2000

The Death of Privacy

Darren W. Bax

THE DEATH OF PRIVACY

Darren W. Bax

An Abstract Presented to the Faculty of the Graduate School of Lindenwood University in Partial Fulfillment of the Requirements for the Degree of Master of Corporate and Industrial Communication

2000

ABSTRACT

This thesis will focus on the issue of personal privacy and the growing threat to its existence in a technological society.

The areas most associated with privacy loss include increased government intrusions, legislation, workplace, healthcare industry, Internet, and identity theft. Chapter one provides a historical perspective beginning with primitive culture and their struggle to maintain privacy in the lives. Interesting enough, privacy protection was not mentioned by the judicial system until 1880 when privacy was defined as the "right to be left alone." To address concerns about privacy reform the Supreme Court cited this right of privacy as having "its foundation in the instincts of nature" and as being "therefore derived from natural law."

Few Americans realize that the landmark Roe v. Wade was not a decision whether a mother could have an abortion. The heart of the case dealt with a mother's right to have total control over her body. The Court believed they found this right embodied in the Fourteenth Amendment's Due Process clause.

Chapter two focuses on research done by the major writers and thinkers associated with privacy protection. The American Civil Liberties Union is one such party that is concerned about protecting the rights promised to Americans in the Constitution. The ACLU shows many instances where the Clinton Administration is pushing for less privacy for Americans. The ACLU claims attempts to undermine privacy can be seen as the administration tries to

implement a national identification card. An individual's complete medical, financial, and personal history could be contained in such an identifier.

Chapter three is an in-depth inspection of the three most profound writers of privacy reform. In their book, The Right to Privacy, Ellen Alderman and Caroline Kennedy bring their own unique perspectives as to what privacy means to them. Kennedy, the daughter of President John F. Kennedy has been in the glare of the public spotlight all her life. Alderman had taken privacy for granted, until recently, when she experienced its loss.

A second profound source in chapter three is Judith Wagner DeCew. She is Associate Professor of Philosophy at Clark University. Her discussion of privacy focuses on the ethical ramifications associated with privacy invasion. DeCew is vehemently opposed to drug testing in the workplace. She believes there needs to be a balance between the employers and the employee's rights.

Rounding out the literature review is The Limits of Privacy by Amitai Etzioni. He is currently a Professor at George Washington University. His book questions such topics as: Under which moral, legal, and societal conditions should this right to privacy be curbed. He also was a senior advisor to the White House during the Carter administration. His political background offers a unique perspective to the issue of privacy.

Chapter four focuses on experiences involving the loss of personal privacy by my family and myself. This privacy loss begins for many when a Social security number is assigned. This number has really become a defacto national identifier. This number is used for driver's license, credit history, school identification

number, and many other ways not originally intended. Personal interviews with State Rep. Rich Chrismer, Denise Lieberman of the ACLU, and Dan Wilson, director of library Services for the St. Louis Public Library provide specific examples of what these particular groups and individuals are doing to protect privacy.

Chapter five is a proposed blueprint for privacy reform offered by the author. Researching the historical significance of privacy and how it relates to the privacy concerns of today aided the author. The major writers and thinkers on the subject of privacy reform gave the author both historical and contemporary viewpoints from which to draw change and shape conclusions. Proposed solutions focus on the areas of government legislation, healthcare, workplace, Internet, and identity theft.

THE DEATH OF PRIVACY

Darren W. Bax

A Culminating Project Presented to the Faculty of the Graduate School of Lindenwood University in Partial Fulfillment of the Requirements for the Degree of Master of Corporate and Industrial Communication

2000

COMMITTEE IN CHARGE OF CANDIDACY:

Professor Michael Castro
Chairperson and Advisor

Associate Professor John Knoll

Adjunct Assistant Professor Ben Kuehnle

Table of Contents

Chapter 1

INTRODUCTION

Privacy invasion has become a highly charged topic of discussion the past few years. Every day, the news is filled with stories of privacy abuses from all areas of our society. Log onto any Internet site and listed is their organization privacy statement. These are company policies regarding how personal information will be used. Many would argue that a truly private existence is a thing of the past. What happened to the right of humans to be left alone? The right to privacy has been debated in our country since the 19th century. Although the right to privacy is never mentioned in the Constitution of the United States, Americans have come to associate privacy as an inalienable right. The founding fathers should have further discussed privacy-related issues and their relevance. I have narrowed the concern for privacy into five topics that I believe to be the most relevant and damaging. These concerns are increasing government abuses, abuses in the workplace, healthcare concerns, identity theft, and Internet privacy. As informed citizens, one should be able to decide what should be private about their lives and how to safeguard this precious natural resource.

Historical Perspective

Long before the writing of the Constitution, people were thinking and writing about privacy. In the Old Testament of the Bible, there is a passage describing how Noah's privacy was violated.

> Noah became drunk. He lay uncovered in his tent and Ham violated his father's privacy by looking on his father's nakedness and by telling his brothers about it. (Genesis 9, 21-22)

Even in the Old Testament, the writers were aware of the times when people should be left alone. According to Judith Wagner DeCew, discussions relating to privacy have played a major role in the political, religious, biological, anthropological, and sociological writings of cultures. If this line of thinking is true, almost all forms of human interaction have some form of privacy guidelines in place.

Jean Bethke Elshtain has argued that many early western thinkers realized the great differences between the public and private sectors. She calls these distinctions between public and private as conceptual categories of our existence.

> The public/private distinction has sometimes been taken to reflect differences between the appropriate scope of government, as opposed to self-regulation by individuals. (Elshtain 1)

In today's society it is difficult to determine what information deserves to be private or public. Aristotle was one thinker who understood the public-private dichotomy. He called this distinction the "polis." According to Aristotle, the polis was a structured body politic and province of political activity, as a public sphere where details of government and the proceedings of the city-state developed. Woman, children, and slaves were not allowed to participate in the polis. Their role was to support the men in their public lives. This private sector of their society was called the "oikos." The status of the man in the polis relied on how well he dominated his oikos. A similar idea can be applied in today's

society. There is a greater likelihood that the happier a person is at home, they will also be happier in their public life.

Alan Westen and Margaret Mead believe that privacy customs and norms stem from biological and anthropological roots. Westen and Mead's studies revolve around the animal kingdom. Westen believes that the desire for privacy is not necessarily distinctive to humans. Studies have shown that all animals seek times of privacy or the need to be in a smaller group. One of the main reasons for this need of seclusion is the propagation of the species.

> The parallels between territory rules in animal life and trespass concepts in human society are obvious: in each, the organism lays claim to private space to promote individual well being and small-group intimacy. (Westen 12)

One way the animal kingdom achieves this private space is by the secretion of urine. This acts as a warning to similar animals that this area is occupied. Mead believes that privacy is a cross-cultural and cross-species happening. Her studies show that almost all societies have their own ways of creating distance to avoid physical contact with others to sustain privacy.

> Concealment of the female genitals, seclusion at moments of birth and death, the preference for intimacy for sexual relations (usually performed away from the view of the children), restricted rules of entry into homes by non residents, and the secrecy of group ceremonies are the most common examples of setting such boundaries. (DeCew 12)

There are also some cultures that define privacy in other ways. According to DeCew, these cultures show no concern for privacy bathing, birth, death,

changing clothes, and excretion. The peer groups constantly make privacy difficult because they are together most of the time. These cultures use psychological methods to create privacy barriers.

