tubes of Proctor & Gamble (P&G) lipstick, when taken from the shelf, activated a video camera whose feed was watched by P&G representatives interested in how consumers interacted with their product. In the latter case, picking up a tagged Gillette razor activated a hidden camera which took a picture of the customer's face. Later, the same package activated a camera by the store's exit. The pictures were then compared by security guards; the store's manager later admitted that they subsequently turned over pictures of suspected shoplifters to police.

However, secret surveillance is not the procedure which raises the ire of most privacy advocates (though the tests mentioned above did lead to boycotts of both companies). The most problematic issue is consumer tracking. It is to be expected that, as an anti-theft measure, stores will have an RFID reader positioned at every exit. The presence of such a reader means that any live tag carried by an individual entering that store will also be read. Should clothes have tags woven in to their fabric (as planned by the Benetton company, but abandoned after protests), they will be able to act as a *de facto* personal identifier. Items such as shoes, which may be worn daily, could then become a quick index number for every store a consumer visits, thus creating a detailed picture of his or her daily activities. The existence of information-hungry marketers means that such a scenario is not particularly unlikely. Furthermore, if a single store chooses to connect payment information with RFID information, it is no longer the actions of an unknown person that are being collected; it is the actions, purchasing habits, and whereabouts of a specific individual. It may be true that tracking from store to store is unlikely to be done by any particular retailer; however, if information in various retail databases were

combined, an aggressive marketer, private investigator, or anyone else with access may construct a very detailed picture of the life of an unsuspecting individual.

The security of an individual may also be compromised by such a scheme. If a person with a scanner is able to quickly determine the contents of a shopping bag, he or she may be able to determine whether it would make an appropriate target for theft. Should cash ever have tags added (as a European Union initiative proposes), everything of value carried by a person could be identified at a distance.

These technological threats may seem remote or unlikely, but they are certainly not infeasible. Are consumers willing to risk even a small chance of these scenarios coming to pass, particularly when they will see little to no benefit themselves? More importantly, shouldn't they at least be given a choice? As RFID pushes further ahead, it has to be ensured that the public voice is not ignored; at the very least, it must have a say on how item-level tagging information is collected and used.

5.2.2. Human Implants

If item-level tagging is a bad dream for privacy advocates, human RFID implanting is a nightmare. This concept, previously limited to dystopian science-fiction, became a reality on December 19, 2001, when Applied Digital Solutions (ADS) introduced the VeriChip. This chip, encased in a glass container approximately the size of a grain of rice, is injected into the fatty tissue below the recipient's tricep, thereby becoming a "secure, tamperproof technology providing immediate identification and access to subscriber-supplied information."[3] ADS sold around 7000 VeriChips for human applications in 2004, including 160 for implantation into Mexico's Attorney General and his staff. [Murray, 2004] There are two bars, the Baja Beach Club in Barcelona and the Bar Soba in Glasgow, which offer patrons VIP status if they are willing to have a VeriChip inserted. Also, the United States Food and Drug Administration (FDA) has approved the chip for use in patients, to provide quick access to medical records. Once again, though, privacy advocates are concerned. ADS claims that the information stored on their system is secure and password-protected, and that their chips can be read only by proprietary readers. Time, however, has a tendency to prove technological statements such as these to be incorrect.

It is not simply the security of the information stored by these chips that has activists worried, however. Rather, it is also misconceptions about the potential benefits of the VeriChip which are of concern. For instance, Mexico's Attorney General and his staff were convinced to accept the implants in the belief that they would be an effective tool in the fight against the rampant kidnapping that occurs in that country. However, VeriChips are passive, and thus do not broadcast their information unless scanned by a reader. Unless extensive networks of readers are created, this technology can do no more than identify a kidnapping victim once he or she is found. In response to this criticism, ADS has developed a prototype personal security chip, which includes a Global Positioning System (GPS) tracking unit that transmits its location via a cell phone carried by the user.

[3] 4VeriChip. (2004) http://www.4verichip.com.

However, as Madeline Albrecht of Consumers Against Supermarket Privacy Invasion And Numbering (CASPIAN) notes, "When someone steals a car, the first thing they disarm is the locator device." [Murray, 2004] Kidnappers will obviously know that this technology exists; in fact, a recently-broken kidnapping ring known as "Los Chips" is already known to search its victims for chips that can aid in their location, and destroy any that are found. Since the chips are always injected into the same location, we are left with a grisly scenario in which identification chips can be removed from their owners. Such an action not only compromises the chip's usefulness against kidnapping, but also for identification, as removed chips could quickly be reinserted into another person. It is unlikely that a Baja Beach Club patron will have his or her chip removed for this purpose, but should banks, or government agencies, begin using chips for access to high security areas (as is proposed by ADS), these chips will become very valuable, and this scenario more likely. While it may be more difficult to steal this form of identification, it is certainly not impossible.

ADS lists three benefits that can be had through the use of VeriChips.[4] The first is that the chips are a "secure, tamper-proof microchip technology providing immediate identification and retrieval of subscriber-supplied information at VeriChip Affiliates." However, this is a benefit of RFID in general, and can be had with use of a pass-card. It is true that a pass-card is more easily lost or stolen than a VeriChip, but the privacy issues associated with the implantation of a chip seem to be a heavy price for this nominal security improvement. The second benefit listed is "password-protected, secure access to your information." This is not a benefit of the VeriChip, so much as a secure database. Third, ADS mentions "support from a growing number of VeriChip Affiliate Financial, Security, and a number of other organizations worldwide." However, since there have been only 1000 chips actually ever implanted in people, how large can this number be? Even if it were a high number, this argument reduces to the fact that these chips add convenience, again, a seemingly poor reason to allow oneself to be remotely identified by anyone with a reader.

Thus, the benefits as seen by the product's maker seem to be convenience and a cure for forgetfulness; roughly the same rationale as pinning a child's mittens to his or her coat. These must be measured against the fact that the chip has all the same tracking and security issues of item-level RFID-tagging, combined with the fact that this tag can never be removed or disabled. Should the company's prototype GPS-enabled unit ever come to market, there is the added drawback of now having an actively transmitting beacon implanted that cannot be disabled or removed. What person would ever choose to have such a device implanted? Perhaps people will not have a choice. Parents may choose to have such a unit implanted in their child at birth, particularly in a country like Mexico, of which the director of Solusat, the company which sold VeriChips to the Attorney General's office, said, "we have more than 150,000 missing kids ... when you're looking at so much kidnapping, privacy concerns become less important." [Murray, 2004] What happens, though, when the child grows up? Can the chip be removed after 18 years? What if they aren't told of the implant? Perhaps this is the scenario that must be protected against; should a person be educated about the pros and cons of the VeriChip,

[4] VeriChip Benefits (2004) http://www.4verichip.com/verichipbenefits.htm

and still choose the procedure, so be it. However, if those who are incapable of consent begin to be injected with an identification microchip, privacy advocates certainly should raise an alarm.

5.2.3. RFID-chipped Passports or National ID Cards

While the previous two problems both create disturbing potentials for attacks on personal privacy, they are not necessarily immediate threats. Item-level tagging is at least a decade away by most estimates, and the idea of implanted chips is still surrounded by an aura of 'creepiness' which will likely keep them from being widely deployed anytime soon. However, there is a threat which must be addressed immediately, as it is already present. This threat is RFID-chipped identification, such as the passports which the United States will begin issuing in August 2005. In response to the terrorist attack of September 11th in New York City, the US has made a concerted attempt to create more secure and difficult to forge identification, and they believe that the way to do this is with an embedded RFID chip. The passports are based on a standard developed by the International Civil Aviation Organization (ICAO), a group sponsored by the United Nations, which insists that the passport must carry a chip that will store all the information printed on the passport, along with a digital photograph and at least one biometric identifier.

These passports raise hosts of privacy issues. The problem of skimming, in which the passport information is read without the knowledge of its holder, could become a serious concern. A person's name, address and date and place of birth could easily be obtained by identity thieves. More disturbingly, the nationality of a person could quickly be established when traveling abroad. This information is very valuable to pickpockets, kidnappers, and terrorists. In a busy marketplace, it would not be difficult to bring a hidden reader within the necessary 10-20cm read range of the chips. Once a person's identity has been established, his or her value as a target can then more easily be established. Skimming would also allow a government representative to quickly identify any attendees of a political rally or religious ceremony who happened to be carrying this chip. Also, when the information has been skimmed, it can be copied onto another chip and used to forge a copy of a passport, as all the necessary printed information will have been retrieved in the process. Finally, when traveling, many people carry their passports at all times; thus, the possibility of surveillance and tracking using passports is created. Such a situation is likely when it is probable that passports will be the most secure form of ID for many people, and will thus be requested for presentation by airports, banks and government offices, effectively making them *de facto* national ID cards.

Again, though, it is perhaps not the potential abuses of this new form of identification that is most disturbing. Rather, it is the lack of effort to prevent these abuses. Many possibilities for securing the card's information, including encryption, have been presented to the US, and all have been rejected. A technical report published in May 2003 recommended that "encryption and digital signing be used to preserve data integrity and data privacy." [ACLU, 2004] It also noted that authenticating users before sending data would help provide confidentiality and prevent skimming. A further proposal was

made to print a physical bar code on the machine-readable zone (MRZ) of passports, which would be the key needed to unlock encrypted data on the chip. The benefit provided by this scheme would be that the passport would have to be opened to be read, and thus could not be read without knowledge of the owner. Each of these proposals was systematically rejected in statements made by the US. On encryption: "Data written to chip and data exchanged between a reader and a passport will be free and clear without the need for encryption." [ACLU, 2004] On authentication: "The U.S. position is that terminal authentication should not be required." [ACLU, 2004] On the use of the MRZ: "The U.S. position is that the MRZ should not be used for this purpose." [ACLU, 2004] The only piece of security that was accepted, and thus incorporated into the ICAO standard, was a digital signature for the data. This signature serves to verify that the information on the chip has not been altered, but does nothing to protect privacy of the data. This lack of security met with great protests from many other countries, including Germany, the UK, Canada and the Netherlands. However, the ICAO bowed to the US position, and chose to agree with it on every security issue. [Note: In April of 2005, after extremely negative reactions from both the public and academics the US gave in to pressures to protect the passport, and agreed to add a hash key to the MRZ, as well as encrypt data during transmission.]

There are two more problems that arise in the analysis of the use of RFID in passports, however. The first, mentioned by Electronic Frontier Foundation attorney Lee Tien, is that regardless of the encryption being used on these passports, it is inevitable that identity thieves, terrorists and others will get their hands on the necessary readers. [Singel, 2004] He notes that 180 countries will need to have the technology for reading these passports, and thus, secure system or not, it is bound to be leaky purely from a technological standpoint. He says, "Any reader system, even with security, that was so widely deployed and accessible to so many people worldwide will be subject to some very interesting compromises." [Singel, 2004]

The second problem that arises is noted by the director of the American Civil Liberties Union's Technology and Liberty program Barry Steinhardt [Singel, 2004] and noted security expert Bruce Schneier [2004]: specifically, there is no good reason to have RFID-tagged passports. Both have publicly asked the question, "Why have a chip that can be read remotely?" Even if the fact that the data should be stored on a microchip is taken as necessary improvement, what is gained by making that chip readable at a distance? If these passports are used exclusively in the way that they are intended, that is, only ever scanned by those with authorized scanners, why not force the chip to require contact with the reader to be activated, rather than giving a 10cm read range? The difference in effort needed is minimal, while the difference in privacy is huge. Similarly, if, as has been proposed, the cover of the passport is constructed to be an electronic shield, meaning that the passport can only be read when opened, why not add a bar coded encryption key to the passport? The passport is already open, so again the difference in read time is minimal, but the data on the passport can be encrypted. There seem to be no benefits to using RFID in this situation other than to allow the surreptitious reading of passport information. Given that, one must ask the question, why? Why risk the privacy and safety of citizens, at a time when ID theft is at an all-time high (as is, possibly, anti-

American sentiment abroad), for the few benefits of an unencrypted, remotely-readable passport? While it is tempting to attribute this plan to plain incompetence or ignorance, it seems as if the motives may be more sinister. In the words of Bruce Schneier, "this seems like a clear case of the Bush administration putting its own interests above the security and privacy of its citizens, and then lying about it." [Schneier, 2004]

5.3. Possible Guidelines and Solutions

In the past few years, numerous groups and individuals have published documents describing the threats to privacy posed by RFID and presenting possible solutions, as well as proposing guidelines for proper deployment of the technology. These groups include the Electronic Privacy Information Centre (EPIC), the American Civil Liberties Union (ACLU), Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the Ontario Privacy Commissioner's Office, the European Privacy Commissioners' Data Protection Working Party 29 and countless others, including the RFID industry itself. This section will describe the views of these groups, and examine the feasibility of some of the proposed solutions.

5.3.1. The RFID Bill of Rights

Encapsulating the general consensus of most privacy advocates is RFID- and privacy expert Simson Garfinkle's RFID Bill of Rights, a set of regulations that he believed would serve as a framework that should be voluntarily followed by any company wishing to use tags in their dealings with the public. The five rights he proposed were:

- The right to know whether products contain RFID tags.
- The right to have RFID tags removed or deactivated when they purchase products.
- The right to use RFID-enabled services without RFID tags.
- The right to access an RFID tag's stored data.
- The right to know when, where and why the tags are being read. [Garfinkel 2002]

These rights were initially developed in response to a foreseen proliferation of RFID tags in the marketplace, but can easily be adapted to any deployment. They are based on two main principles: awareness and non-coercion. He admits that at times, these rights may have to be compromised. For instance, federal legislation may decree that certain safety critical components of vehicles must keep their tags, as an aid to the recall process. However, in general, the public should not be forced to play an elaborate game of 'hide-and-seek' to determine the presence of tags or readers. It must also be informed, or at least have access to information, about the purpose of RFID usage. By making information available, accountability will be encouraged, as retailers will be more likely to reconsider marginal uses for the technology if the public is aware of them. Also, those who use RFID should not be able to coerce the public into using or keeping tags. This coercion can be subtle; for instance, the Massachusetts Turnpike Authority gives discounts to those who use RFID-transponders at tollbooths, essentially punishing those

who refuse to carry such a transmitter. Other examples include allowing receipt-less returns of merchandise only if the RFID tag is still active and attached, or faster processing of travel documents at an airport for those with RFID-enabled passports. Protected privacy should be the default condition, rather than only being available at a premium.