> Thus restriction of access to oneself or the flow of information about oneself by withholding feelings and expression, averting one's eyes, facing a wall, and so on provide more subtle ways of putting up social barriers. (Westen 12)

This almost innate need for privacy has led societies to guard against intrusions. Surveillance tactics are used to watch people who violate the group's norms. According to Westen, these privacy rules are aggressively enforced. Westen's studies document modern societies' quest to gain privacy through economic autonomy, anonymity, and mobility. Meaning that society wants enough money to purchase what they want, live where they want, and lead a private existence; however, factors out of their control dictate the amount of privacy they have in their lives. Newer technologies, increased government regulation, and population density all play a part in dictating personal privacy. This evolution, though for the greater good of society, also damages the individual quest for autonomy.

Privacy Recognized

One of the earliest mentions of privacy concerns was in 1880 by Judge Thomas Cooley in his legal treatise on torts, in which he conclude the right to be left alone. Strangely enough, the word privacy wasn't mentioned until a year later in DeMay v. Roberts. The defendant in the case had visually observed a woman

during a time of childbirth without her consent. Although the original charge in the case was battery, it was really about the woman's right to be left alone. The Court stated,

> The plaintiff had a legal right to the privacy of her apartment at such a time, and the law secures to her this right by requiring others to observe it, as to abstain from violation. (DeCew 14)

Supreme Court Justices Samuel Warren and Louis Brandeis aided the fight for privacy reform in their landmark article, "The Right to Privacy." According to Warren and Brandeis, "Political, social, and economic changes entail recognition of new rights and the common law, in its eternal youth, grows to meet the demands of society" (1). Many believe that Brandeis was so concerned with privacy because of newspaper publicity surrounding his daughter's wedding. Warren and Brandeis used the words of Judge Cooley, "the right to be let alone" in their article:

> Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops. (2)

Brandeis and Warren were not trying to change judicial legislation with their article. They believed that ample legislation concerning the principle of privacy was in place. Brandeis and Warren wanted citizens to have rights to verify their public information. They also wanted to repress information that wasn't relevant to a person holding pubic office. "Gossip is no longer the resource of the idle and

of the vicious, but has become a trade, which is pursued with industry as well as effrontery" (2). They did believe that laws were in place that would meet the needs of privacy issues in a changing world. Warren and Brandies also understood that there were always going to be concerns with privacy legislation. Assessing monetary damages in privacy suits would be difficult. How does one judge or jury go about deciding a case based on the emotional harm caused a person? (4) DeCew writes,

> Pursuing protection and damages in court for the right that Warren and Brandies defended often requires exposure and more loss of the very same kind of privacy. (DeCew 16)

Landmark Decisions

It was not until 1905 that the Georgia Supreme Court recognized a legal right to privacy. According to DeCew, in Pavesich v. New England Life Insurance Company, the court cited the right of privacy as having "its foundation in the instincts of nature" and as being "therefore derived from natural law." The case dealt with the unauthorized use of the plaintiff's photograph. The court ruled that this indeed was an invasion of the plaintiff's privacy rights. According to DeCew, this recognized privacy as a right in tort law by invoking common law, natural law, and constitutional values (14).

In 1928, the Supreme Court decided another important decision that challenged the Fourth Amendment. In Olmstead v. United States, Olmstead was convicted of the illegal sale of alcohol. This was a direct violation of the National Prohibition Act. Before any of the defendants had been formally charged, they

were put under government surveillance for over five months. A telephone wiretap was the method that the government used. Over this five-month period, eight phones were tapped in the homes and offices of the defendants. At least six prohibition agents listened over the tapped wires and recorded over 775 typewritten pages of conversations. The defendants vehemently objected to the admissibility of the evidence obtained by the wiretapping. They claimed the wiretapping constituted an unreasonable search and seizure that violated their Fourth Amendment rights.

The defendants also argued that these overheard conversations forced them to be witnesses against themselves and thus violated their Fifth Amendment rights. Olmstead believed his Fourth Amendment rights afforded him a "reasonable expectation of privacy." The Court ruled against Olmstead, claiming he intended "to project his voice to those quite outside and that nothing tangible was taken." In 1934, the United States Congress enacted the Federal Communications Act.

> The act prohibited the interception of any communications and the divulgence of the contents of intercepted communications. The Court then overturned the Olmstead decision, extending the exclusionary rule to include wiretapping in federal prosecutions. (Ducat 820)

In 1960, William Prosner believed that more American courts recognized that privacy was in tort law. According to Ducat, a tort can occur with an act causing injury for which there are remedies (G8). Intrusion by the government against individuals is protected by the Constitution. Prosner outlined privacy as comprising four distinct kinds of tort invasion.

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.
3. Publicity that places the plaintiff in false light in the public eye.
4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness (Prosner 21).

Prosner's writing became influential to many courts in the United States. In 1964, Dean Edward J. Bloustein took Prosner's writing a step further. He believed the emotional distress suffered by a victim because of a loss of their privacy should be compensated. He believed the main damage caused by privacy violations was to human dignity (21).

The Court struggled with privacy rights for many years because these rights were never explicitly mentioned in the Constitution. By 1965, the Supreme Court was realizing that privacy violations dealt with other areas of the Constitution. Griswold v. Connecticut was the case that changed many misconceptions the Supreme Court had concerning privacy rights. A Connecticut state appellate court and the Connecticut Supreme Court originally upheld the convictions. Estelle Griswold, executive director of a Planned Parenthood League, and Dr. Buxton, its medical director, were the defendants in this case. They were convicted of a Connecticut statute that made it illegal to use birth control devices and giving information regarding their use. They were fined $100 for providing such information to married couples. The Supreme Court believed this case had roots in the Fourth, Fifth, and Fourteenth Amendments. Justices Goldberg, Warren, and Brennan agreed that Connecticut's birth-control law was unconstitutional and intruded upon the right of marital privacy. Justice Douglas

wrote: "We deal with a right of privacy older than the Bill of Rights, older than our political parties, older than our school system" (840).

According to Douglas, there was a certain amount of privacy that a husband and wife shared with their physician. Douglas argued that this blanket of freedom protected the sexual relationship of married couples. Douglas believed this Connecticut law could have a negative impact upon a marriage. Instead of outlawing the sale of contraceptives, its goal was to forbid their use.

> Would we allow the police to search the sacred precincts of marital bedrooms for the telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marital relationship. (Douglas 840)

The Supreme Court eventually overturned the decision in Griswold v. Connecticut. Questions remained how the Court decided that this law was a violation of Griswold's privacy. The first question that opponents asked was where in the Constitution was this right to privacy found? According to Craig DuCat, author of Constitutional Interpretation, the Court did a poor job of narrowing down exactly which amendments this law violated. In the course of this case, at least six amendments were mentioned in violation of the Connecticut law. Another problem with the decision of the Court was that it seemed to be biased towards a marital relationship. Ducat wrote, "Their depictions of the right stressed its foundation in a particular kind of association rather than in the person" (846).