5.3.2. Fair Information Practices

The principle of Fair Information Practices (FIPs) is the cornerstone of data protection law throughout the world. As such, many groups, including the International Conference of Data Protection & Privacy Commissioners [Cavoukian 2004], have used FIP to model their responses to the challenges posed by RFID. There are three main principles in the proper collection of data, which the RFID industry has agreed need to be addressed. These principles are notice and consent, choice, and control of data. In relation to RFID, these standards mean that all readers and tags must be clearly labeled, and participation in any RFID data collection scheme must be voluntary; all consumers must have the right to have tags deactivated or removed after purchase, without cost; and that consumers must have the right to prevent personally identifiable information from being associated with an item's tag. These are noble principles, but they are also sufficiently self-evident that it is safe to assume that they will be recognized and accepted. These are not the only procedures outlined in FIPs, however. Position papers from the Ontario Privacy Commissioner [Cavoukian 2004] and a consortium consisting of CASPIAN, EPIC, the ACLU and others [CASPIAN et al., 2003] have described the need for the enforcement of some of the lesser known principles, such as:

- **Openness**: Developments, practices and principles should be made openly available to the public.
- **Purpose Specification**: Users must give notice of the purpose of data collection.
- **Collection Limitation**: Data should only be collected for the purpose at hand. Also, users should consider alternate methods of achieving their means before adopting RFID.
- **Accountability**: Users must be responsible for the implementation of the system, and the collection of data. This must be done through legal responsibilities in complying with these principles.
- **Security Safeguards**: Personal data must be protected through reasonable security measures from the risks of loss, unauthorized access, destruction, modification or disclosure.

These groups argue that it is only when all these issues have been addressed that the public will be accepting of widespread RFID use, which might give strength to the saying, "Good privacy makes good business."

5.3.3. Technical Solutions (and their failings)

Many people take issue with guidelines for proper use of RFID because they have no power until they are supported by legislation. Many countries have data protection laws currently in effect, but no country has any bill which addresses specifically data collected from RFID chips, or the ways in which that data can be gathered. Some individual American states, such as New Mexico [Swedberg, 2005], have attempted to introduce bills which would require a retailer to remove or disable tags after purchase, but none have been passed as of this writing. Not surprisingly, RFID users have claimed that no law is needed, as those companies testing RFID implementations are 'committed to protecting privacy.' [Gross, 2004] Additionally, they note that there are numerous technological methods which can be used to prevent RFID tags from being read surreptitiously. A sampling of these methods follows, along with the failings of each.

Aluminum Foil

The least technological of the forms of protection, aluminum foil is also the easiest and cheapest, and will likely be the most widely used privacy protection 'technology.' An RFID-enabled chip, when wrapped in foil, cannot be read. Any conductive metal has this property, and thus a screen may be added to passport covers, for example, to ensure they cannot be read unless opened. However, there are limits to how many chips can be protected in this way. A passport can be protected, as well as any RFID-tagged cash that may be in your wallet. However, tagged clothing will still be vulnerable, as will ID implants, and any other tags that cannot conveniently be covered. Aluminum foil is a quick fix to passport privacy issues, but it is not a realistic long term solution.

Tag Killing

In the realm of item-level tagging, 'tag killing' is often pointed to as the solution to privacy issues. Most RFID tags have a built-in 'kill' feature, which when activated renders the tag inoperable. If this were to be done at the point of sale, it is argued, then privacy would be unaffected by the dead tags. While this statement is true, CASPIAN and others have argued that it does not mean that tag killing is an effective solution to the privacy problems arising from item-level tagging. [CASPIAN, 2003] First, it is noted, this practice does nothing to halt in-store tracking. Given that RFID-enabled shelves have been used to trigger hidden cameras and video feeds, pre-purchase privacy needs to be addressed as well as post-purchase privacy. Secondly, incentives or disincentives may be used by a company to coerce a customer into carrying a live tag home. It is possible that 'killer kiosks' could be used as the kill mechanism, forcing those who do not trust live tags to wait in another line to disarm them, as well as singling themselves out as being 'paranoid.' It is also possible that a store may offer faster returns on products with live tags, or a theft-retrieval program in which high-value items can be registered to their owners, and potentially returned upon recovery by the police. Also, products may use their tags for more than simply inventory purposes. The potential exists for development of a 'smart' microwave, for example, which would read the tag of the item to be cooked, and instantly be able to retrieve proper cooking instructions. One final point is that since

conscious action is required on the part of consumers, two classes of shoppers may be created by tag killing: those who care enough to disable the tags, and those who don't. Membership in either class may have negative ramifications.

Finally, the Article 29 Working Party [2005] mentions that all tag kills are not the same. A tag can be killed completely, by scrambling its data or disabling a fuse. However, a temporary kill could also be achieved by using a software lock, or by other mechanical means; this would allow the tag to be 'woken up' and read in the future, with the knowledge of the tag's carrier. Also, another idea has been presented to simply overwrite the data on the tag with zeroes. When tags are widespread, this may be an effective 'kill' alternative, but initially the mere presence of a zeroed tag will present valuable information, as reasonable guesses may be made as to the origin of the tag, knowing that only limited stores will follow the practice. Thus, while tag killing may seem to be an effective privacy measure, there are many questions about it which must be answered before it can be accepted as a true solution to RFID's privacy problems.

The Blocker Tag

On the assumption that many people would not disable many of the tags which come into their possession, whether by desire for a live tag or apathy, RSA Laboratories developed an alternative method to protect privacy: the blocker tag. This tag is able to effectively block the functioning of a reader by broadcasting every possible RFID identification code, thus preventing the reader from discerning valid information from a legitimate tag from garbage being sent by the blocker. The ingenious technical specifications for the tags are presented in a paper by Juels, Rivest and Szydlo [2003], and are well worth reading, but shall not be discussed further here.

The blocker tag seems to create a good halfway point between aluminum foil and tag killing. Assuming, say, a 1.5m read range for this tag, a single blocker tag could create a zone of privacy around an individual, in which every other tag carried cannot be read, effectively being 'dead' within its sphere of influence. However, tags would remain functional, should a person require them for any purpose. Also, all tags that are carried would be affected by the blocker, including implanted IDs and passport chips. Since these tags are only slightly more complicated than regular RFID tags, the marginal cost to manufacture such items would be nominal, in the range of 10-20 cents, and thus they can be sold to the public for a small price, or given away by a company wishing to appear strong on privacy protection.

Unfortunately, there are many problems with the blocker tag solution. First, by providing a sense of security for those who carry one, it will promote further widespread RFID deployment. This is certainly a problem for any person who does not know of such a tag, or forgets to carry one, or is apathetic towards tags. Secondly, it is possible, if not likely, that these tags will quickly be banned in many areas. If a store's security system is based on RFID, it will be eager to prohibit blocker tags from being used within their confines. Similarly, blockers will likely not be allowed within airports, as they will affect the identification (and tracking) of those with electronic passports or RFID-tagged

tickets. Many other scenarios will arise in which these tags are required to be disabled temporarily; eventually, it may become more convenient to simply not carry one. Third, this solution again shifts the burden of privacy protection to the consumer. Assuming that every individual will be well versed on the dangers of RFID (or any other technology) is unrealistic; the companies dependent on RFID should be ensuring that the tags are being used responsibly, not those who carry tags.

5.4. Analysis of the Situation

5.4.1. A Critical Point for RFID

The deployment of Radio Frequency Identification is currently at a crucial point, as the industry is faced with a public that is becoming knowledgeable, worried about the implications of the remote data collection, and angry about perceived abuses of the technology. Surveys have revealed a recent 45% increase in the proportion of people aware of RFID, from 28.2% in September 2004 to 40.8% in March 2005. [Big Research, 2004] The majority of this group is not simply aware of the technology, but is in fact knowledgeable, as 68% rate themselves somewhat or fully aware of how retailers intend to use RFID. [Big Research, 2004] However, with this knowledge comes fear. Of those aware of RFID, fully two-thirds are worried that information being collected about them will be shared without their consent. [Big Research, 2004] Even when groups are educated directly by the RFID industry, they tend to react negatively to the technology. Confidential documents leaked by the AutoID Center, an RFID developer, revealed that 78% of those interviewed reacted negatively when questioned on how they felt the technology would affect their privacy. [Kim, 2001] More than half were extremely or very concerned, and in 15 separate cases the term 'Big Brother' was used in describing RFID. Dislike for tagging is not solely to be found in survey data, however, as the general public has reacted angrily to what are seen as inappropriate uses of tags. For example, on January 30, 2005 the Brittan School Board in Sutter, California received a complaint from a parent about a test being conducted by the Brittan Elementary School, in conjunction with the company InCom, in which students were forced to wear RFID-chipped ID cards around their necks. No notification of the test had been given, as parents found out about it when their children came home wearing the IDs. By February 8, EPIC, EFF and the ACLU had taken up this parent's cause, and written a joint letter to the school board condemning the practice. [Ozer, 2005] By this time, the test had begun to receive a flood of media attention, almost universally condemning the practice of tagging children, comparing it to the tagging of inventory or livestock. The protest became so strong that it in fact resulted in the termination of the program on February 15. ["Victory...", 2005] This case showed that not only are the opponents of RFID ready and willing to mobilize at a moment's notice, but that the users of RFID recognize that such a public outcry cannot be ignored. The RFID industry needs to find a way to convince the public that their privacy is not at risk due to these tags for RFID to have hope of being accepted as a beneficial technology. The question must then be asked, 'in what way can this be done?'

5.4.2. Is Legislation the Only Viable Option?

The privacy problems that come with widespread RFID deployment will not be easily solved, but they still must be addressed. In order to do this, it must first be determined how these issues can best be handled. This paper has previously discussed technological means of protecting privacy, and also mentioned the ways in which such solutions will fail. Those failings are certainly not limited to the technologies described, however. Any device of that type will create two classes of citizens: those who actively protect their privacy, and those who don't (due to choice, apathy or lack of information). Further, any technological protection measure can be outlawed in, say, a time of emergency, leaving the privacy of the average citizen at risk. Since consumers are already wary of technological means for privacy protection (the aforementioned AutoID Center Study noted that people found the argument that tags could be turned off, and thus privacy protected, 'unconvincing' [Kim, 2001]), it is highly unlikely that any technological solution will allay the public's fears of an RFID-driven Big Brother. It is also very improbable that a system of voluntary guidelines to be followed by RFID users will remove the public's worries. As previously noted, already 30% of a randomly sampled group of 8500 people both know of RFID's uses and fear that data collected about them will not be safe. This group will not be pacified by a reaffirmation of the RFID industry's commitment to privacy protection. It will quickly be seen that without some strong force monitoring the truth of the statement, this commitment is rather toothless.

What option remains? Legislation. Though RFID makers and users may object, it must be seen that this technology poses unique privacy threats which must be addressed before the public will be accepting of it. Through the introduction of appropriate legislation, accountability will be introduced to the industry, and the public may come to understand that it now has legal recourse against any company which abuses the technology, and may thus come to be more comfortable with its presence.

5.4.3. Legislative Choices

It should be noted that RFID is not a company's sole option for data collection. Multi-billion dollar companies exist in the United States, such as Acxiom, ChoicePoint, and LexisNexis whose sole function is to collect and sell data about individuals, which is done by scouring public records and acquiring existing databases. Many laws are already in existence which govern this collection and trading of information, from which data collected by RFID systems will not be exempt. It is true that many would argue that these laws are insufficient; this chapter will not debate that point. Rather, the focus will be directed toward regulations concerning the uniqueness of the way in which RFID allows data to be collected.

RFID poses a threat to privacy due to its ability to allow data to be gathered surreptitiously. Most forms of data about a person only come into existence because of an action undertaken by that person, whether it is using a store loyalty card, using a building access fob, applying for a driver's license, or one of hundreds of others. Many

uses of RFID tags will fall under the same category of voluntarily provided data, such as using an electronic pass to pay for toll booths, or scanning a tag at a checkout counter. However, much of the personally identifiable information collection done via RFID can occur without the subject's knowledge. It is this information that must be protected legislatively.

The author feels that there are three main point of legislation which must be addressed:

- limiting retail RFID use
- prevention of hidden readers
- prevention of RFID chips in driver's licenses

In the retail setting, prevention of the surreptitious collection of personally identifiable information is remarkable easy. A 96-bit EPC, as would be stored by an item-level tag, contains 4 sections: an 8-bit Header (identifying version number), a 28-bit EPC Manager (storing the manufacturer name), a 24-bit Object Class (storing the exact product type), and a 36-bit Serial Number. ["The EPC Network", 2005] If a retailer were allowed to read tags, but not allowed to store the tag's serial number (except if the item in question is unpurchased), it would be much more difficult to develop individual shopper profiles, while still allowing for a company to garner any marketing information it may desire from the type of product. Further, if the tag being read turned out not to be an EPC, but instead were from an ID card, say, that information could be immediately deleted. Legislation such as this would likely draw criticism from both sides (privacy advocates claiming this is still too much information, the RFID industry claiming it is too limiting), but it seems to be a reasonable, and technologically feasible trade-off between information and privacy. Secondly, legislation should be introduced to force readers to be conspicuous. The notification of a read having occurred could be in the form of a light or a sound, but reading without any form of notice should be strictly prohibited. Again, while this does not prevent reading from occurring, or place an undue burden on RFID makers, it will allow for the public to be aware of the technology, and to take appropriate action should they feel it is invasive. Finally, RFID tags should not be allowed to be incorporated into driver's licenses (a bill which is being examined in the state of California). The driver's license is frequently the only piece of identification (excepting a passport) which is accepted in many everyday situations, and is thus carried at all times by many people. Adding an RFID chip could then not only allow for individuals to be identified surreptitiously at any time, but also cause more establishments to depend on electronic identification, which will promote the spread of RFID in identification documents, causing more establishments to use electronic identification, and so on, eventually leading to an uneasy ubiquity of RFID which must be carried at all times.