Roe v. Wade

In later cases, the Court did recognize privacy of individuals, including single people. This decision, giving a constitutional right to privacy, led to the contestable Roe v. Wade abortion case. Originally, three plaintiffs brought suit against Wade, the district attorney of Dallas County in Texas. They were suing because Texas law made it illegal for anyone to destroy a fetus except if a doctor was consulted and the purpose was to save the mother's life. The Supreme Court decided that of the three plaintiffs, only Jane Roe, an unmarried pregnant woman, had cause to sue. Roe claimed the Texas law blocked her rights as a pregnant woman. Supreme Court Justice Blackmun writes,

> Appellant would discover this right in the concept of personal liberty embodied in the Fourteenth Amendment's Due Process Clause; or in personal, marital, familial, and sexual privacy said to be protected by the Bill of Rights. (847)

One question that the Court refused to debate was "when does life begin" for the child. This one question is a main stumbling block for abortion opponents to agree upon. According to DuCat, the Court focused on a scholarly examination of abortion. They were concerned with the first noticeable movements of the fetus. The court also wanted to know the reasons behind the state's abortion law (848). Why was Texas, for example, so worried about abortion procedures? The Court came up with two reasons why Texas was concerned about the abortion issue. Originally, when most abortions were performed, the woman's life was in danger because of the procedure. The state took the stance of restraining the

woman by law to keep her safe. The state's second reason, according to DuCat, was to protect the life of the fetus. This reasoning can be traced to the theory that human life begins at conception. He writes,

> Only when the life of the pregnant mother herself is at stake, balanced against the life she carries within her; should the interest of the embryo or fetus not prevail. (848)

The Supreme Court did believe that Roe should be guaranteed a right to privacy with regards to her unborn child. In deciding against the state's right to prohibit abortion unilaterally, the Court reasoned that maternity or additional offspring could lead the mother to a stressful life and future. The mental and physical health of the mother could also suffer because of the added burdens of childcare. Also discussed was the distress suffered by other parties involved with the unwanted child. What happens to the child when the family is not capable of physically, emotionally, and financially supporting the child? Social issues dealing with the negative stigma of being an unwed mother were also considered. Though some abortion proponents may argue that the woman's right is absolute and she may terminate her pregnancy at any time, the Court did not go so far as to agree with this reasoning. The state and other opponents of abortion, based on the Fourteenth Amendment, argued that the fetus was a person and was guaranteed the rights that accompany this amendment. DuCat writes,

> If this suggestion of person hood is established, the appellant's case, of course, collapses, for the fetus' right to life is then guaranteed specifically by the Amendment. (850)

Texas lawmakers believed that life begins at conception. With this in mind, the State of Texas believed they had a genuine interest in protecting the life of the child until they are born. The Supreme Court, however, believed that Texas law should focus on the well being of the mother more than the unborn child's. The Supreme Court took a middle ground between two absolute arguments about the personhood of the child. It decided that until the end of the first trimester, the state could not get involved with abortion procedures. But after the first trimester, it felt that the state does have the right to regulate abortion procedures. The licensure of the physician, the facility in which the abortion is to be performed, and the licensing of the facility are examples of state requirements that can be regulated. Although members of the Court offered valid dissenting opinions, the majority decided that until the end of the first trimester, the mother, in consultation with her doctor, could decide to terminate the pregnancy without state interference. One of the main factors that influenced Roe v. Wade was the Court's decision a year earlier in Eisenstadt v. Baird.

> If the right to privacy means anything, it is the right of the individual, married or single to be free from unwarranted government intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child. (Brennan 845)

Since the Court decided Roe v. Wade, the Justice Department has given numerous invitations to the Court to overturn their decision but to no avail.

Bill of Rights

One year after the American Revolution in 1776, the Continental Congress met to adopt the Articles of the Confederation. Under these rights, the states declared their freedom from federal government. The weakness of the Articles was that the federal government held little power over the states. In 1789, James Madison took state proposed amendments and wrote nine amendments that would protect citizens from the federal government. The ten that were ratified and added to the Constitution came to be known as the Bill of Rights. In the Bill of Rights, the term privacy is never specifically mentioned but almost everyone will tell you that they all have reasonable rights to privacy. Constitutional litigation regarding privacy concerns has skyrocketed in the past twenty-five years. Until recently, it was famous citizens in the public eye that moaned about their loss of privacy. Now the threat of privacy loss can happen to anyone, at anytime, in all walks of life. The loss of privacy from government agencies, employers, healthcare institutions, privacy on the Internet, and identity theft are five areas of concern.

When the rights to privacy are threatened, there is usually an opposing viewpoint. The rights of the pregnant mother clash with the state's right to protect human life. The rights of the citizen clash with the government's right to protect national security. The rights of the employee clash with the rights of the employer to expect an honest day's work. The question, we, as citizens of the United States, should be asking is: what privacy, if any, does truly exist and how do we safeguard this privacy?

In the remaining chapters, I will explore the ethical, social, legal, medical, and historical ramifications of privacy loss. The questions surrounding privacy loss are: what are the areas where our privacy is being compromised? Who has the power to violate our privacy rights? Where is this personal information being used? When privacy has been compromised, what resources exist to prevent further abuses? How do we safeguard the shrinking privacy that remains?

Chapter II

LITERATURE REVIEW

Any discussion of privacy is incomplete without providing an historical literary perspective by the major writers and thinkers of privacy debate. There is much evolving literature on this topic and I have chosen what I believe to be the most relevant. This chapter discusses five issues related to privacy: government legislation, the workplace, the Internet, healthcare, and identity theft.

Government Legislation

Many current privacy abuses stem from legislation that our government has or is trying to pass. One of the main opponents of government privacy abuses is the American Civil Liberties Union. According to the ACLU, they are a national organization of more than 250,000 members dedicated to preserving the principles of liberty embodied in the Bill of Rights and the Constitution (1). A re-occurring message while researching the ACLU addresses their dedicated effort to stop government legislation creating a national ID card. The Clinton Administration claims the need for a national ID card in order to curb and control the flow of illegal aliens into the United States. This card would be a complete file on the carrier. The person's vital statistics, Social Security intake, address, occupation, medical history, and possibly genetic predisposition for some illnesses could be found on this card. Laura Murphy, Director of the ACLU, is concerned that all this vital information could be used in some way to

discriminate against the carrier.

> A national ID card would infringe on the privacy of all Americans, and would likely result in an increase in discrimination against those who "look foreign" or speak with an accent. (Murphy 4)

Science fiction writer, David Brin, believes there is an advantage to less privacy in our society. In Brin's article in Wired News, he writes of the onslaught of surveillance cameras that seem to be everywhere. Brin, the writer of such post-apocalyptic novels as The Postman, wonders if freedom and privacy can coexist in the future. Brin believes, because of the Internet, the images are passed across the globe instantly. He reasons, in Britain there are more than 500,000 surveillance cameras that keep the peace. The benefit is that the crime rate is lower in Britain than in the United States. According to Brin, the onslaught of information that is available to the government can work both ways.

> In all of history, no government has ever known more about its people than our government knows about us. And yet in all of human history, no people have ever been anywhere near as free. (Brin 3)

The Electronic Privacy Information Center is another group that has vowed to protect the rights promised in the Constitution. They believe that the United States government is trying to use the Social Security number as a new national ID. Recent legislation has been introduced in the House and Senate that would require the inclusion of the SSN on every application for a professional license, occupational license, commercial driver's license, marriage license, divorce

decree, and death certificates. They believe that the inclusion of the SSN runs the risk of creating a national identification system. Created in 1935, the SSN was used for accurately recording individual worker's contributions to the social security fund. Even is 1935, legislatures were distrustful of the SSN and feared that it would be used for keeping personal information like race, religion, and family history. Since that time the SSN has been used for many of these same privacy concerns. The EPIC reports,

> Moreover, even Federal government officials have conceded that the cost of implementing and mandating this database will be astronomical. Although both House and Senate bills contain limits on the use of this database, it is inevitable that political pressure will lead to expanded use of this database for a multitude of unforeseen purposes. This is truly an Orwellian nightmare. (2)

U.S. Rep. Ron Paul of Texas writes that it's too late to stop the SSN from becoming a national identifier. He believes that legislation passed in 1996 has led to this growing problem. This was a welfare-reform bill that states businesses must report the SSN of every new employee to be added to a national database. Even parents of a newborn are forced to get their child an SSN so they can claim him as a dependant for tax purposes (Paul 1). Paul writes that since the inception of the SSN there have been over 40 congressional uses of the SSN for programs not associated with the Social Security program.

> The Social Security number was created to administer the Social Security system and nothing else. We must restore the integrity of the system by restoring the integrity of the accounts. That will only occur when we rein in the use of the account numbers and secure the privacy of the people. (2)

Aaron Russos, former Hollywood movie producer and Nevada gubernatorial candidate, also opposes a national identifier. When he ran for governor in 1998, privacy reform was one of his major platform issues. He states,

> I believe that America is rushing headlong into becoming a socialist totalitarian society and I want to stop it. I see the federal government disobeying the Constitution. When the government is allowed to take control by force and act unlawfully, then that's tyranny. (Russos 5)

Much of what Russos warns against is legislation that was signed into law by President Clinton in 1997. The Omnibus Appropriations Act was designed for the purpose of keeping illegal aliens from working in the United States. This law establishes in reality a national database to track employment eligibility. In Russos's bid to fight big government, his beliefs are influenced by the Tenth Amendment, which is based on states-rights issues (Dowbenko 16).

Recent government legislation has shifted its efforts to the telecommunications industry in attempts to curtail certain forms of privacy. With the help of the Federal Communications Commission, a government appointed agency; the Clinton Administration will try to implement the Communications Assistance for Law Enforcement Act. Under section 103, all whirling, cellular, and broadband personal communications services would be required to adhere to certain guidelines.

> Section 103 generally requires a telecommunications carrier to ensure that its equipment, facilities, or services are capable of: (1) expeditiously isolating, and enabling the government, pursuant to a court order or other lawful authorization, to intercept all wire and

> electronic communications; (2) providing access to call-identifying information that is reasonably available to the carrier; (3) delivering intercepted communications and call-identifying information to a Law Enforcement Agency in an acceptable form and at a remote location; and (4) protecting the privacy and security of communications and call-identifying information not authorized to be intercepted. (CALEA 1)

The carriers that follow these standards will be given a rating as CALEA compliant. Unfortunately, the FCC doesn't state if they agree with CALEA and its proposed misuse of so-called private communications.

Simon G. Davis, of the University of Essex, believes that biometric technology will eventually be a true national identifier. Biometric identification uses fingerprints, hand geometry, and retinal scanning to tell us apart from others. He believes that widespread use of biometric technology would create a class of outcasts from society. According to Davis, the potential benefits of biometric identification are: the cost of administration, the integrity of identification, information integrity, speed of delivery of services and benefits, accuracy and quality of research and statistics, and technical security of communications (1). Davis believes the harm that biometric identifiers will cause outweighs the benefits.

> That people will be de-humanized, the system will enhance the power over individuals of particular organizations and the state, the system is a hostile symbol of authority, that society is becoming driven by technology-assisted bureaucracy, rather than by elected government, and that such identification schemes are the mechanism foretold in religious prophecy, "The Mark of the Beast." (2)

In 1998, Vice-President Al Gore announced his plan towards an Electronic Bill of Rights. Gore's plan focuses on privacy reform dealing with the protection of medical records, the protection of the privacy of children on-line, and the challenge to protect privacy on-line and halt identity theft (2). Gore believes that privacy reform is needed because the rise of new technology makes the sharing of information easier. Gore has pledged to work with state officials to create a balance between information that is collected by the government and citizens' rights to confirm the validity of information.

> You should have the right to choose whether your personal information is disclosed; you should have the right to know how, when, and how much of that information is being used; and you should have the right to see it yourself, to see if it's accurate. (Gore 1)

On August 11, 1998, the Center for Democracy and Technology offered a rebuttal to Vice-President Gore's plan. They believe that although the Clinton Administration made an effort to address the need for privacy reform, that plan was conservative to say the least. Gore's plan to increase penalties for identity theft was an endorsement of legislation previously passed. The CDT believes Gore's attempt to protect the privacy of medical records was a smokescreen for the Clinton Administration's plan for an unpopular health care ID number. Also troubling to the CDT was the administration's attempt to protect privacy while also pushing legislation for backdoor encryption products (1).

> While this is a first step, CDT believes that a more formal privacy office should be created to provide the government and private sector with an ongoing source of privacy expertise, a forum for

> discussion of technology and privacy issues, and focal point for the development of privacy policy. (CDT 1)

Workplace Privacy

Present and future privacy concerns in the workplace deal with the use of monitoring software. This is a concern for privacy rights' activists because network administrators can watch what each employee does down to the keystroke. Ultimately, the goal is to increase performance and lower the cost of PC ownership. Some could argue this is the electronic version of looking over one's shoulder to invade privacy. Valerie Rice of PC Week writes that an estimated seventeen- percent of Fortune 1000 companies has monitoring software (Rice 83). According to International Data Corp, eighty percent of these companies, by the year 2001, will have either evaluated or installed monitoring software. Robert Rubin, CIO of Atochem North America, doubts whether monitoring employees really improves productivity. "You have to treat people like they are professionals-otherwise morale suffers. And if you're wondering whether they're using an application on their desktop, don't monitor them, just ask" (Rubin 83).

Companies interested in hiring talented people must realize they have an obligation to preserve the privacy rights of applicants. Kim S. Nash, of Computerworld writes that employers can be sued for faulty hiring practices. Previously, background checks were only performed for upper management

positions. "If companies don't do them, they may get some bad apples and even face lawsuits for negligent hiring. But employers also must be careful not to trample applicants' privacy rights in the process," writes Nash. Financial information can only be obtained with the signature of the applicant. Employers can get criminal records from any town where the applicant has lived. Civil suits against a former employer are also public information and are routinely checked. Nash writes that employers cross the line of privacy invasion when they seek medical history or worker compensation claims. Employers who deviate from proper guidelines can turn to a wealth of black market information (Nash 43).

To privacy extremists, any form of employee monitoring is a privacy violation. Joseph R. Garber of Forbes is not against monitoring of employees. He opposes the protection of those who abuse their privileges. He believes those who oppose monitoring fail to realize that this practice is nothing new. Many organizations have been monitoring phone and computer usage for years. Only recently has this practice taken center stage in the work place.

> Last year American industry's tab for computer hardware and software, communications, training and support was half a trillion dollars. That's big money and those who spend it have an obligation to make sure it's spent right. (Garber 297)

Even the ACLU believes that employees have limited, if any, rights in the workplace. As of Garber's writing, there were over 57 pieces of privacy legislation in the House and Senate.

> Computers make it easy to measure productivity; no surprise, the unproductive resent it. The technology can't be stopped, so

> malingerers are pinning their hopes on the courts and legislatures. (Garber 297)

A recent proposal, presented by Missouri State Senator Larry Rohrbach, is aimed at protecting state employee's privacy rights. According to Gerry Tritz of the Jefferson City New Tribune, the bill would prevent state agencies from releasing information on state employees. Currently, the names and addresses of any state employee can be purchased from the Department of Revenue. The main culprits for this abuse are direct mail companies and union groups. The state employees can request their names to be taken off the list sold to direct marketers. Unfortunately, state regulations don't allow employees to delete their names from union lists. The Office of Administration sends union groups updated lists of state employees and their addresses on a quarterly basis (Tritz 9). Rohrbach's plan is to ban state agencies from releasing any personal information without prior consent. Union representatives claim this is an attempt to weaken the unions and hinder their efforts to recruit new members. Rohrbach states, "I have difficulty understanding why organized labor wants to violate the privacy of state employees. It's very disrespectful to them" (9).

Drug testing in the workplace has become a common occurrence in today's society. Solange E. Bitol, of the ACLU, believes all drug testing in the workplace is a privacy violation. "These tests are unnecessary because they cannot detect impairment and thus, in no way enhance an employer's ability to evaluate or predict job performance," writes Bitol (1). Bitol doesn't dispute that employers have the right to run a productive workplace. He believes that testing only

indicates that drugs have been taken in the past. In no way does a drug test rate job performance of employees. In 1989, the Supreme Court ruled that workplace drug testing is a violation of Fourth Amendment rights. Although the court ruled in favor of privacy rights activists, some occupations don't apply. Occupations where the government has an interest in maintaining a drug-free workplace outweigh Fourth Amendment privacy rights. The courts have done little to protect the rights of private sector employees against random drug testing. Bitol claims that drug testing reveals more than the existence of illegal drugs. Genetic predisposition to disease, physical and medical conditions, and pregnancy can be detected through drug testing (Bitol 3). In 1988, The Washington D.C. Police Department admitted it had screened female employees for pregnancy through urine samples without their consent.