Other points exist, such as that stores should have to provide the ability to kill or remove tags with no penalty to the consumer, and to clearly label RFID-tagged items as such. However, these measures are currently being voluntarily complied with by RFID-users, and are unlikely to be removed even absent legal necessity. It is felt, however, that the three points suggested above will be contentious, and require the powers of government to be enforced. By introducing these legislative protective measures, and

fully educating the citizenry on issues concerning RFID, the industry might find that it is able to gain the necessary public acceptance.

5.5 Conclusion

RFID is a well-established technology; that cannot be changed, nor should it. Used correctly (and carefully) it can be very beneficial for all parties involved. However, when tags begin to be associated with individuals, privacy is threatened. Item-level tags, human implants and RFID-chipped passports are all realities of the near future; it must be ensured that expanded personal marketing, a lack of anonymity and human tracking are not. Good RFID use policies and privacy protecting technologies, while providing a good first step, are not enough to protect individual privacy. RFID is a new type of threat to personal information and must be treated as such; indeed, it must be recognized that existing privacy legislation is not adequate. New laws must be passed to control the use of RFID if it is to be welcomed by an already skeptical public; the three points of necessary legislation listed above will be a necessary beginning to the control process.

6. Anonymity & The Internet

6.1. The Foundation of the Internet?

In 1993, *New Yorker* magazine published a now-famous cartoon by Peter Steiner, which was captioned "On the Internet, no one knows you're a dog." This statement quickly became a mantra among researchers, journalists and 'net users, and for good reason. No realm is more synonymous with anonymity and the ability to hide or modify one's true nature than the Internet. The vast majority of online interactions take place between "avatars", a word which is well known throughout the computing world. An avatar is defined as "a temporary manifestation of a continuing entity," [American Heritage Dictionary, 2000] exactly the reality of a person's online presence. Online, one is as he or she chooses to be. A person can control multiple avatars, each used in different situation, or develop a fully-formed personality (whether the same as or radically different from the person him- or herself) in much the same way a novelist creates fully elaborated characters. Alternatively, one could choose to be a 'lurker', a presence which observes but does not act upon a particular community; there are near-endless possibilities. This ability to break free from one's 'real world' identity allowed thousands of people to step beyond their mental boundaries and explore new ideas, new personality traits, and even new genders. Cultural taboos, shyness or disabilities could be ignored when constructing one's avatar, on the assumption that the thin connection between that manifestation and the actual could be severed at any time. Of course, we now know that this severance was not always possible, as electronic traces like IP address were often left in the avatar's footsteps; however, this fact was either ignored or discarded by many early Internet users. In fact, this author would argue that it was the Internet's provision of anonymity (or the appearance thereof) which popularized it, and turned it from a research tool to a massive public network.

The question must be asked, then: 'Why did the Internet develop in this manner?' As will be described in section 6.3's tale of anon.penet.fi, many researchers would have preferred for every online interaction to carry with it some proper identifier of the actual people involved. This did not happen, as even now one can interact on the 'net with practical (and, arguably, actual) anonymity. However, the reasons that a system of universal online identification did not occur are not fully known. Certainly, there were technical limitations. The creator of anon.penet.fi, for instance, did so in order to prove that any measure undertaken to enforce such a system could easily be circumvented. It seemed that those who wanted the ability to keep names hidden were as knowledgeable as those who wanted the names exposed. However, technological savvy was not enough reason to fight against online identification; the community must have had some philosophical reason for wanting the ability to remain anonymous (or, at least, pseudonymous). Below, we present some possible philosophical foundations for the presence of online anonymity.

6.1.1 Michel Foucault

In 'Author Function' [Foucault, 1977], Michel Foucault outlines the functionality of attributing the authorship of works to their writers. He notes that initially this practice was not done to allow an author to maintain ownership of his work, but rather it was done when the author became subject to punishment. Transgressive works were considered dangerous, and thus penalties for their writing were meted out. It was only when copyright laws were established that authorial identification became desirable to a writer. Furthermore, he notes, there was a time when so-called 'literary' works were accepted anonymously without question, with their age standing in as guarantee of authenticity, while scientific papers were only considered truthful based on the reputation of their authors. However, as controlled systems of truths emerged, the names of authors of scientific texts no longer became the index of truth, and the papers were accepted on their own merits. It is true that authors still provide a measure of both reliability and the resources available during the experiment, but the description of a duplicable result is adequate to establish scientific truth.

The author function strongly relates to the concept of online anonymity. On the Internet most interaction takes place through a textual interface. Authors of newsgroup postings are not substantively different than authors of philosophical or scientific treatises: both desire their works to be examined for their innate truths, not for the name of the writer. By Foucault's theory, this should be possible without the sacrifice of anonymity. Furthermore, many Internet posters do not desire to maintain possession of their postings; copyright of messages posted in chat rooms or on newsgroups is almost non-existent. Thus, what does the assignation of authorship provide for the online participant? The initial function: punishment. By identifying the person behind a posting, that person is exposed to accusations of libel or copyright infringement, and threats of embarrassment or harassment. Authors in the physical world may have much to gain from having their names known, but mandatory identification is generally only detrimental online.

6.1.2 Jacques Lacan

The legal implications of anonymity are certainly not the only reasons that it became a cornerstone of the online world. Much more subtle arguments can be made about its necessity, one of which can be found by examining the world of psychoanalyst Jacques Lacan. In 1949, Lacan described the *mirror stage* [Lacan, 1949] of an infant's development as the stage in which the child, though still intellectually inferior to a chimp, views itself in a mirror, and in recognizing the reflected image as such, identifies itself and begins the formation of the ego, or the *I*. This is a traumatic process, which in the end "turns the *I* into an apparatus to which every instinctual pressure constitutes a danger, even if it corresponds to a natural maturation process." [Lacan, 1949] The child now must interact within the social world, and is no longer able to maintain its blissfully free fragmented self-image.

Online, our avatars are the children of our minds. They are created, generally fragmented and poorly formed, and allowed to interact with others. When avatars are seen as

separate from the individual, they never need to form their own ego, or at least never need to be associated with the ego of their creators. Thus, they (and by extension, their controllers) are allowed to freely explore the digital environment. However, in a situation where anonymity is forbidden, these manifestations are forced to look in the mirror, so to speak. The creator is forced to identify him- or herself with the avatar, and by doing so must undergo the same formative traumas as he or she did as a child. This is a natural maturation process for humans, but it is painful, and there is no reason that a human avatar need undergo it. By allowing others to discover the true name behind the mask, we remove the freedoms of the fragmented self-image, and now force the avatar to conform to the same social pressures that its creator faces. Freedom to experiment in ideas and identity is removed, and the Internet becomes a communications tool, rather than a new mental realm. Clearly this is not desirable for Internet users, and thus another reason that the ability to remain anonymous was vital to 'net development.

6.1.3 J.L. Moreno

Examining the work of the previous two researchers has allowed us to shed some light on why the Internet developed by allowing anonymity. Examining psychologist J.L. Moreno's treatment method, called Psychodrama, will allow us to see why anonymity became a vital aspect of 'net culture. Psychodrama is a method of group therapy in which participants actively explore one another's problems using techniques such as role reversals, mirroring, or doubling in an attempt to allow them to become more spontaneous and independent. Moreno believed that through the spontaneity and creativity of role play, healing of the mind, body and spirit would occur. [Casey, 2001] He also believed, though, that for spontaneity to occur a safe and playful environment must exist, in which the group participants must be free of any consequences of exploring new attitudes, beliefs and behaviours. Anonymous participation in Internet culture certainly creates this environment; thus the online realm has become a haven for those looking to explore new knowledge, or new identities. This exploration of identities, Moreno would argue, is very spiritually beneficial. The benefits of, and the necessity of anonymity for, online role-playing are discussed in the next section.

6.2. Identity Exploration

The statement "On the Internet, no one knows you're a dog" is interesting to examine. Clearly, it overstates the reality of the situation for comic effect; any Internet user can (hopefully) differentiate a human conversational partner from any other type, excepting perhaps some artificial intelligences. However, can anything but species be determined about an entity at some far distant keyboard? A skilled communicator can fake the dialogue of a member of another race, age group, or gender, making identification due to conversational clues quite difficult. Photos and webcam images can be, and frequently are, modified to alter the visual appearance of one's discussion partner, and thus are unreliable. [So unreliable, if fact, that there is significant debate about the admissibility of digital photography in criminal trials.] Beyond the physical description of a person, personality traits can also be enhanced or hidden when online; the boastful Internet Lothario is frequently timid and socially awkward in an offline setting. In fact, general

Internet wisdom states that the safest online assumption to make is that no-one is really who they claim to be. This does not lead to mass distrust in social forums, however, so much as the realization that one is interacting with adopted personae when online. These are no less 'real' than the personae of their physical world counterparts, simply a new creation or extension. Importantly, by accepting this occurrence and providing an anonymous, consequence free environment, the Internet allows people to freely experiment with character traits, and undergo the vital psychological process of identity exploration when online.

Identity exploration has been praised by a number of psychologists and psychoanalysts. As previously mentioned, J.L. Moreno believed that one of the best ways of approaching psychological traumas was through role play. By exploring characteristics that may be foreign to, or repressed in, one's own nature during role play sessions one could learn how to adopt those traits, should they prove beneficial. This type of play also allowed for the child-like aspects of the self to emerge, which he believed were powerful elements of integration for a fragmented psyche. [Casey, 2001] Psychoanalyst Erik Erikson also saw the benefits of identity exploration, and in fact identified it as an absolutely necessary aspect of human development. The fifth of his eight psychosocial development stages was named 'Identity vs. Identity Confusion.' This stage generally happens during adolescence, when a person must develop a vocational identity, cultural identity, sexual identity, personality, and many other character traits. However, as the number of choices available to an individual increase, establishing this sense of who one is becomes increasingly difficult. [Palmer, 2005] It is in this stage, which begins in adolescence but may now extend throughout the lifespan, that one finds the 'identity crisis', in which an individual cannot discern his or her rightful place in the world. However, by providing a forum in which an individual can freely experiment with various potential identities, these crises need not be harmful. New identities can be tested without abandoning current ones, allowing smarter, more rational choices to be made, without the consequences associated with 'giving up' one's old life.

Statistics are hard to develop about the number of people who have taken advantage of the Internet's explorative capabilities, but it is safe to assume that the majority of people have at least in some way tried a new identity. This is not to say that the average person has lied about who he or she is, or explicitly tried to be something that he or she is not. Rather, it is simply an extension of our real world multiplicity of identities. Most people will show or hide different aspects of their personalities, depending on the situation: employee Joe, husband Joe and sports fan Joe are simply different personae of the single individual, Joe. This is not lying; it is adapting to the demands of the situation. Online, however, a person gets to choose his own set of demands: an S&M newsgroup might evoke masochist Joe, a multi-user dungeon (MUD) might bring out warrior Joe, and a romantic chat room may even elicit female Joe. An anonymous Internet allows its users to adopt whatever identity they desire, and its lack of physical cues and consequences in fact makes it difficult to be exactly the same person online as off.

Researchers believe that people are very well aware of their explorations. Psychologist Sherry Turkle, who is one of the foremost names in this field, promotes the benefits of

using multiple online personalities, and notes that people recognize when they have chosen to adopt them. She claims: "people who assume online personas are aware of the lives they have created on the screen. They are playing different aspects of themselves and move fluidly and knowledgeably among them." [Rosenberg, 2004] She cites the story of a particular young man who considered his 'real life' personality to be simply another 'window', much like the many he will use when interacting online. Sometimes, she notes, it is not even his best window. [Rosenberg, 2004]

In order to create an environment in which people feel safe enough to reveal what they may consider 'embarrassing' or else potentially damaging personality traits, simple yet effective means of protection must be created. Some current anonymizing services, such as Anonymizer and Ultimate-Anonymity create such a system; they are not free, but they are effective. In the eight years in which Anonymizer has been in existence, its operators claim there has not been a single breach of security. [Cottrell, no date] Some services are not that lucky, however; in the section that follows, we examine the story of the pioneer of anonymization services: anon.penet.fi. Its creator's vision of an Internet in which people could interact without fear of reprisal has not come to pass, but it is certainly not for lack of trying on his part.

6.3. The Story of anon.penet.fi

In the early days of the Internet, when the World Wide Web was still in its infancy, most social interaction took place within Usenet forums. Outside of Usenet, the online world was dedicated largely to academic and military purposes; fields in which anonymity may actually be a hindrance, rather than a desirable condition. Within Usenet, though, was a massive network of newsgroups, a highly social environment in which one may have wished to express controversial or unpopular opinions without making known his or her identity or associations. Readers of Usenet's widely varied groups had little to fear, as they were effectively unknown. However, newsgroup posters did need to worry about issues such as harassment and lawsuits claiming libel or copyright infringement. Thus, anonymity when posting became a desirable condition, and technological solutions were sought. The most effective tool developed was anonymous remailing, which strips the original header from an e-mailed message and replaces it with a header that cannot be traced back to the original sender. What follows is the story of the rise and fall of the first, and for a time most famous, anonymous remailer: Johan (Julf) Helsingius's anon.penet.fi.

Anon.penet.fi can trace its roots back to an argument within the Finnish research community. In newsgroup discussions, some university network administrators were insisting that every email message should be traceable back to the sender (whose name should be attached to the message), in order to enforce accountability. Helsingius insisted that the Internet did not work that way, and that if an organization were ever to attempt to enforce such a rule, there would always be a technological means of circumvention. To prove a point, he took two days and coded the first version of his anonymous remailer. The point: "don't try to control the network because it's impossible anyway." [Helsingius, 1994]

The mechanics of Helsingius's remailer were not complex, though it should be noted that it was technically a pseudonymous, rather than truly anonymous, system. A person wanting to use his system would send an e-mail to the server, which would return an identity such as an698304@anon.penet.fi. Subsequently, that person would send their e-mails through the server, which stripped off any identifying information in the header and replaced it with the anonymous identity/server information. Replies made to the anonymous address were routed through Helsingius' server back to the associated real address. To prevent identification through traffic analysis, Helsingius had his server delay forwarding messages for a random amount of time (eventually up to two days), and did not send out messages in the same order that they were received. Thus, as long as he or she trusted Helsingius (as he controlled the database with associations between real and pseudonymous ids), a person could feel confident that his or her true identity could not be determined when posting a message to Usenet.

Fortunately, Helsingius proved trustworthy. He had been an Internet user since the 1970's, the days of ARPANET, and realized that he was providing a very valuable service for the community of which he was such an integral part. He firmly refused to give up the identity of any of his users, while providing a mechanism to ensure at least some accountability. Every message that emanated from anon.penet.fi had attached to it the procedure for how to complain to him about that user. Should that person be the subject of numerous complaints, or be found to be posting hundreds of meaningless messages to newsgroups, he or she would receive a message from Helsingius reading "People really don't like this ... please stop or I will do something about it." Should the person continue to abuse his system, Helsingius would ban him or her from his server. In either case, though, the person's anonymity would never be compromised.

There was great pressure on Helsingius, however, to give up this practice. Many 'flame' messages were sent to him, extolling the principle that people must be accountable for what they say. In fact, an appeal was made to the administrator of the Finnish domain to shut down anon.penet.fi, which forced Helsingius to move the server from a network partially shared with a university to one which was wholly commercial. However, he maintained his principle of non-disclosure as long as possible: specifically, until he was served with a search warrant by Finnish police.

In early 1995, the front-page headline of the British newspaper 'The Observer' read "The peddlers of child abuse. We know who they are. Yet no one is stopping them." Inside, Helsingius's name and picture were printed with the caption 'the Internet middleman who handles 90 percent of all child pornography.' The accusations were obviously false; anon.penet.fi did not allow postings to picture newsgroup, nor was it technically capable of transmitting images due to size limits imposed by Helsingius. However, the server had been noticed by Finnish police, and though further investigations absolved him of any wrongdoing, anon.penet.fi was now under observation.

In February 1995, when anon.penet.fi had had over 200 000 users and was processing ten thousand e-mails per day, the Church of Scientology contacted Helsingius, claiming that

user 'an144108' had posted stolen, copyrighted Church documents in the alt.religion.scientology Usenet newsgroup. The Church asked Helsingius to provide that user's identity; he refused. The Church then contacted Interpol and Finnish prosecutors, who provided police with a search warrant for Helsingius's home. The warrant requested the entire mapping of IDs to users; in order to prevent this from being made public, Helsingius relented and released 'an144108's identity. He then posted word of this breach on Usenet, and offered to remove any person who requested from his database; not a single person accepted this offer. However, even with the outpouring of support he received, Helsingius realized that the law would not support him in future cases, and due to the accusations that had been leveled at him and the lack of protection for his users, he chose to close down anon.penet.fi on August 30, 1996.

The story of anon.penet.fi is not necessarily unique, but it does very poignantly illustrate the problems associated with anonymity on the Internet. Because the remailer was created and run by a single man with a vision of a free Internet, it stood on strong philosophical but weak legal grounds. Without government or corporate support, Helsingius could not fight attacks on his server indefinitely. As long as the system was being used for legal (or semi-legal) purposes, the attacks could be withstood. However, once a single individual chose to break copyright law using the anonymous server, and the police intervened in the situation, anonymity was compromised. It should be noted, though, that it was only due to quick legal intervention on the part of Helsingius's lawyer that it was only the anonymity of the offender was removed; one abuser nearly caused a loss of privacy for tens of thousands of the system's users.

The Scientology attack on anon.penet.fi led to outrage and solidarity with Helsingius throughout the Internet community. The most vital aspect to this solidarity is that the vast majority of letters of protest, the use of remailers for ensuring privacy was not the most important issue. Rather, the focus was on the principle of freedom of information and the free exchange of data online. People didn't care that a particular remailer was being shut down; they cared that any remailer could be compromised due to material passed through its servers. The Internet community believed in the ideal of anonymity, and was infuriated to learn that this ideal would not be protected in the offline world.

Modern anonymous remailers have learned from the mistakes of Helsingius: Ultimate Anonymity, Anonymizer and others refuse to keep any customer information to prevent said data from being subpoenaed. In fact, this protection has become strong enough that law enforcement agencies themselves have begun to use anonymising services in order to infiltrate online crime organizations. However, pressure still exists to prevent nameless usage of Internet services. US Rep. Lamar Smith has stated that "The government must play a greater role in detecting those who conceal their identities online." [Smith, 2004] Authorities want to know who uses the Internet, because as previously described, identification is strongly associated with control. This is not the nature of the Internet, though. There will always be a technological work-around to any system of mandatory identity, and groups of people who want to bring this ideal to the masses. As Helsingius has stated: "Don't try to control the network, it's impossible anyway."

6.4 Freedom to Access Information

Up to this point, we have only examined the reasons that a person has for desiring anonymous communication online. This is a vital aspect of the Internet community, but it is certainly not the only action in which one may not wish to be identified. Web browsing itself can be a subversive undertaking, and thus one may wish to do it without being recorded. It has previously been mentioned that surveillance creates a state of self-censorship of actions in the physical realm; there is certainly no difference in the digital. Anonymous web browsing, though, allows a person to avoid the 'watchers', and thus explore the vast quantities of information that the Internet has to offer.

Should a person be granted freedom to access *any* information of their choosing, without fear of reprisal? This is a philosophical question which clearly cannot be debated here; rather, we will turn to the answer provided by an organization which claims, at time of writing, 191 member countries worldwide: the United Nations. According to Article 19 of the UN's Universal Declaration of Human Rights,

> "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media regardless of frontiers." [United Nations, 1948]

This endorsement of free access to information certainly implies a positive answer to this paragraph's opening question: yes, a person should have the freedom to seek the knowledge of their choosing. Naturally, there will be limited exceptions to this openness, such as trade secrets and matters of national security, but these should be rare and proven necessary. However, it is not the case that information is always allowed to flow freely. To illustrate this point, we will examine censorship and the potential benefits of anonymous browsing in two scenarios which have in fact very little to do with the Internet: employee/employer relations and sexual education.

In 2001, a survey done by the American Management Association found that 77.7% of companies surveyed "record and review employee communications and activities on the job, including their phone calls, e-mail, Internet connections, and computer files." [AMA, 2001] Many reasons are given for this practice, including legal liability, performance review, and the simple fact that since the company owns the machines being used, they can do what they choose. While this practice is nefarious in and of itself, it will not be fully examined here, as anonymity is very difficult to come by in the workplace; company resources are being used, and thus it becomes very difficult to hide one's identity. However, where anonymity becomes vital to employees is when an employer begins to regulate off-duty communications. In July 2005, Canadian communications giant Telus blocked access to two websites associated with the Telecommunications Workers Union during a strike-lockout. The reasons given were that one of the sites contained information on service-jamming that was harmful to the company, and another showed pictures of workers crossing a picket line, a potential danger to those employees. While legal challenges forced Telus to remove this block, the question must be asked: with what might the company replace this block? It does not seem far-fetched to imagine that it begin logging accesses to the site from any Telus account; it would be a simple

task, and might chill the use of the website in the same way as blocking it. This may not be a lawful step to undertake, but neither was blocking the site in the first place.

More disturbing than this incident, however, are some of the legal rights to limit off-duty activities given to companies in the United States. The US-based security firm Guardsmark has a rule stating that employees may not "fraternize on or off duty, date, or become overly friendly with the client's employees or co-employees." ["Big Brother", 2005] As this rule would seem to twice violate the US Constitution's First Amendment (by limiting the freedoms of speech and peaceable assembly), as well as Section 7 of the US's National Labor Relations Act (NLRA) of 1935 (by limiting the right of employees to associate for unionization purposes), the rule was challenged as an unfair labour practice. Incredibly, though, in June 2005 the US National Labor Relations Board upheld the rule, claiming that employees would likely interpret it as a ban on dating alone, which is allowable due to the threat of sexual harassment. ["Big Brother", 2005] Thus, an employee working 'at will' (meaning they can be fired at any time), as most do, must differentiate between legally allowed association under Section 7 of the NLRA (of which there is no legal obligation for an employer to inform his or her employees) from disallowed 'fraternization', which is the essence of workplace solidarity (as noted by the dissenting opinion in the ruling ["Big Brother", 2005]). How can this be done? This simplest means are to either avoid such associations, or to communicate without identity. Anonymity in this case provides a vital tool not only for organization of labour associations, but for simply speaking, or exchanging information, with a person one has met on the jobsite. This situation is frightening, but at least anonymity provides a method to circumvent a chilling rule.

The debate about anonymity's role in the freedom of information is not simply about using the Internet for subversive purposes, though. This can be seen when we examine the information being made available through sexual education in the United States. The argument that will be made is not that any particular form of "sex-ed" is best, but that a child should not be categorically deprived of educational material, a situation which currently occurs in many school systems.

In 2005, the US Congress allocated approximately $170 million to abstinence-only education. ["Abstinence", 2005] [Abstinence-only sexual education informs students that the only safe choice is to completely abstain from sex. Teaching children about forms of contraception, reproductive systems, or sexual mechanics is prohibited.] This brand of teaching has been denounced by every reputable sexuality organization in the US, including the American Medical Association, ["Abstinence", 2005] but has a strong backing from the religious right, as well as powerful support from President Bush. In some areas, it is not a matter of choice. North Carolina state law, for example, mandates abstinence-only sexual education, going as far as to remove three chapters (covering AIDS and other sexually-transmitted diseases, marriage and partnering, and contraception) from high school health textbooks. Limitations on materials that can be taught are certainly being enforced: a teacher in Missouri was suspended for answering a student's question about oral sex, and a Florida teacher was suspended for showing a student-made video about preventing the transmission of AIDS. In fact, 35% of public

school districts in America require abstinence to be taught as the only option for unmarried people, and either prohibit the discussion of contraception or limit its discussion to contraception's ineffectiveness. ["Abstinence", 2005] Strangely (though comfortingly), given its prominence, this type of education is not popularly supported. 75% of US parents want their children education about contraception, abortion, sexual orientation, STDs, etc, and only 1 in 5 would remove their children from a comprehensive sexual education class, given the choice. ["Abstinence", 2005] However, for the children subjected to abstinence-only education, there is little recourse for a fuller education. School libraries are censored to remove any non-conforming materials, and school Internet connections are filtered to block out sites regarding comprehensive sexual education. In 2000, Congress passed the Children's Internet Protection Act (CIPA), which was deemed constitutional by the Supreme Court in 2003. This Act mandated the filtering of all computers in public libraries, if that library were receiving federal funds to help defer the costs of their public networks. This filtering can be turned off on request for adult patrons, but a child wishing to do personal research on sexuality is likely to be prevented by the frequently over-sensitive filters. Put simply, there is virtually no method for some US children to access proper sexual education.

Consider the case of a female child whose parents are rabidly pro-abstinence-only education. It will be near-impossible for this child to become knowledgeable about contraception. She will not learn it, and will in fact be prohibited from talking about it, in her health class. The school library will not have books about it, and Internet connections from the school or public libraries will not have access to the information. It is also safe to assume that this child will not be able to learn about condoms or birth control pills at home. Since the subject is clearly being made into a taboo, she may be uncomfortable or ashamed to ask about it. If this child were to then become pregnant (abstinence-only, does not delay or lessen sexual activity, but does make contraceptive use more likely; also, the US has the highest teen pregnancy rate in the developed world ["Abstinence", 2005]) contract a sexually transmitted disease (US adolescents have a higher rate of HIV contraction than almost any other American demographic ["Abstinence", 2005]), or be curious about her sexuality, to whom could she turn?

The answer to this question is an anonymous Internet. A truly identity-free system would allow the exploration of such taboo subjects. Somewhere, it is true, the child must find an unfiltered computer. Upon doing this, though, she could learn without shame. Anonymous support groups are everywhere online, as is frank, preventative, scientifically-founded information about sexuality. What makes the Internet such a wonderful resource in such a situation is the amount of freedom it can allow. Anonymity, we must remember, is a matter of degree, and the level it is possible to achieve in the physical world does not compare to that possible in the virtual. A librarian, for instance, may not know one's name, but he or she hears a person's voice, sees his or her face, can likely guess at least the town of residence, if not the neighbourhood, and may know people who know that person. On an anonymous Internet, all of these aspects can be discarded; on a truly identity-free system, even an IP address cannot be correlated to an actual person. In this way, the freedoms to hold

opinions and seek new knowledge, as guaranteed by the Universal Declaration of Human Rights, can be exercised.

6.5 Threats to Online Anonymity

The main problem with the benefits of online anonymity that have been discussed is that *complete* anonymity, or at least the perception thereof, is required. It is not enough to believe that it is unlikely that one will be identified, or that it will be difficult to do so. There are still positives associated with these cases, but they are not enough to support the full range of benefits provided by true unidentifiability. However, even with all the benefits of online anonymity, it is not universally supported. Naturally, the ability to conceal one's identity can be, and is, used for unethical purposes. Slanderous comments are posted by those using anonymous remailers, websites containing sexist or racist propaganda are registered under false names, and sexual predators lure their victims by posing as young adults in chatrooms. It is far-fetched to say that a scenario of full-identity disclosure would prevent these incidents, but many point to anonymity as a major cause of much of the illegal activity online. For example, as previously mentioned Texas Republican Lamar Smith has stated that "The government must play a greater role in detecting those who conceal their identities online," [Smith, 2004] when justifying the passing of a bill which would increase by 7 years the prison term of a person convicted of a felony committed using a website registered with false information. Studies have shown that up to 10% of domain names are registered in this manner; ["House", 2004] it seems rather harsh, then, to sentence a person to 7 additional years in prison for an action undertaken by 1 in 10 webmasters. However, this is the level of fear of the criminal potential of online interaction is not unique; many lawmakers have taken steps to prevent the possibility of untraceable Internet usage. Two main legal threats to online anonymity have arisen: data retention/lawful access, and the USA PATRIOT Act.