> Employers may be tempted to use hair testing to deny employment to people with these conditions. Because it enables employers to learn such personal medical information about employees, hair testing, like urine testing, is a serious invasion of privacy. (Bitol 3)

Internet Concerns

The Internet has experienced a tremendous growth cycle the past two years. In the early stages of the Internet, it was thought by many to be a fad; a novel way to find information and communicate with friends. I remember asking my boss about three years ago if our company would be getting a company website. His response was that the Internet would never take off. Not less than a year later, he had a great idea about getting someone to design a company website. It's funny

how fast people can realize the error of their ways. Not only is the Internet a valuable tool for finding information, it will eventually be a major force with regards to business transactions. Companies that don't prepare for this day will be left to fight for the leftovers. So it is no surprise that privacy issues have arisen in the Internet world. Stephan Manes of PC World writes, "Here as elsewhere, the Internet is merely an extension of the rest of life, where privacy has become a casualty of a capitalist paradise where we trade personal information for cash, convenience, and goodies" (Manes 316). According to Manes, people have little knowledge of who possesses their personal Internet information. Giving out one's e-mail address is one of the worst ways to lose privacy. That information can be transmitted to others instantly.

This loss of privacy also has its advantages. Much of our financial history is bought and sold by credit bureaus that supply this to credit card companies, mortgage companies, and banks. This sharing of information is critical to our being able to function financially. Manes writes, "The alternative—passing up credit entirely—is impractical in a world where plastic money is a virtual necessity" (316).

A recent court decision by Detroit Federal Judge Nancy Edmonds may have set a major precedent for free speech in cyberspace (Biskupic A02). This case was a dispute over confidential Ford Motor Company documents that were being broadcast over the Internet. The operator of the website claimed to have received the documents from an anonymous source. Edmunds refused to block the publishing of these documents on the Internet. "In this case, the battle is won by

the First Amendment," Edmunds concluded (A02). Joan Biskupic of the Washington Post states that the Internet has changed the way people live but the law hasn't followed suit.

> Unlike the rise of broadcast television and other media over the decades, in which new technologies generated new bodies of law and extensive government regulation, the Internet is being treated much like newspapers or books, with judges emphasizing the primacy of the First Amendment. (A02)

Recently, state organizations have started to publish information about state employees on the Internet. This information has been public record for many years. Before, however, this information was not easily accessible to people. The Internet allows users the ability to transmit large amounts of information immediately. Jeff Moad of PC Week reports that's what got Illinois State Comptroller, Loleta Didrickson into trouble. First, she started to publish state financial information on the web. This tactic met with positive feedback from taxpayers. Her next act was posting public information about state employees on the web (Moad 83). Moad writes, "Once the data was easily accessible up on the Internet, employees saw it as a threat to their privacy" (83). The Internet is forcing many organizations to rethink what information should be made public. Many groups are consulting with employees to get their input on what information should be made public. Several states are creating committees to come up with an Internet posting policy. Moad writes that government organizations will continue to publish information on the Internet primarily because legislation isn't in place to protect these privacy rights.

Medical Records

Citizens that are worried about their medical records remaining a private matter are fighting an uphill battle. Amiee Howard of Insight on the News claims a lack of legislation is causing the concern. Medical and technological advances have grown faster than the legislation (Howard 18). Who has the right to access your medical records, besides a doctor? Currently, insurance companies, pharmaceutical companies, and employers all have access to private medical history. Some companies claim to have medical records of 15 million Americans and Canadians. This data is supplied to over 700 insurance companies. The files contain a complete medical history ranging from surgical procedures, and family medical history, to previous prescriptions (Howard 18). What happens if employers have access to private medical history when screening job applicants? The last presidential administration to appoint a commission for privacy protection was the Carter Administration. David Linowes, who chaired the commission writes, "About 35 percent of Fortune 500 companies use medical records in making personnel decisions" (18).

The Center for Democracy and Technology is another lobbyist organization that supports medical record privacy legislation. One such bill that they supported was the Medical Records Confidentially Act of 1995. This bill would have given people the right to see and correct their medical records, limit disclosure to outside sources, and impose strict penalties for violating the Act (Goldman 2). The CDT believes that a strong medical record's policy must be in

place to ensure continued public trust of the healthcare system.

> In March of this year, a 13-year-old daughter of a hospital clerk printed out the names and phone numbers of patients who had been treated at the University of Florida's Medical Center. As a hoax, the 13-year-old girl then contacted seven patients and erroneously told them they were infected with HIV. After receiving one of these prank calls, a young girl attempted suicide believing she had the HIV virus. (CDT 2)

Jeremy Gruber of the ACLU believes there need to be strict guidelines on data discovered from genetic research. Genetic research is the identifying, analyzing, and manipulation of DNA (Gruber 1). A current government project, the Human Genome Project, is designed to study the estimated 100,000 human genes. These findings can tell genetic predisposition to many diseases and aid in the cure. The ACLU has discovered this genetic information has been used for employment discrimination purposes.

> In a 1996 Georgetown University study of 332 families belonging to genetic disease support groups, 22% of the respondents stated that they had knowingly been refused health insurance and 13% stated that they had knowingly been terminated from their jobs because of the perceived risks attributed to their genetic status. (Gruber 1)

Studies by the U.S. Department of Labor show that genetic testing in the workplace is increasing. This testing can be discriminatory for prospective employees, current employees, and the family members of such employees.

> Consider the pregnant woman whose fetus tested positive for cystic fibrosis and whose managed-care health plan limited coverage for her pregnancy and future children while offering full coverage should she choose an abortion. (Gruber 2)

Gruber claims that inadequate genetic legislation exists to properly protect the privacy rights of individuals. Only twenty-four states offer protection from genetic discrimination. This only protects individuals from discrimination from health insurance claims.

Identity Theft

The National Organization for Victim Assistance held their twenty-fifth annual conference in Los Angeles on August 29, 1999. The keynote speaker was Beth Givens of the Privacy Rights Clearinghouse. The discussion focused on identity theft. Identity theft occurs when someone obtains vital information about an individual. This may begin with someone using a person's social security number for misrepresentation.

> Examples are obtaining credit cards and loans in someone else's name and then not paying the bills. Opening utility accounts, renting an apartment, getting a cellular phone, purchasing a car or a home, and so on. Another type of identity theft – what I call the worst case scenario – is when the perpetrator commits crime in the victim's name and gives that person a criminal record. (Givens 1)

Givens blames much of identity theft on the credit bureaus. She believes they make it much too easy for people to obtain credit. This usually come in the form of pre-approved credit cards received in the mail. She warns that these solicitations should be shredded immediately. Many victims of identity theft are helpless because such thefts do not get the attention of law enforcement officials.

The officials spend the majority of their time focusing on violent crimes.

> Many violent criminals are moving to identity theft because they know that law enforcement resources are not yet sufficient to investigate the majority of such crimes. (Givens 2)

On July 12, 1999, Queen's New York District Attorney, Richard A. Brown, announced a 268-count indictment against nine Nigerian nationals for credit identity fraud. The investigation began with evidence of heroin trafficking and led law enforcement officials to uncover an elaborate identity theft scheme.

> Our investigation revealed that the defendant Ayodele Peters and his co-conspirators had accumulated financial and personal information, including mothers' maiden names, of approximately 1,300 legitimate citizens from across the country, which gave the defendants access to about $10 million dollars in credit. (Brown 2)

According to Brown, the defendants allegedly stole over $1.4 million dollars from twenty banks and credit card companies. The defendants obtained most of this information from a former employee of a car rental company who supplied them with customer car rental forms. These forms had the person's social security number, credit card number, and copies of his driver's license. Once armed with this information, the defendants are alleged to have established new accounts, transferred accounts, withdrawn funds, and filed false tax returns (2).

Gill Klein of Media General News Services writes that identity theft is one of the fastest growing crimes in the United States. This problem has become so large that law enforcement officials have difficulty determining the size. In 1997, the two largest credit card companies reported fraud losses of several hundred

million dollars. Klein states a report by the Secret Service claims losses associated with identity fraud increased from $442 million in 1995 to $745 million in 1997. To make up for these losses, credit card companies charge customers in the form of higher interest rates and fees (Klein 1).

A task force appointed by Washington State Attorney General Christine Gregoire is focused on identity theft issues. The task force will address what direct marketers, retailers, and banks do with consumer information. Jane Hadley of the Seattle Post reports that Gregoire created the task force because of several complaints concerning the use of credit card and personal information obtained from financial institutions.

> Seattle resident Dick Dickenson said his bank sold his account information to a company. Which then told him it would send him a credit report and charge him unless he said no. (Hadley 2)

Members of local banks urged the task force not to stop them from disclosing this information to other parties. Bob Harvey, president of the Seattle Metropolitan Credit Union, claims they sell lists only to companies that can offer their customers a benefit. Many customers don't mind the trading of information; however, they would like to know when it happens (Hadley 2).

As with any major societal concern, there are many major thinkers and writers addressing privacy issues, however, not all were relevant to the concerns of average citizens. There is a plethora of authors writing on privacy concerns but not all were relevant to this literary review. These authors, although highly credible, did not adequately address the scope of the five topics. The related

issues not explored here include the privacy anxiety of famous people sparked by the death of Princess Diana and the Clinton/ Lewinsky scandal. Much has been written as well concerning records being given to adopted children, enabling them to find out who their birth parents are and possibly contact them. Many parents, who gave who gave their children up, are fearful that the children's ability to use records to locate them compromises their privacy. Colleges and Universities also face their own privacy debate. Do institutions give out the private information of their students like grades, crimes, and disease to the parents?

Privacy is an issue that has been debated for hundreds of years. What has changed the scope of privacy more than anything is the rapid expansion of technology. What Justices Brandeis and Warren envisioned as invading our privacy were mechanical devices used to create newspapers and photographs, where private concerns could be shouted from rooftop to rooftop. With today's emerging technology, those same concerns from two hundred years ago can now be spread from desktop to the world.

Chapter III

SELECTIVE LITERATURE REVIEW

A tremendous resource concerning privacy issues is The Right to Privacy by Ellen Alderman and Caroline Kennedy. Alderman and Kennedy met while attending the Columbia University School of Law. With the writing of this book, both added their unique perspectives as to what privacy means. Kennedy, the daughter of the late President John F. Kennedy, has been in the public eye all her life. Alderman had taken privacy for granted, until recently, when she experienced its loss. In their book, they tell the stories of average citizens who have suffered privacy loss at the hands of government agencies, law enforcement, and employers.

Illegal Searches

When people claim their right to privacy, the Fourth Amendment is usually the basis for their discussion. The amendment states that people have the right to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures. Alderman and Kennedy write of such abuses that were, until recently, still going on within the Chicago Police Department.

One such abuse involved Mary T. and Lillian who were secretarial students. According to Kennedy and Alderman, the two had borrowed a friend's car for the afternoon. While driving, they were pulled over for not having proper identification for the car. Mary T. and Lillian tried to explain to the officer that they had borrowed the car. They began to argue with the officers and were

arrested for disorderly conduct (Alderman & Kennedy 6). At the police lockup, they were subjected to full body cavity searches from a female officer. Mary T. stated,

> Then the lady put her hand all the way up inside Lillian. She didn't even wear a glove. I kept telling her she didn't have to do that and to stop. The more I yelled the more the matron kept saying, "You just better shut up, because your turn is coming." She told me she was going to do the same thing to me and she was going to let the men watch, if I didn't cooperate. (6)

This abuse had been standard procedure in the Chicago Police Department since 1952. It was policy that any woman arrested for anything from traffic violations to murder were subjected to a strip search. The policy for men was different than that for women. The men were only subjected to a pat down instead of a full body search. Also a concern was that there was only one lockup for woman in the city of Chicago. They had to be transported, sometimes great distances, to be searched.

> The blanket strip-search policy did not discriminate on the basis of race, age, or class. White, Black, Asian, and Hispanic women, teenagers and grandmothers, doctors, housewives, and college students – all were stripped searched. No exceptions were made. Menstruating women were simply told to remove tampons or drop sanitary napkins. (Alderman & Kennedy 6)

In 1979, the American Civil Liberties Union of Illinois had heard rumors of such abuse by the Chicago Police Department. The ACLU called the NBC television station in Chicago about these abuses. NBC then interviewed several women who had told their stories to the ACLU. Their story encouraged hundreds of women who had suffered this humiliation to contact the ACLU. A class action

suit was filed on behalf of the women against the City of Chicago. Their suit claimed the strip searches violated their Fourth Amendment rights against unreasonable searches and seizures. They also claimed this search violated the Equal Protection Clause of the Fourteenth Amendment because the policy only applied to woman (Alderman & Kennedy 10). Shortly after these abuses were uncovered, the Illinois legislature passed a law prohibiting strip searches unless there was a belief that the woman was hiding a weapon or contraband.

> The City of Chicago agreed to change the police department's policy. But it did not agree that the policy was unconstitutional in the first place. The city defended itself against the charges in the women's lawsuit, claiming that the strip searches were reasonable under the Fourth Amendment. (Alderman & Kennedy 10)

The official policy of the Chicago police was different from what actually happened during these searches. The policy required each woman to:

1. Lift her blouse or sweater and unhook and lift her brassiere to allow a visual inspection of the breast area, to replace these articles of clothing.
2. Pull up her skirt or dress or to lower her pants and pull down any undergarments, to squat two or three times facing the detention aide and to bend over at the waist to permit a visual inspection of the vaginal and anal area. (12)

In this description, there is nothing stated that police officials have the right to physically search the body cavities. Also, the court found no need for two sets of search rules for men and women. The federal district court found the Chicago strip search policy unconstitutional. The City of Chicago appealed to the United States Court of Appeals to overturn the original verdict.

Alderman and Kennedy write that assessing damages in a privacy case is always difficult.

> The harm is almost always emotional rather than physical. The reasons we value our privacy are often hard to articulate. And by definition, the invasion is personal to the individual. (13)

Since each women's experience was different, the court decided that each case be tried separately. A recurring theme throughout each trial was the sense of betrayal and mistrust felt by the women. They also claimed lasting effects from the trauma in their personal lives. Mary T. and many other women claimed they had relationships end because of the experience. They believed that people didn't understand their fear of intimacy, anger, and humiliation after the event (Alderman & Kennedy 13). By going to court, the women were faced with the humiliation of recalling these terrible experiences to the public. The jury awarded Mary T. $45,000, yet she still was angry about the verdict. "No amount of money that they could have awarded me could give me back my dignity – What they took away from me in that jail," she states.