6.5.1. Data Retention/Lawful Access

One of the main reasons that anonymity is vital within the online environment is the Internet's archival nature. There, any statement which is made essentially cannot be retracted; the 'net's digital makeup makes it relatively simple to construct a picture of the entire environment at any given time, with storage space being the main restriction to this activity. Thus, when one makes a comment which can clearly be linked to him or her, such a link will always exist. Comments made as a rebellious teenager will be preserved for the world to see when one becomes an adult; should one's opinions or politics change drastically, or should he or she hold a position of power, these youthful indiscretions could come back to haunt him or her. In order to combat this effect, a poster truly desiring anonymity must hope that all traces tying the message to the sender (for instance, temporarily assigned IP addresses) are quickly deleted during standard data purges. The amount of storage required to retain all Internet traffic would be tremendous; thus, ISP's frequently clear data on a regular (often weekly) basis; these clearouts are an important aspect of online privacy. However, based on the assumption that this data may be used to catch criminals and terrorists, governments have begun to

pass laws aimed at preventing the deletion of data, thus creating the first major legal threat to online anonymity which shall be discussed.

The principles of data retention and lawful access are well rooted in legal history, and do in fact serve as valuable legal tools. Lawful access consists of the lawful interception of telecommunications and the search and seizure of telecom information, while data retention simply provides mechanisms to ensure that such data exists to be examined. Lawful access, for instance, is frequently used in the investigation of organized crime; the wiretapping of phones, for instance, is a well known technique of this kind. However, many countries' lawful access regulations are highly technologically specific, and thus do not transfer well to Internet traffic data. As such, the laws of some of these nations are undergoing reviews and updates in order to generalize access regulations; however, many also are taking this opportunity to broaden the use of such tools. For this thesis, the focus will be on two such sets of laws: those being proposed in Canada, and those within the European Union.

The Canadian lawful access proposal, though still troublesome, is reasonable. Mandatory data retention is not being proposed; rather, any peace officer will be given the authority to give a 'do not delete' order to an ISP for information which will subpoenaed in the future. ISPs are also not being forced into a scheme of 'know-thy-customer', in which they must have accurate information about all subscribers. Agencies will be able to demand any user data that is kept, but service providers will be under no obligation to collect any information. Any new telecommunications system which was to be installed would require an intercept capability (such that traffic from a particular individual could be isolated and collected), but existing systems would not need to be retrofit.[5]

While any police interception of data raises privacy issues, they are necessary for effective law enforcement. Thus, short of some minor glitches (the lessening of the burden of proof required for data collection, an atrociously poorly conducted 'public consultation' scheme, occasional over-empowering of low ranking peace officers), Canada's lawful access scheme is a near-model of the protection of online anonymity. Yes, there are means made available to find out a user's identity, but they are kept to a small enough scale (and enough provisions are made against their abuse) that there is no major threat presented.

In contrast, current European Union data retention plans are quite frightening. A mandatory data retention scheme has been proposed, with an amazingly broad scope; means of communication which shall be recorded included: telephone, including text messages, Short Message Service (SMS) systems, email, Voice over Internet Protocol (VoIP), file transfer protocols (ftp), hypertext transfer protocols (http), world wide web, network transfer protocols, and many others. [Council, 2005] In regards to these forms of communication, any information necessary to identify the source of the information must be stored, along with any data regarding the routing, destination, time, date and duration, device used, and location or the communication. [Council, 2005] This information is to be retained for a period of 12 months, though member states can

[5] March 2005, Canada Lawful Access Proposals consultation, Vancouver BC

increase that time to 36 months at their discretion, or reduce it to 6 months should the new directive conflict with national laws (though such a reduction would be subject to annual review). Member states will have two years after adoption to comply with this framework; thus, such a scheme will most likely exist by early-2008. The Madrid bombings in March 2004 gave this bill considerable momentum, which has only been increased by the July 2005 London transit attacks – it will likely be officially presented in mid-September. ["EU", 2005]

The purposes of such a scheme are "prevention, investigation, detection and prosecution of crime and criminal offences including terrorism." [Council, 2005] However, there will clearly be much larger effects. Sjoera Nas, a board member of the European Digital Rights group, has noted that, "Large scale data mining will lead to many people's innocent behaviour becoming suspicious." ["EU", 2005] Such data mining is inevitable, as since the proposal does not allow for the recording of the contents of the various transmissions, subtler trends will have to be recognized in order to identify potential 'terrorists.' In fact, it is the word 'prevention' in the statement of purpose which presents the biggest threat to anonymity; prevention involves the prediction of the future, which itself requires significant guesswork and near limitless information; thus, anything resembling 'suspicious activity' will have to be investigated. A newsgroup which is frequently posted to anonymously is clearly such a red flag, though it may simply be a support group for people who are unable or frightened to reveal themselves, such as sexual abuse victims. In fact, due to the knowledge that information is be collected in this way, it is likely that any anonymous communication will be seen as an attempt to hide one's self from the government, a clear sign of illegal activity. An over-arching data retention scheme of this nature serves to shine light into the shadows of anonymity: it will certainly flush out many criminals, but it will also expose many of those in need of the darkness' veil of safety.

6.5.2. USA PATRIOT Act

In the aftermath of the attacks on September 11th, 2001, the United States government launched its largest ever offensive against terrorism, and at the same time against Internet anonymity. Since it was possible for terrorists to use computer systems to plan and co-ordinate future actions, it was seen as vital that the FBI and other organizations have access to Internet traffic, and that individuals who were innocently using the system accept this new police presence as a necessity for safety. The 'Uniting and Strengthening America by Providing Appropriate Tools to Required to Intercept and Obstruct Terrorism" (USA PATRIOT) Act, passed just 45 days after 9/11, thus included large and frightening additions to the FBI's ability to monitor the Internet, and made it very clear that individuals have little to no right to dissociate their online activities from their offline identities.

The most dramatic changes to police power come in section 215 of the Act. By this section, the FBI is allowed to collect *any* tangible things from any person or entity so long as it specifies that it does so "for an authorized investigation ... to protect against international terrorism or clandestine intelligence activities." [ACLU, 2002] The person

or entity that is served this order is then prohibited from revealing that fact; thus, a person will be completely unaware if they are being monitored. The reasons for which an investigation can be authorized are also broadened; US citizens can be subject to scrutiny based partially on the exercise of their First Amendment Rights – non-citizens can be inspected wholly on this basis. [ACLU, 2002] If the FBI wishes, they can obtain permission to surveil because of the books a person reads, the websites he or she visit, or due to a letter to a newspaper's editor that is critical of the government. It need not show probable cause that the person is involved in criminal activity or that he or she is the agent of a foreign power. It simply needs to have some desire to place that person under surveillance, and to use the word 'terrorism' in its justification.

This solution is very reminiscent of the Panopticon. The prisoner knows that the guard might be watching, but has no way to find out. Further, the prisoner cannot find out if they have been watched in the past. Not only are the subjects of information requests not allowed to reveal the fact, but even general information about how often these new powers of surveillance have been used are kept hidden: Attorney General John Ashcroft classified that data. [ACLU, 2002] It is not safe to assume that the average person is safe from scrutiny simply because the FBI has no reason to take an interest in him or her. The FBI has also claimed that they have no interest in what people read; yet, over 200 requests for borrower records have been made to libraries since PATRIOT was passed. [Wilson, 2005] Online, there is particular worry about the place of anonymity, as other sections of the Act make it very clear that the US intends that no one will escape the gaze of the guard tower.

First, it must be made clear that §215 covers any level of Internet activity that is stored. If American ISPs were forced into a data retention scheme (fortunately, they have not been, yet), that data falls within the 'anything tangible' category of items that can be ordered by the FBI. As it is, §212 allows an ISP to 'voluntarily' hand any non-content information requested by the FBI (and it will take a very powerful or extremely principled ISP to not 'volunteer'). Further, §210 and §211 allows the government to seek more detailed information, such as session times and durations, payment information, and temporary network addresses among others using a simple subpoena (i.e. without court review). [EFF, 2003]

Next, the definition of 'terrorist' is changed by the Patriot Act. §802 redefines domestic terrorism to include any activity that appears to be intended "to intimidate or coerce a civilian population" or "to influence the policy of government by intimidation or coercion." [H.R. 3162, 2001] This raises great concern about legitimate protests, particularly if they (intentionally or otherwise) erupt into violence. Since the Internet is so frequently used to air grievances, where will the FBI choose to use their new powers? Is an inflammatory newsgroup posting and attempt to coerce the civilian population? Is the entirety of the ACLU's site an attempt to influence government policy by exposing misuses of powers (ie, by coercion)? Both of these certainly fit into the definition of a domestic terror situation, thus opening the entire new surveillance arsenal of the FBI for deployment.

There will always be illegal threats to online privacy: hackers may break into networks, employers may install keystroke recorders on the laptops of employees, and jealous lovers will keep track of their partners' online activities. However, there are attempts being made to control these acts; malicious hacking has always been illegal, workplace rights organizations are petitioning for online freedom for workers, and in August 2005 the owner of a company which manufactured and distributed software to surreptitiously record emails and website visits was indicted on 35 charges of violating US privacy law, as were four customers. ["Jealous", 2005] However, there is little real difference between these violations and those being done by government agents in the name of national security. When the protection of online anonymity becomes a matter of splitting hairs (i.e. does the violator have a badge or not?), it must seriously be considered to be 'under attack.' Online anonymity serves functions that virtually nothing else can, such as the free allowance of identity exploration. To take this away would be to negatively affect the well-being of hundreds, if not thousands of users. While no law is perfect, it can be seen through Canadian lawful access rules that it is at least possible to allow law enforcement to function while still maintaining a sense of privacy online; it is encouraging to think that a government might be willing to recognize anonymity for what it's worth, and work to protect it.

7. Possible Solutions

Anonymity is being threatened by new laws and new technologies; of this, there can be no doubt. The technological ability exists to monitor all of an individual's transactions, movements, associates, online activities, etc; essentially, to create an incredibly intricate description of a person's entire life. The only reasons that this have not occurred have to do with cost and will.

The cost of an over-arching surveillance scheme will not be a deterring factor for much longer. Many surveillance systems are already in place, or simply need a small change to be put into place. A cashless society, for instance, would be able to record every transaction ever made. Such a society is not impossible; the Organization for Economic Co-operation and Development has written that "Money's destiny is to become digital." [OECD, 2002] In France, some 850 000 people use the 'Moneo' card regularly ["Cashless", 2003]; this card is 'charged' with cash, and then accepted for small transactions. It is a simple, anonymous Smart Card, requiring no PIN or other authorization; thus, transactions are completed as quickly as with paper money and coins, and with less hassle. It is true that it is unlikely that cash will disappear entirely with the next few decades, but should an acceptable alternative to it arise it may see a significant decline in use (as it did when credit cards and ATM cards became more popular). In such a society, the only limit to the amount of data collected from transactions is storage; and as the price of memory tends to decrease at a dramatic rate, this will not be a limit for long.

A change of societal structure of that magnitude may seem extreme, but can we truly say it is? Consider how many transactions are recorded already. As previously mentioned, WalMart alone estimates that it has collected 460 terabytes of transaction data already, and it will certainly continue to this accumulation. Also, many people already carry nothing but electronic forms of payment; cash, one will frequently hear, is too dangerous to carry. Credit and debit cards make many feel much more secure. Thus, it is certainly not true that every transaction is monitored; however, we may be closer to that stage than we realize. The costs, then, of implementing a system which simply gathers together all the data already being collected by various retailers and organizations would not be overwhelming. In fact, data aggregators have already turned this concept into a profitable business model.

Every surveillance technology that has previously been described has a monetary cost which is declining. Surveillance cameras are extremely cheap, and the back-end support necessary is becoming affordable. RFID tags will cost pennies once they have been widely adopted. GPS is already being incorporated into vehicles and cell phones, at little to no cost to the consumer. Quite simply, the monetary expenditure required to create a completely surveilled society will soon no longer be a limiting factor.

Thus, the reason that such a society does not exist is will. As of yet, no government or corporation has made the decision that the benefits of total surveillance are worth the difficulty of either convincing the populace that the advantages thereof outweigh the

costs to their freedoms, or else thrusting such a system into place by force. The current American government seems to be attempting to subtly move towards Big Brother, but as of this writing they are still hesitant to appear to be doing so. True comprehensive surveillance will require a supreme act of will, either to rewrite or ignore all the rules of privacy currently in place. Is such an act possible? To answer this, we turn back to Orwell, who notes that it may simply require a government to change its motivations.

In *Nineteen Eighty-Four*, the protagonist, Winston, is captured and brought to the Ministry of Love for re-education. During this process, he is asked why the Party should want power. Guessing, Winston replies that the Party seeks power for the good of the citizens, ruling them because they are not fit to rule themselves. He receives a jolt of electricity for this answer, and is then told the truth:

> "The Party seeks power entirely for its own sake. We are not interested in the good of others; we are interested solely in power. ... We are different from the oligarchies of the past, in that we know what we are doing ... they pretended, perhaps they even believed, that they had seized power unwillingly and for a limited time, and that just around the corner there lay a paradise where human beings would be free or equal. We are not like that. ... We know power is not a means, it is an end." [Orwell, 1949]

Perhaps all a surveillance society needs is a government to recognize this fact. Knowledge, after all, is power. Knowing every piece of information about a person can be a very effective first step towards controlling that person. Should a government choose to use this power, it would be very difficult to overthrow. Former Iraqi dictator Saddam Hussein used clever tricks of surveillance to prevent internal actions against him; for instance, he declared that anyone not reporting talk of a revolution would be killed. Then, he let it be known that he would send agents out to speak of an overthrow; anyone could be a government spy. Thus, anyone hearing such talk could not know if they were being tested by Hussein or learning of an actual coup against him; in this way, the listener risked his or her own life should they not report the incident, and Hussein had effectively created a country of civilian agents. In a country of total surveillance revolution is extraordinarily difficult.

However, it is not only through a power hungry government that such a society could come to be. In 1967, privacy advocate Vance Packard opined, "My own hunch is that Big Brother, if he comes to the United States, will turn out to be not a greedy power-seeker but a relentless bureaucrat obsessed with efficiency." [Packard, 1967] Complete surveillance is extremely efficient. Crimes would be solved quickly and expediently, all records of a person would be quickly accessible for credit checks or even during legal actions, and the location of every individual would be ascertainable should they be needed for some reason. There are endless reasons why an effective bureaucracy desires complete, indexed information about all individuals; and unless there is a means (such as law) to prevent this, they will likely be able to gather together the resources necessary to make that desire a reality.

Frankly, if the only reason given that the surveillance society did not exist was that no-one has yet chosen to create it, it would almost certainly come into being eventually. Thus, there must be systems set up to protect privacy and anonymity, lest they fall victim

to the threats against them. In this section, we examine possible solutions to these threats, and evaluate their likely effectiveness in both a real and worst case scenario.

7.1. Free Market Regulation

Free market regulation is the dream of corporations. A 'free market' is one in which, at least theoretically, every transaction is undertaken completely voluntarily. The consumer plays a 'game' with the shopkeepers, with the government acting as a neutral referee to enforce the rules. This game, if played completely logically, eliminates theft and coercion; a shopkeeper will not cheat in the game under the assumption that if he or she is found out, the cost in lost business will far outweigh the gains of the initial swindle.

This may not seem like it favours corporations, but it is they who tend to be the free market's strongest proponents. Each time a law is proposed which would protect consumer privacy, companies line up to describe how unnecessary it is. 'Protecting privacy is just good business,' some say. Others claim that, 'If a consumer feels violated, he or she can simply move his or her business elsewhere.' Currently, both the data aggregation and RFID industries are sounding this call: 'we don't need laws, we will police ourselves.' When one of a game's players so strongly insists that it continue, it is certainly worth examining his or her motivation; upon doing so, the corporate advantages of the free market regulation of privacy become immediately evident.

The benefits to corporations fall into two main groups: limited detection, and power. The former encompasses the fact that generally, it is excessively difficult for any consumer to find out that his or her privacy has been violated. If his or her address has been sold, perhaps he or she begins to receive more junk mail. Even if this is noticed, it is near impossible to determine what company sold the address; was it a charity giving out a donations list, or the post office selling change-of-address information, or a data aggregator licensing out its database? Short of using unique names every time an address is requested, tracking the path of this information is near impossible. Credit card information can similarly be stolen at many locations; did a thief physically copy the data by some means, or was it a breach into a bank's computer network? Possibly it was even an online company unsafely storing transaction information. Credit card fraud is detectable only by examining closely one's monthly statements; many people will go months without actually looking at a statement, particularly in this age of automatic withdrawals. Even so, it took a law being passed in the United States for companies to be willing to inform consumers when they lose critical customer information.

Some forms of privacy violation are completely undetectable. Genetic testing of DNA collected for other purposes is imperceptible to an individual, but could allow an employer to know more about an employee than the employee does. Given that numerous people work 'at will', a person could be fired in part due to a genetic condition of which he or she is unaware, and never told the reason. RFID or GPS tracking can be done completely covertly as well; world leaders attending a summit on the Internet and Technology were unknowingly given RFID-equipped name badges and tracked throughout the conference [Hudson, 2003], while police have begun secretly affixing

GPS units to the vehicles of suspects. [McCullagh, 2005] WalMart, as mentioned in chapter 5, has also been caught running secret RFID tests. How can an individual complain to the free market if they don't know that his or her privacy has been violated? Furthermore, even if the person does know, can he or she find out who has violated it? It certainly is not an easy task. Let's say, then, that a person does have a legitimate complaint, and knows what company it is against. In a free market system, do they have any recourse?

This is where the second corporate benefit, power, comes in to play. Frankly, does WalMart care if a single person changes his or her buying habits? It seems unlikely. In many areas, WalMart is now the only option when looking for a department store; it would be virtually impossible in these areas to initiate a large enough boycott to have any kind of effect. Also, suppose a data aggregator violates privacy. How can the free market regulate that? The only way to keep a person's information out of its files is for him or her to 'live off the grid'; a rather draconian solution to the problem. It would take an absolutely egregious privacy violation for the public to rise up and have a major effect on a corporation; for instance, if a credit card company chose to unsecure all its information, and let it remain that way from here onwards. If such a decision were publicized, it is likely – not certain, but likely – that a good portion of the public would cancel their accounts with the company, and potentially run it out of business. However, numerous banks and credit card companies have already admitted to losing records: the Bank of America lost 1.2 million records in February 2005 due to lost backup tapes; Citibank Financial lost 3.9 million with the same cause on June 6 2005; not two weeks later MasterCard admitted a security breach exposed 40 million credit card records. [Swartz, 2005] Several hundred Canadian Imperial Bank of Commerce (CIBC) customer records, including social insurance numbers, addresses, phone numbers and detailed bank account information were faxed to a West Virginia junkyard over a period of three years; when the owner of the junkyard called the bank to inform them, the operator informed him that "it's not our problem." He finally raised attention by calling some of the involved customers and bringing the matter to their attention. [Akin, 2004] In all of these cases, though, a single uniting thread can be found: there was little to no customer uproar, and the companies involved suffered virtually no loss of income.

Why do people feel unable to contend with big businesses in the free market? Because it takes a good deal of time, money and effort to do so. All large corporations have both legal and public relations teams at their disposal; the individual has neither. To raise enough awareness about a privacy slight, particularly one that does not affect a large number of people, to make a difference is extremely difficult in the open market. Individuals must have some reasonable form of recourse in case of a serious privacy violation; forcing them to start a movement in order to affect the entire marketplace is asking the impossible. Both realistically and in the worst case, free market regulation simply cannot protect the privacy rights of individuals.

7.2. Purchasable Privacy

An offshoot of the practice of free market regulation is the idea of purchasable privacy. This is precisely what its name would suggest; should a person truly desire privacy, they should be able to pay for it. This situation frequently occurs in an online situation: anonymizer.com and ultimate-anonymity.com will both sell a person methods to completely disguise their identities. Proxy servers are provided for accessing websites without allowing them to install cookies, anonymous credit cards are provided for online purchases and untraceable e-mail systems allow safe posting of newsgroup message. Both of these companies refuse to maintain any kind of log of users' identities or actions, and though this may mean that users who lose their passwords have no means to retrieve them, it also means that there is no 'tangible thing' that can be collected by the FBI. At the time of this writing, Anonymizer charged $30US per year for these services, while Ultimate-Anonymity's use cost a one-time charge of the same amount.

Similar ideas were described in Chapter 5, about ways to foil RFID. For instance, blocker tags could be made available which would prevent both seen and hidden readers from identifying any tags carried on one's person. Similarly, for the price of time and future tag use one could simply have the chip removed or deactivated. Another similar technology, GPS, can frequently be deactivated by keeping one's phone turned off.

In each of these cases, the individual must pay a price for his or her privacy, be it in time, money or functionality. This may be extremely effective for a single person, but is it a good solution for society as a whole? There are some signs which point to 'no'. Privacy is an established 'right'; putting a price on it will remove that label. This practice will encourage violations of those who choose, or cannot afford, to protect themselves. Their lives will be laid open, creating a very strong have-have not division within the population. The justification for this is clear: privacy is available, but the individual is not utilizing it. Thus, he or she must not care what information we gather about him or her. This may be clearly fallacious, but such an argument will almost certainly be used.

Furthermore, one must have great faith that these technologies are reliable, and that they will remain legal and in existence. Without some form of recourse against a company, a person only has that organizations word that they are doing what they claim. It is impossible to know if Anonymizer keeps records; it must simply be accepted that they don't. It must also be understood that GPS units in cell phones turn off when the phone is off; there is certainly work in progress to create a self-powered unit, which will be added to cell phones for 'emergency' locating of individuals. Will cellular companies even tell their customers when the change takes place? Can anyone without a reader truly know that his or her passport is shielded, or that his or her blocker tag is functioning? Most importantly, can there be a way to be sure that the use of these products won't be outlawed by a government, under the rationale that anyone disrupting the constant flow of information must have something to hide? The unfortunate answer to all of these questions could be 'no'. In the worst case, buying privacy simply will not work, as the systems set up to allow people to do so will be shut down. In the realistic case, these practices will be allowed, but they will be heavily monitored. This is not to

mention the fact that by commoditizing privacy it is turned from a right to a privilege; the benefits is affords should not be horded by the elite few.

7.3. Personal Information as Property

A different, yet very similar take on the issue of privacy and anonymity is the notion that companies, rather than charging those who wish to remain private, will reward those who are willing to freely give it up. If personal information were to be considered property, it could then be bought from an individual. That individual can set his or her own price, choose to whom it is sold, and in the best case even choose how it is used (i.e. license it, rather than sell it outright). Thus, those who wish to keep their information to themselves can do so, and others can receive some recompense for surrendering the use of their names, addresses, etc.

This scheme does work slightly better than purchasable privacy, even if it is the same basic idea. In this case, privacy is the default situation; a person has to actively choose to yield his or her rights, rather than having to choose to protect them. Also, the financial burden is shifted from the consumer to the company desiring information, which seems like a more equitable scenario. The flow of information would not be completely cut off, as it seems likely that many individuals would be happy to allow direct marketing to occur if they were to be paid for it. However, there are many subtle issues that arise when considering this scheme, which make its implementation unrealistic and somewhat undesirable.

The first is the sheer magnitude of such a plan. The information already in existence about virtually every individual in North America would have to be handled in some way. This information could either be completely prohibited from use, which would cripple the trillion dollar data aggregation industry, many retailers, and the government (which uses the data for tax purposes, the census, and many other everyday operations). Clearly, this situation is not realistic. It is possible, then, that immediate enforcement of some form of 'royalty payments' could be initiated for information already collected. Should an individual wish to have his or her information removed from this system, he or she could be provided with that option. However, this system leads to even larger problems. First, such a payment system would require the compilation of a massive database of names, aliases, current and previous addresses, and banking information. This is an absolute privacy nightmare, as every company that holds information on individuals would have to be given access to it. Also, royalty payments would be virtually worthless. Names simply aren't worth that much. For instance, Consumer's Union reported that when they sold 92,000 names and addresses to the magazine *U.S. News & World Report*, they received $8000, or approximately 9 cents per name. [Garfinkel, 2000] At a generous royalty fee of 15%, each of these individuals would receive approximately a penny for this use of his or her information. Finally, it is unlikely that data aggregators would allow individuals to 'opt-out' of these payments, and thus have their names removed from the system. They have a very interesting argument based on Lockean notions of property, which claim that there are two ways to claim property: to make use of it, or to fence it off, letting others know it is your own.

Data aggregators have done both; they have taken information made freely available to them and used it, or else have staked claim to it by purchasing it. [Harper, 2005] A very strong argument can be made that the data is theirs, and that they have no mandate to allow others to remove parts of it. Thus, it seems a system of royalty payments cannot work. The final method, then, would be to allow corporations to freely use all the information collected before the payment scheme was implemented, and only pay for that gathered later. This is ineffective for the consumer, as it will force them to change names, or move, in order to being to receive compensation for some forms of data (like addresses), and never allow them to receive anything for other forms (such as collected DNA). The chances of finding a practical method of turning data into personal property seem very remote.

Even if such a method is found, will it protect privacy or anonymity? Much depends on where the line is drawn between personal information that requires payment, and that which does not. For instance, clearly a person who sees another walking down a street cannot be charged for that piece of information. Thus, the operator of a surveillance camera similarly should not be charged. A friend who recognizes one on the street will also not be charged; can a surveillance camera with facial recognition expect the same protections? Both the camera and the friend can tell others that they saw Person X; the camera is simply a 'friend' to everyone, and can thus recognize each passerby. A scheme of personal information as property actually does nothing to protect anonymity. When one attempts to shed his or her identity, it is often for reasons of comfort, mental relief, or physical safety. The violation of any one of these is easily worth more than whatever price the person receives for the revelation his or her identity. Small violations of privacy may be protected by such a scheme (if a reasonable way of implementing it can ever be developed), but important matters are left completely unaffected. In addition, it is not just individuals that will be able to assert property rights over information; once a company has that data, they will own it as well; and once a corporation has paid for information, is it a certainty that it will be used to the fullest possible extent.

7.4. A Completely Open Society

In response to the failures of the ideas already presented, the concept of the completely open society has been developed. If privacy cannot (or should not) be bought by individuals, and schemes to reward individuals for resigning their rights are not feasible, perhaps we must look at abandoning this concept of privacy altogether. Why fight a battle which in the end, it is thought, will inevitably be lost? New technologies for privacy invasion will constantly be released, and existing technologies will be made less expensive and more undetectable. Perhaps, then, we must strike a hasty compromise: individuals will relinquish all notions of privacy, so long as this transparency is enforced at all levels. In this way, a new Panopticon is created; one in which everyone is now both a guard and prisoner. For the individual that was destined to be a prisoner anyway, this may not be the perfect solution, but at least his or her situation is slightly improved (at least relatively, given that the condition of many others is worsened).

Many of the problems with such a society were already raised in the discussion of David Brin's *The Transparent Society* in chapter 2. Foremost among them is the assumption that transparency at all levels will lead to accountability. Such a statement is certainly true at the lower levels of such a society; the people at those levels will have their actions monitored, recorded and used against them is legal prosecutions or otherwise. However, what recourse does one of these individuals truly have should his or her privacy be violated?

Supposed that individual wished to don the cloak of anonymity in order to report an abusive teacher, or corruption in government or business. That person no longer has such an option, and must weigh the personal consequences of exposing a wrong-doer who knows all of his or her secrets (or who holds power over the individual) against the societal consequences of not reporting the action. It seems very improbable that the average individual would, in this case, not step back and hope that someone else notices the problem, particularly if that individual is not personally being harmed by the company's (or person's, or government's) transgressions. The survival instinct is not easily overcome.

Also, in such a society, how can the powerful have transparency enforced against them? An analogy to a typical schoolyard exists. If a bigger, stronger, older child asks another to reveal his or his dearest secret, claiming that he or she will tell his or her own in return, how can that reciprocation be guaranteed? If the weaker child does reveal the secret, they are now in the power of the stronger. If the older child refuses to tell his or her own, what recourse is there? The smaller child cannot physically coerce the other, nor can he or she report the incident, for the older child will simply threaten to spread the information told to him or her. It is only by sheer good will that the powerful play games like this; do we truly wish to entrust all of our information to the goodwill of corporate handlers?

Finally, there is no reason to believe that total surveillance is inevitable. If no changes are made to societal structures and laws then perhaps we are destined for such a situation; but there is no reason why these changes cannot be made. It will certainly be difficult, and it cannot happen quickly, but the ability to control the flow of information in a way that is beneficial to givers and receivers, individuals and corporations, and citizens and governments, is not lost. This thesis will end with a call to arms; should it be heeded, hope is certainly not yet lost.