Abortion Rights

The abortion debate has been mistakenly identified as an issue of whether a mother has a right to terminate the life of her unborn child. It is, however an issue of a woman's right to privacy over her own body. Since the Roe v. Wade decision the Supreme Court has been bitterly divided on the abortion issue. The arguments among the courts are not whether abortion is right or wrong; the controversy is whether the courts should be involved in the debate at all. Alderman and Kennedy write,

> In one view, since the word privacy does not appear anywhere in the Constitution, that is the end of the matter. In the opposing view, the concept of liberty in the Constitution necessarily includes a right as fundamental as the right to privacy. (53)

When the Supreme Court decided to overturn the Texas law criminalizing all abortions except those necessary to save the mothers' life, the vote was 7 to 2 making this unconstitutional. Within the last twenty years, the additions of Justices O'Connor, Kennedy, and Scalia have many thinking Roe v. Wade may be overturned.

In Webster v. Reproductive Health Services, the Supreme Court almost did just that. Missouri had passed a law that encouraged childbirth over abortion. This law banned the use of pubic facilities and staff except to save the mother's life. Also, a doctor had to examine women over twenty weeks pregnant to see if the fetus was viable (Alderman & Kennedy 61).

The vote was 5 to 4 in favor of upholding the Missouri law that set restrictions on legal abortions. Justice Scalia wanted the court to overrule the Roe v. Wade decision altogether. Three other justices wanted to do away with the trimester framework described in Roe v. Wade. Justice Sandra Day O'Connor was against revisiting the Roe decision but was in favor of the Missouri restrictions. The original author of Roe v. Wade, Justice Blackmun, criticized the other justices for avoiding the issue at the heart of the case: the right to privacy (Alderman & Kennedy 62). Justice Blackmun believed the court's trimester framework still protected the interest of the state and the mother's right to decide. One last time, Blackmun tried to defend the decision that defined his career as a justice.

> In a nation that cherishes liberty, the ability to control the biological operation of her body must fall within that limited sphere of individual autonomy that lies beyond the will or power of any transient majority. This court stands as the ultimate guarantor of that zone of privacy, regardless of the bitter disputes to which our decisions may give rise. In Roe, we did no more than discharge our constitutional duty. (Blackmun 63)

Medical and Workplace Privacy Collide

In The Right to Privacy Alderman and Kennedy explain how the right to medical privacy and workplace privacy collides. In Doe v. City of New York, John Doe was interviewed by Delta Airlines for a job opening in 1992. Doe claims that Delta asked questions concerning his sexual orientation, marital status, and living arrangements during this interview. Doe was denied employment because of his HIV positive status and homosexuality. Doe filed a complaint with New York City Human Rights Commission claiming discriminatory employment practices. The commission had received over three hundred previous complaints against Delta for the same charge.

Doe settled his case with Delta and was given a job as a customer service representative and awarded back pay, seniority privileges, and a monetary settlement. Both parties also agreed that Doe's name would never be mentioned in the case.

Days after the settlement Doe claims the New York City office issued a press release outlining the settlement. Doe believed the release gave enough information that he was identified as the person, therefore his coworkers

discovered his HIV status (Alderman & Kennedy 141). Doe sued the City of New York and based his case on a 1977 Supreme Court decision, Whalen v. Roe.

> The controversy in Whalen centered on a New York statute, which required that the name, address, and age of every patient obtaining certain dangerous yet legitimate prescription drugs be recorded in a centralized computer bank. (Alderman & Kennedy 141)

Whelan claimed that disclosing names violated privacy and would stop people from seeking medical help. Alderman and Kennedy write that the Court declared that the Constitution protects two types of privacy: One is the right to make fundamental decisions and the other is the right to avoid disclosure of personal matters. In 1994, the U.S. Court of Appeals used Whalen v. Doe as precedent to decide the Doe case. The court stated that a person's HIV status was a protected medical record, therefore granting a constitutional right to privacy. The court declared,

> Extension of the right to confidentiality to personal medical information recognizes there are few matters that are quite so personal as the status of one's health. Clearly, an individual's choice to inform others that she has contracted what is at this point invariably and sadly a fatal, incurable disease is one that she should normally be allowed to make for herself. (142)

Alderman & Kennedy write that although individuals have a right to privacy concerning medical information, it is a limited right. "Anyone wishing to bring a constitutional privacy claim must remember that the Constitution only protects us against violations by the government," write the authors.

In Doe v. City of New York, Delta Airlines did what many companies are doing daily, only they took their search too far in finding the best candidates. Alderman and Kennedy state that a pre-employment drug screening, video surveillance, and telephone and computer monitoring are standard practices in today's competitive job market. Employees concede many privacy concerns in turn for a stable working environment. Many employers argue they have a right to know what employees do on their free time. This clashes with employees' right to privacy. Two important factors that drive an employer's need for personal information are health insurance and liability (Alderman & Kennedy 276). Employers worry about insuring people with health risks and being sued for negligent hiring. "Indeed, in some workplaces, such as day care centers, employers are required to check the background of their applicants," write the authors.

Employer's Right to Know?

Alderman and Kennedy discuss Soroka v. Dayton Hudson Corp. This case challenged and employer's use of psychological testing as a part of hiring practices. Sibi Soroka was an out of work actor living in San Francisco. While visiting a local Target department store, he ran into an old friend. Soroka told his friend how he was looking for work. His friend encouraged Soroka to apply for a position as a security guard. Soroka held a similar job while in college and enjoyed the work. Soroka had a first interview that consisted of standard paperwork and a short meeting with the Asset Manager. This was Target's

official name for their security division. Soroka was invited back for a second interview which, he was told, consisted of a test called the Psychscreen. This was a test given only to people applying for security positions. The test began with questions concerning his favorite part of the newspaper, if he enjoyed being with people, and other harmless topics. As Soroka continued, he believed the questions became less relevant to his job description. Alderman and Kennedy explain these irrelevant questions.

> They asked about the regularity of his bowel movements, about any homosexual urges he might harbor, about perverted sex acts he might practice or want to practice. The test also asked questions about his religious beliefs: whether he believed in the afterlife, his feeling about sins and sinners, and if he believed in the resurrection of Jesus Christ. (280)

After completing the test, Soroka managed to make a copy of it before he turned it into Target. Immediately, Soroka called the ACLU and started interviewing lawyers to take his case. Days later, Target offered Soroka a job and he started soon after. His employment at Target was short-lived. Soroka found a lawyer and he filed a lawsuit claiming that the Psychscreen had invaded his privacy and that of others who had taken the test (Alderman & Kennedy 281). Target claimed the rigid screening process existed to find the best people. Target used this to combat their greatest money losers: shoplifting and employee theft (281). Martin-McAllister, a testing company who created the Psychscreen, argued they were only looking for deviant behavior in the applicants. Karen Grabow of Martin-McAllister stated, "I would not expect to see the caliber of our whole workforce improve as a result of this test. What I would expect was that

we might identify lunatics and keep them out of our workforce." The authors write that this case was the first to seriously challenge a private company's use of psychological testing.

In October of 1991, the California Court of Appeals stated, "Any violation of the right to privacy must be justified by a compelling interest and must serve a job-related purpose" (287). While the case was in discussion, the court prohibited Target from administering the Psychscreen to others. Regarding the questions about religious and sexual matters, the court decided Target had failed to demonstrate a job-related purpose. Before a decision was rendered, Target decided they were better off settling the case out of court. Under terms of the settlement, Target agreed to discontinue use of the Psychscreen. Target also set aside $1,300,000 to be divided among the people who had taken the test. Soroka was pleased with the outcome and received the largest sum of $22,000. He stated,

> I would still like to be evaluated on my past record of performance. Not what I do on Sunday, not on what I do in the bedroom, not on what happened to me as a child. Whether you are a little guy or a CEO, job performance should be the key. (289)

Is Sexual Orientation Private?

Can an employer use a person's sexual orientation to determine job performance? In the case of Shahar v. Bowers, Alderman and Kennedy write that sometimes employers do have this right.