7.5. Government Regulation

A single unifying theme can be seen in each of the previous four privacy protection schemes: the government is given a very minor role. Laws are not the solution; privacy should be worked out between individuals and information gatherers. This makes great sense from the standpoint of the latter; companies tend to only be accountable to the government, and governments are held accountable by nothing but their own laws. Should this level of responsibility be removed, ultimate power now goes to those who collect information.

Individuals must have some concrete means of redressing their grievances in order to have any kind of effective privacy protection. If a person must rely on boycotts, purchased technologies, or the goodwill of others to enforce the right to privacy, that right will essentially become meaningless. Furthermore, the government itself has the ability to be, and frequently is, one of the most flagrant violators of privacy. In this instance, there is no free market correction or technological innovation that can protect the individual. If one is fortunate enough to live in a democracy, perhaps the government can be voted out of power at the end of term; otherwise, even this mild form of redress isn't possible. However, does not a person desire some stronger measure of protection than the threat of popular revolt? Without strong privacy laws, the individual is powerless.

Anonymity cannot be protected by small sanctions, or unsecured technologies. It is different than many forms of privacy, in that damage done cannot be undone. A surveillance camera installed on a street can be removed, and its tapes destroyed; the threat to privacy is gone. Similarly, removing information from the world of data aggregators and corporations, while difficult, can be done in order to restore privacy. However, attacks on anonymity cannot be repaired. A person may seek the shadows for many reasons, which have been previously described: he or she may have committed unlawful acts, it is true, but he or she may also be afraid. This fear may be of someone who wishes him them harm or of the consequences of a socially unpopular message or action; regardless, the person may legitimately need protection. Once that person's identity has been revealed, though, there is no recourse; whatever it was that drove that person to anonymity is now free to react in any way it chooses. Even if there are no consequences immediately evident, others learn that the shadows do not truly hide one from exposure; thus, each violation weakens the power of anonymity. A person must feel comfortable in order to obtain the mental benefits described in chapters 2 and 6; he or she cannot be forced to guess whether or not he or she will be the next to be found out. The tangible benefits, such as protection of the First Amendment rights of free speech and of courage to report corruption and abuse require a strong, staid ability to remain anonymous should one choose to do so; any violation of anonymity weakens the perception of this ability. Thus, there must be very strong motivation not to violate in the first place; powerful laws, while certainly not perfect, are the best method extant to provide such motivation

This is why the best protection for anonymity, and in fact the entirety of privacy, is legislation. A degree of privacy and anonymity are required for wellbeing and security; thus, their violation should be a crime. Other crimes against the person are covered by various laws: a person cannot be assaulted, confined against his or her will, subject to fraudulent transactions, nor any other violation. Privacy must be protected in the same manner. Much as each of the crimes above, privacy violations are a matter of degree; improperly selling a person's address to a marketer is a lesser crime than revealing the name of an anonymous accuser. Thus, degrees of punishment will exist. However, there must be some way for a person to face his or her attacker; the courtroom is the best venue currently available.

Even governments must be held accountable to their own laws. The Patriot Act created such an uproar because it expanded government powers drastically; most individuals are not naïve enough to believe that these powers were not already being exercised, but they at least had the comfort of knowing that retribution could be had if necessary. If a government (at least, a democratic one) is found to be in gross violation of its own laws, there are means of securing its immediate removal. Again, this may be small comfort for those who have been violated, but it at least ensures that others will not suffer the same fate.

This thesis will not begin to suggest the laws that will be necessary to contain the threats of new technology; many foundations have spent thousands of man-hours examining this same question. Such an examination will be left for future work. However, if it is to make any suggestion at all, let it be this: legal protection of privacy and anonymity is the necessary course. It may be flawed, but it does not suffer from the fatal flaws apparent in all other possibilities. Once this framework is chosen, work can begin on the details of the necessary laws; first, though, the unified choice must be made.

7.6. Education

Throughout this thesis, the phrase 'knowledge is power' has been used, generally as a warning about why a person needs to safeguard his or her personal information. This usage will now be reversed, and it will be stated that knowledge is also one of the most fundamental ways to protect one's right to privacy. Simply put, if an individual is educated about the benefits of, and threats to, any of his or her rights, he or she will be much more willing to protect them.

Privacy advocates are not necessarily media friendly, and unfortunately that is the only arena in which the public tends to hear from them. They tend to be allowed very brief statements, and thus the words 'Big Brother' and 'violates privacy' are brought out in an attempt to convince the public that they have been wronged. I do not fault the advocates for this; I would be loath to describe the message of this thesis in a thirty second soundbite. However, the groups against which the privacy advocates act tend to have easily expressible agendas: 'we need this power to fight terrorism', or 'this is necessary to combat credit card fraud.' It is simple for the average person to understand the consequences to him- or herself of a terrorist attack, or identity theft; privacy violation is much more difficult to comprehend. In the absence of a statement of why privacy is important to the individual, a subtle and intelligent violator can quickly justify his actions, and make privacy concerns secondary.

What can be done to counter this? The public must be educated about why they have the rights that they do. Few Americans could name everything contained in the Bill of Rights; fewer still can tell you why they are all necessary, other than in vague terms (i.e. 'to preserve freedom.') It is certainly not only the right to privacy (which itself is not explicitly enshrined, but inferred from other rights) which is in danger of being lost to indifference or misunderstanding. For instance, one study showed that one in three high-

school students believed that the First Amendment went too far in its protections. Only one half believed that newspapers should be able to publish freely without government approval. [Feller, 2005] However, the study also showed that when students are given a chance to embrace First Amendment freedoms, through a school newspaper, for instance, they were significantly more likely to support them. However, schools simply do not make teaching the matter a priority.

It may be unlikely to occur, but the suggestion of this thesis is that an educated citizenry is absolutely necessary to preserve liberties. Thus, it should be absolutely mandatory that high schools teach not just the rights available to individuals in various countries, but also the meanings of those rights. The reasons to protect privacy, for instance, are subtle, and not necessarily immediately apparent. Even the freedom of speech can come under threat during war-time; it must be made extremely clear that that is the time when the right is needed most, during turmoil, not peace. It is true that it is notoriously difficult to educate adults about issues such as civics; however, at least exposing children to these ideas while they are still in school will go an extremely long way towards creating a fair and just society. Privacy and anonymity need great changes to occur if they are to survive; perhaps, as the old cliché goes, that future is in the children.

8. A Wake-Up Call

One important notion can be found throughout this thesis: anonymity is not simply the refuge of the criminal. This point cannot be made strongly enough; so long as that is the prevailing opinion, anonymity will never receive the protection it needs and deserves. Privacy and anonymity are being assaulted by new technologies, and unless they receive popular or legal support, they will not survive intact. Thus, rather than a conclusion, this thesis will end with a wake-up call.

The fight for anonymity is not lost, but it is certainly not proceeding quickly. For example, a California bill (SB 682) which would have kept RFID out of everyday identification such as driver's licenses and medical benefits cards, until such a time as the technology can be shown to be safe for privacy, has been shelved for the time being. However, much of the language from that bill has been added to another, SB 768, which would again provide safeguards for personal data in id's, including mandatory encryption as well as a one-year prison sentence for anyone caught surreptitiously reading these cards. By the support of such bills, the public can make a large difference in privacy policy: recall that it was only after more than twenty-four hundred comments were received by the Department of Homeland Security that US passports had much-needed privacy protection measures added. However, before they will be willing to provide such support, the public will need to be educated about many of the issues described within this thesis.

The beginnings of this education will involve the media reasserting its role as a 'watchdog' for the public good. Soon after the July 7th public transit bombings in London, footage of the attackers, as caught by security cameras, was being broadcast throughout the world. CCTV's 'effectiveness' was being lauded as the men were captured; in the United States, there was outrage about the lack of ubiquitous surveillance systems. However, throughout this process, major news outlets were discussing neither fact that again the cameras had failed to prevent attacks in the first place, arguably the reason that they were installed, nor the impact of cameras in non-crisis situations. The fact that police confiscated many cellular phones in the area, hoping to find pictures of the attackers, was also given little mention other than as a praiseworthy new form of detective work, rather than as both a privacy violation and yet another instance of private citizens being coerced into becoming agents of the state. In a more disturbing situation, the devastation left by both the 2004 Boxing Day Tsunami and 2005's Hurricane Katrina were seized upon as a means to promote RFID. In both instances, groups were described as using the technology to help identify victims, by tracking chips inserted into body bags. In fact, after the Indonesian tsunami which killed hundreds of thousands of people, a VeriChip spokesman stated that it would have been much easier to identify remains had everyone been implanted with a chip beforehand. By doing this, RFID is legitimized in the public eye; mention it in the future, and it will be at least subconsciously thought of as an effective tool for disaster aid. CCTV found a similar benefit from the London bombings, as public perception changed radically when surveillance was purportedly linked to the capture of the attackers. It is in times of crisis that technologies are

frequently introduced or legitimized; a properly functioning press corps helps to ensure that these measures do not pass without critical review.

There is much future work left to be done. The actual development of effective privacy laws will be a gradual process, but one which must be undertaken. There are many future trends identified in this paper (RFID, GPS, intelligent surveillance cameras, Patriot Act powers online) which must be examined as they progress and develop. Also, though this thesis has made attempts to be generally applicable, the author realizes that it is focused on North America and Europe; privacy in Asia, and particularly in developing nations must be studied.

The reader of this thesis is not asked to undertake these tasks, but to make an effort to remain aware of the work of others. Privacy is a vitally important right, and one which must be defended by many groups, from governments and corporations to the general public. Even if the reader disagrees with this statement, he or she is asked to at least develop a rationale of why he or she disagrees; an educated opposition is far more constructive to both sides than ignorance. If the battle for privacy is lost on well-reasoned grounds, so be it; this author desires only that it not be lost due to apathy.

9. Works Cited

"Abstinence-Only Sex Education", (2005, January) (*Planned Parenthood)*, Available: http://www.plannedparenthood.org/pp2/portal/files/portal/medicalinfo/teensexualhealth/fact-abstinence-education.xml (Last Accessed: 2005, September 8)

ACLU. (2002, October 24), "Section 215 FAQ", (*ACLU*), Available: http://www.aclu.org/Privacy/Privacy.cfm?ID=11054&c=13 (Last Accessed: 2005, September 8)

ACLU. (2002) "What's Wrong With Public Video Surveillance?" (*ACLU*)Available: http://www.aclu.org/Privacy/Privacy.cfm?ID=13482&c=130, (Last Accessed: 2005, January 13)

ACLU. (2004, November 26), "Naked Data: How The U.S. Ignored International Concerns and Pushed for Radio Chips In Passports Without Security", (*ACLU*), Available: http://www.aclu.org/Privacy/Privacy.cfm?ID=17078&c=130 (Last Accessed: 2005, April 6).

Akin, D. (2004, November 26), "CIBC faxes go to scrapyard", (*The Globe And Mail*), Available: http://www.theglobeandmail.com/servlet/story/RTGAM.20041126.wxcibc1126/BNStory/Business/ (Last Accessed: 2005, September 8)

AMA Research. (2001) "2001 AMA Survey: Workplace Surveillance and Monitoring", (*American Management Association*), Available: http://www.amanet.org/research/pdfs/ems_short2001.pdf (Last Accessed: 2005, September 8)

The American Heritage Dictionary of the English Language, Fourth Edition. (2000) Houghton Mifflin Company.

ARTICLE 29 Data Protection Working Party. (2005, January 19), "Working document of data protection issues related to RFID technology", Available at: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf (Last Accessed: 2005, April 22).

Bednarz, A. (2004, November 29), "Leeway found in Wal-Mart's RFID Mandate", (*Network World*), Available: http://www.nwfusion.com/news/2004/112904walmart.html (Last Accessed: 2005, April 22).

Bentham, J. (1995) The Panopticon Writings. Ed. Miran Bozovic. Verso. p. 29-95

"Big Brother Nixes Happy Hour", (2005, July 27), Eye on the NLRB: Workers Rights Watch. (*American Right at Work*), Available: http://www.americanrightsatwork.org/workersrights/eye7_2005.cfm (Last Accessed: 2005, September 8)

Big Research. (2004, December 16), "Consumer Awareness and Concern About RFID on the Rise", (*Big Research*), Available: http://www.bigresearch.com/news/big121604.htm, (Last Accessed: 2005, April 22).

Brin, D. (1998) *The Transparent Society*, Perseus Books.

Carey, B. (2005) "The Secret Lives of Just About Everybody", New York Times, January 11 2005.

Casey, A. (2001) *Psychodrama: Applied Role Theory in Psychotherapeutic Institutions*, Journal of Heart Centered Therapies, Spring 2001. Available: http://www.findarticles.com/p/articles/mi_m0FGV/is_1_4/ai_74221526 (Last Accessed: 2005, September 8)

"Cashless society gets mixed reviews", (2003, February 8), (*CNN*), Available: http://edition.cnn.com/2003/TECH/ptech/02/08/cash.smart.ap/ (Last Accessed: 2005, September 8)

CASPIAN et al. (2003, November 20), "RFID Position Statement of Consumer Privacy and Civil Liberties Organizations", (*PrivacyRights.org*), Available: http://www.privacyrights.org/ar/RFIDposition.htm (Last Accessed: 2004, September 13).

Cavoukian, A. (Ontario Privacy Commissioner). (2004, February), "Tag, You're It: Privacy Implications of Radio Frequency Identification Technology" Available: http://www.ipc.on.ca/docs/rfid.pdf (Last Accessed: 2005, April 22).

"Common Sense", (2005, September 9), (*Wikipedia*), Available: http://en.wikipedia.org/wiki/Common_Sense_%28Book%29 (Accessed: 2005, September 9).

Cottrell, L. (Date Unknown), "MediaFAQ", (*Anonymizer*), Available: http://www.anonymizer.com/media/faq.shtml (Last Accessed: 2005, September 8)

Council of the European Union. (2005, February 24), "Draft framework decision on the retention of data ...." Available: http://www.statewatch.org/news/2005/apr/draft-data-retention-proposal.pdf (Last Accessed: 2005, September 8)

EFF. (2003, October 27), "EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities", (*EFF*), Available: http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (Last Accessed: 2005, September 8)

"The EPC Network", (2004) (*SmartCode*), Available: http://www.smartcodecorp.com/solutions/EPC_overview.asp (Last Accessed: 2005, April 22).

"EU data retention plan set for 'climactic battle'", (2005, August 22), (*silicon.com*), Available: http://hardware.silicon.com/storage/0,39024649,39151584,00.htm (Last Accessed: 2005, September 8)

Feller, B. (2005, January 31), "First Amendment No Bid Deal, Students Say", (*Yahoo News*), Available: http://news.yahoo.com/news?tmpl=story&cid-519&u=/ap/20050131/ap_on_re_us/students_first_amendment (Last Accessed: 2005, January 31).

Foucault, M. (1977) "Author Function", In Foucault, M. "What is an Author?" Trans. Donald F. Bouchard and Sherry Simon. In *Language, Counter-Memory, Practice.* (1977) Ed. Donald F. Bouchard. Cornell University Press, pp. 124-127.

Foucault, M. (1983) *The Subject and Power.* Afterword.*Michel Foucault: Beyond Structuralism and Hermeneutics*. 2nd ed. Hubert Dreyfus and Paul Rainbow. University of Chicago Press. 208-26.

Garfinkel, S. (2000) Database Nation: The Death of Privacy in the 21st Century, O'Reilly Media, Inc.

Garfinkel, S. (2002, October), "An RFID Bill of Rights", (*Technology Review*), Available: http://www.technologyreview.com/articles/02/10/garfinkel1002.asp (Last Accessed: 2005, April 7).

Garfinkel, S. (2004, November 3), "RFID Rights", (*Technology Review*), Available: http://www.technologyreview.com/articles/04/11/wo_garfinkel110304.asp (Last Accessed: 2004, November 3).

Gidari, A. (2005) Comments during panel session: "Location Tracking: The Future of Surveillance" April 15, 2005 at CFP2005, Seattle, Washington, USA.

Gill, M. and Spriggs, A. (2005) "Assessing the Impact of CCTV", Available: http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf, (Last Accessed: 2005, May 14)

Green, M. (1999) "The Appropriate and Effective Use of Surveillance Technologies in U.S. Schools", Available: http://www.ncjrs.org/school/ch2a_5.html (Last Accessed: 2005, January 13)

Gross, G. (2004, July 15), "RFID users say no privacy law needed", (*ComputerWorld*), Available: http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,94543,00.html (Last Accessed: 2004, December 20).

H.R. 3162 (2001, October 24) USA PATRIOT Act, (107th Congress, 1st Session) Available: http://www.epic.org/privacy/terrorism/hr3162.html (Last Accessed: 2005, September 8)

Harper, J. (2005, April 15), Prepared Remarks of Jim Harper, Editor of Privacilla.org, to the Computers, Freedom, and Privacy Conference Panel Entitled "The Economics of Privacy: Market or Regulation?", (*Privacilla.org*), Available: http://www.privacilla.org/releases/CFP_Remarks_04-15-05.html (Last Accessed: 2005, September 8).

Harris, L & Assoc. (2003) Harris Study #18203, Available: http://cgi.irss.unc.edu/cgi-bin/POLL/search.all.cgi?w1=Harris%20study%20no.%2018203, (Last Accessed: 2005, June 13)

Harris, L & Assoc. (2004) Harris Study #20621, Available: http://cgi.irss.unc.edu/cgi-bin/POLL/search.all.cgi?w1=Harris%20study%20no.%2020621, (Last Accessed: 2005, June 13)

Hays, C. (2004, November 14), "What Wal-Mart Knows About Customers' Habits", *New York Times.* Sec. 3 p. 1.

Helsingius, J. (1994, December) Interview with Volker Grassmuck. IC Magazine, NCC Publishing. Available: http://waste.informatik.hu-berlin.de/Grassmuck/Texts/remailer.html (Last accessed: 2005, September 8)

Hines, M. (2004, July 23), "Portuguese pooches to get radio-tagged", (*CNet*), Available: http://news.com.com/Portuguese+pooches+to+get+radio+tagged/2100-7343_3-5281608.html (Last Accessed: 2005, April 22).

"House OKs penalties for false Web records", (2004, September 22), (*CNN*), Available: http://edition.cnn.com/2004/TECH/internet/09/22/web.records.reut/index.html (Last Accessed: 2004, September 22)

Hudson, A. (2003, December 14), "Bug devices track officials at summit", (*The Washington Times*), Available: http://washingtontimes.com/national/20031214-011754-1280r.htm (Last Accessed: 2005, September 8)

"Information on subscribers of Cellular telephone ... in Japan" (2005) Available: http://www.soumu.go.jp/joho_tsusin/eng/Statistics/telephone.html (Last Accessed: 2005: September 9)

Introna, L. and Wood, D. (2004) Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems, 2, 177-198.

"Jealous Lovers: No Web Snooping", (2005, August 27), (*Wired News*), Available: http://www.wired.com/news/privacy/0,1848,68674,00.html (Last Accessed: 2005, September 8)

Jha, A. (2003, July 19), "Tesco tests spy chip technology", *(The Guardian)*, Available: http://www.guardian.co.uk/uk_news/story/0%2c3604%2c1001211%2c00.html (Last Accessed: 2005, April 22).

Juels, A. et al. (2003) "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy". In V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press.

Kim, P. (2001, November 14) Auto-ID Center Communications. Available: http://www.cryptome.org/rfid/pk-fh.pdf (Last Accessed: April 22, 2005).

Kinzer, S. (2004) Chicago Moving to 'Smart' Surveillance Cameras, New York Times, September 21, 2004.

Krebs, B. (2005, July 18) "Data Breeches Spur Congressional Action" (*The Washington Post*), Available: http://www.washingtonpost.com/wp-dyn/content/article/2005/07/18/AR2005071800613.html (Last Accessed: 2005, September 9)

Lacan, J. (1949, July 17) *The Mirror Stage as Formative of the I Function.* In Lacan, J. (2002), Ecrits, Trans. Bruce Fink, Norton & Company, pp. 3-9.

"In Landmark Ruling, Washington Supreme Court Says Police Need Warrant for Surveillance with Global Tracking Devices." (2003, September 11), (*ACLU*), Available: http://www.aclu.org/Privacy/Privacy.cfm?ID=13575&c=130 (Last Accessed: 2005, September 9)

LaRoche, G. (2004, July 7) "More than nine million cell phones in Sweden", (*Industry Canada*), Available: http://strategis.ic.gc.ca/epic/internet/inimr-ri.nsf/en/gr125713e.html (Last Accessed: 2005, September 9)

Lyon, D. (1994) The Electronic Eye: The Rise of the Surveillance Society, University of Minnesota Press.

Lyon, D. (2001) Surveillance Society: Monitoring Everyday Life, Open University Press.

Lyon, D. (2003) Surveillance after September 11, Polity Press.

Lyons, B. (2005, January 11) "Ruling gives cops leeway with GPS" (*Times Union*), Available: https://lists.resist.ca/pipermail/shadowgroup-l/Week-of-Mon-20050110/000990.html (Last Accessed: 2005, September 9)

McCullagh, D. (2005, January 12), "Snooping by satellite", (*News.com*), Available: http://news.com.com/2102-1028_3-5533560.html (Last Accessed: 2005, September 8)

McDonough, S. (2005) Surveillance Cameras Reduce Public Space, MyWay News, April 18 2005.

McHugh, J. (2004, July), "Attention, Shoppers: You Can Now Speed Straight Through Checkout Lines", (*Wired*), Available: http://www.wired.com/wired/archive/12.07/shoppers_pr.html (Last Accessed: 2004, August 24).

McIntyre v. Ohio Elections Comm'n (93-986), 514 U.S. 334 (1995).

Murray, C. (2004, July 26) "Implantable chips get under the skin of security experts", (*Electronic Engineering Times*), Available: http://www.4verichip.com/nws_07262004.htm (Last Accessed: 2005, April 22).

Nieto, M., Johnston-Dodds, K. and Simmons, C. (2002) Public and Private Applications of Video Surveillance and Biometric Technologies, California Research Board.

Norris C. and Armstrong G. (1999) The Maximum Surveillance Society: The Rise of CCTV, Oxford Press.

Norris, C., McCahill, M. and Wood, D. (2004) The Growth of CCTV: A Global Perspective on the International Diffusion of Video Surveillance in Publicly Accessible Space, Surveillance and Society, 2, 110-135.

OECD. (2002) The Future of Money. (*Organization For Electronic Co-operation and Development*), Available: http://www1.oecd.org/publications/e-book/0302011E.PDF (Last Accessed: 2005, September 8)

Orwell, G. (1949) Nineteen Eighty-Four. Available: http://datadump.galeropia.org/textz.gnutenberg.net/textz/orwell_george_1984.txt (Last Accessed: 2005, September 8)

Ozer, N. et al. (2005, February 7), Letter to Brittan Board of Trustees, (*ACLU*), Available: http://www.eff.org/Privacy/Surveillance/RFID/schools/ACLU_EFF_EPIC_letter.pdf (Last Accessed: 2005, April 22).

Packard, V. (1967, January 8), "Don't Tell It To The Computer", *New York Times Magazine*, 236.

Palmer, D. (2005), Psychology 315: Psychology of Adolescence course notes. (*University of Wisconsin-Stevens Point*), Available: http://www.uwsp.edu/psych/dp/website%20psych%20315%20spring%202005/Psychology%20315%20Identity%20Development.pdf (Last Accessed: 2005, September 8)

Parenti, C. (2003) The Soft Cage, Basic Books.

Privacy International (1995) "Statement on Closed Circuit Television Devices", Available: http://www.privacyinternational.org/issues/cctv/statement.html, (Last Accessed: 2005, January 18)

Privacy International. (1997) "CCTV: Frequently Asked Questions", Available: http://www.privacyinternational.org/cctv/, (Last Accessed: 2005, June 13)

"Quarterly statistics find that 90 percent of Germans have a cell phone." (2005, August 16), (*Heise Online*), Available: http://www.heise.de/english/newsticker/news/62858 (Last Accessed: 2005, September 9)

Retail Industry Leaders Association, (2004, June 21) Presention at the Federal Trade Commission RFID Workshop, Washington DC. Available: http://www.ftc.gov/bcp/workshops/rfid/wood.pdf (Last Accessed: 2005, April 22).

"RFID", (2005, April 21), (*Wikipedia*), Available: http://en.wikipedia.org/wiki/RFID (Last Accessed: 2005, April 22).

Rosenberg, R. (2004) *The Social Impact of Computers*, Third Edition, Elsevier Academic Press.

Schneier, B. (2004, October 4), "Passport radio chips send too many signals", (*International Herald Tribune*), http://www.iht.com/articles/541711.html (Last Accessed 2005, April 15).

Sexual Offences Bill. (2003), House of Commons (Britain), Home Affairs Committee. Fifth Report of Session 2002-03. HC639.

Singel, R. (2004, October 21), "American Passports to Get Chipped", (*Wired*), Available: http://www.wired.com/news/privacy/0,1848,65412,00.html (Last Accessed: 2005, April 6).

Smith, L. (2004, April 1) "Remarks to the American Bar Association Intellectual Property Section", (*Congressman Lamar Smith*), Available: http://lamarsmith.house.gov/News.asp?FormMode=Detail&ID=378 (Last Accessed: 2005, September 8)

Stanley, J. (2004) "The Surveillance-Industrial Complex", (*ACLU*), Available: http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16226&c=282, (Last Accessed: 2005, June 13)

Swartz, J. (2005, June 20), "40 million credit card holders may be at risk", (*USAToday*), Available: http://www.usatoday.com/money/perfi/general/2005-06-19-breach-usat_x.htm (Last Accessed: 2005, September 8)

Swedberg, C. (2005, March 16) "New Mexico Kills RFID Privacy Bill", Available: http://www.rfidjournal.com/article/articleview/1449/1/1/ (Last Accessed: 2005, April 22).

Thoreau, H.D. (1849) *On the Duty of Civil Disobedience*, Available: http://eserver.org/thoreau/civil.html, (Last Accessed: 2005, June 13)

United Nations. (1948), Universal Declaration of Human Rights, Available: http://www.un.org/Overview/rights.html (Last Accessed: 2005, September 8)

US Bill Of Rights. (1791) Available: http://usinfo.state.gov/usa/infousa/facts/funddocs/billeng.htm (Last Accessed: 2005, September 9)

"Victory for Students, Parents and Civil Liberties Groups: Company Announces it will End Tracking Pilot Program" (2005, February 16) (*EPIC*) Available: http://www.epic.org/privacy/rfid/prs_rls-021705.html (Last Accessed: 2005, April 22).

Wallace, J. & Green, M. (1999) "Anonymity, Democracy and Cyberspace", Final Draft of Law Review Article, Unpublished. Available: http://www.computorney.com/anonarticle.htm (Last Accessed: 2005, September 9)

Walton, G. (2001) "China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China", (*International Centre for Human Rights and Democratic Development*) Available: http://www.dd-rd.ca/english/commdoc/publications/globalization/goldenShieldEng.html (Last Accessed: 2005, January 23)

Warren, S. & Brandeis, L. (1890, December 5) "The Right To Privacy", Harvard Law Review, Vol. IV, No. 5. Available: http://www.lawrence.edu/fast/boardmaw/Privacy_brand_warr2.html (Last Accessed: 2005, September 9)

Westin, A. (1970), *Privacy and Freedom,* Atheneum.

Williams, David. (July 29, 2004) "The Strategic Implications of WalMart's RFID Mandate", (*Directions Magazine*), Available: http://www.directionsmag.com/article.php?article_id=629 (Last Accessed: 2005, April 22).

Wilson, J. (2005, June 21), "Censorship: FBI trawls libraries for terrorist readers", (*The Guardian*), Available: http://www.guardian.co.uk/international/story/0,,1510850,00.html (Last Accessed: 2005, June 22)

Wolinsky, H. (2003, November 9), "P&G, Wal-Mart store did secret test of RFID", *Chicago Sun-Times,* p. 36.

"Worldwide Internet Users will Top 1 Billion in 2005" (2004, September 3), (*Computer Industry Almanac*), Available: http://www.c-i-a.com/pr0904.htm (Last Accessed: 2005, September 9)