Robin Shahar graduated from Tufts University in 1986 with honors. She later was awarded a full academic scholarship to attend Emory Law School. Soon

after, Shahar met Francine Greenfield and the two fell in love. The authors write, "As their relationship developed, they bought a house together, got a couple of dogs, and settled down to pursue their respective careers." In Shahar's second year of law school, she took a summer job with Michael Bowers, the Attorney General of Georgia. Shahar eventually told some of her summer co-workers of her sexual orientation. This revelation did little to hurt her position with the attorney general's office. In her third year of law school, Shahar passed the Georgia Bar Exam and graduated sixth in her class. Soon after, Shahar was offered a full time position with the attorney general's office. Later that year, Shahar and her partner decided to have a marriage ceremony with friends, family, and a few of Shahar's coworkers in attendance. Days before Shahar was to start her new job, she received a letter stating that her job offer was being rescinded. The letter from Attorney General Bowers read,

> I regret to inform you that I must withdraw the State Law Department's offer of employment. This action has become necessary in light of information, which has only recently come to my attention relating to a purported marriage between you and another woman. As the chief legal officer of this state, inaction on my part would constitute tacit approval of this purported marriage and jeopardize the proper functioning of this office. (297)

Shahar was stunned with the news and contemplated a lawsuit against Bowers. Her firing seemed to be a prime example of how sexual orientation should have no bearing on job performance. Shahar was concerned her case would be a stepping stone to advance Bower's political career. Shahar

contemplated whether a jury would sympathize with an openly gay woman suing the Attorney General in a conservative state.

In 1982, Bowers had prosecuted the case Hardwick v. Georgia. Hardwick was charged with violating the state sodomy law when police found him in bed with a man. Georgia's sodomy law was like many others which defined sodomy as "any sexual act involving the sex organs of one person and the mouth or anus of another" (298). This charge carried a prison sentence of twenty years and applied to homosexuals and heterosexuals. Hardwick v. Georgia ultimately was decided by the Supreme Court. Alderman and Kennedy write, "In a 5 to 4 decision, the Court refused to recognize a fundamental right to engage in homosexual sodomy" (298).

After the Hardwick decision, gay rights activists decided that privacy was not the proper right to claim. Shahar claimed discrimination on the basis of her sexual orientation and religious choices. The authors write,

> The case became a rallying point not only for gay rights advocates but also for workplace privacy advocates concerned about employer's control over the off-duty behavior of their employees, whether it is sexual practices, religious affiliations, or recreational activities. (299)

Bowers denied that it was Shahar's religious beliefs that led to his decision. He believed her homosexual relationship would undermine his department's authority to uphold the laws of Georgia. The court agreed that Shahar's relationship was protected under the Constitution's right of intimate association. The court ultimately decided,

> The unique circumstances of this case show that Bowers' interest in the efficient operation of the Department outweigh Shahar's interest in her intimate association with her female partner. (302)

Judith Wagner DeCew, Associate Professor of Philosophy at Clark University, began her privacy research while at Harvard University. DeCew's book, In Pursuit of Privacy, is a study of law, ethics, and the rise of new technologies that threaten our privacy. The goal of DeCew's research is to provide a firmer philosophical foundation for future discussions of privacy doctrines in tort and constitutional law (7). I chose DeCew as a source because she discusses privacy from a different perspective. Her discussion of privacy and the ethical ramifications of privacy invasion are different than many sources that I researched. Most sources discussed privacy in terms of whether it violated Constitutional rights and little else. Her research of drug testing and new technology was a fresh look at privacy and the dangers of such abuses.

Workplace Drug Testing

According to DeCew, the use of illegal drugs and related health concerns has driven many organizations to implement mandatory drug testing (125). The perceived threat of the AIDS virus and the threat of being exposed to people with the disease are a concern. This perceived threat to public safety in many organizations takes precedent over privacy invasion. DeCew reasons that there are far greater issues at stake than public interest versus privacy rights. The questions that need to be justified are: what type of testing is being proposed,

what is being tested, who performs the tests, what are the goals of the tests, will the test curb the problem, what harm would result without the test, whether the tests are random or mandatory, and how will the test results be used? (126) DeCew writes,

> The crucial question is to determine when that balance provides adequate moral justification for the testing; that is, when privacy claims are determinative and when they may be legitimately overridden. (126)

DeCew believes there needs to be a balance between the employer's and the employee's rights. She opposes drug abuse in the workplace but cautions that testing not intrude on the employee's privacy rights. Current drug testing procedures exist to balance the need for testing with the privacy concerns of individuals. DeCew believes that to achieve this goal the current and future technology must be used with caution and on a selective basis (127).

DeCew's research claims government and private employers have a right to test for many reasons: to flush out drug users and curb drug use, to ensure the safety of employees, to fight the drug war, to reduce health care, and to maintain the integrity of their operations. While agreeing with many concerned parties, DeCew believes that it is unfair to force the non-users to pay the increased cost of healthcare caused by drug users.

The illegal sale of narcotics in the United States alone is an estimated $110 billion dollar industry yearly (DeCew 127). Researchers make a strong case of the direct correlation between narcotic sales and violent crimes committed. DeCew writes,

> In fact, studies showing that drug use is very much a characteristic of serious and violent offenders and that increasing or reducing the level of drug abuse is associated with a corresponding increase or reduction in criminality may have provided the earliest theoretical justification for initiating drug-testing programs. (127)

Besides crime issues, DeCew states, concerns associated with drug use include lost jobs, injuries, illness, and death .The economic loss associated with drug abuse, according to recent government studies, is between $60 and $100 billion. Many times, end results of drug abuse are tardiness, absenteeism, lost productivity, increased health insurance, and employee theft (DeCew 128).

To many companies, drug testing has been commonplace for many years. In 1986, President Reagan ordered random testing to those government employees that held "safety sensitive" positions. Drug testing in the public sector has also been used for screening applicants for many years. Studies conducted by the University of Michigan estimated 25 percent of Fortune 500 companies have drug-testing policies in place. The concern is how to administer the test without compromising privacy for the individuals.

Threats to Privacy

Despite the growing popularity of drug testing, many opponents believe the practice does more harm than good. Supreme Court Justice Antonin Scalia has called drug testing a "needless indignity." DeCew believes a main concern lies in the intrusiveness of the of drug test.

> If a blood test is used, it necessarily involves puncturing the skin. If a urinalysis is required, the sample must sometimes be gained under direct observation to guard against drug-free substitutions and falsification of results. (129)

The physical and psychological intrusions are not the only shortcomings associated with drug testing. Test results can reveal pregnancy, epilepsy, manic depression, diabetes, schizophrenia, AIDS, and many other bodily activities (DeCew 129). Once these results are known, questions concerning the assimilation, storage, use, and access to results are considerations. DeCew's concern is with who has access to test results and what guidelines exist in maintaining the confidentiality of the results. This disclosure of information can lead to embarrassment, discrimination, financial loss, and loss of employment (DeCew 130).

Another argument against testing is the belief that people should be free from employer control on non-working hours. DeCew supports this thinking only if the activities don't interfere with job-related functions. DeCew writes,

> Hence drug testing also threatens expressive privacy by intruding on one's body and behavior, making one fearful about one's choices of activities. (130)

Accuracy Concerns of Testing

DeCew believes that accuracy of testing is one of the downfalls associated with drug testing. The inaccuracy of the test is what constitutes the perceived threat to privacy. Many opponents of drug testing agree that considerable weight should be placed on privacy protection because of the high probability of error

(DeCew 131). Some forms of drug testing have been known to be wrong up to sixty percent of the time. A false positive is one testing error that indicates drug use when there has been none by the subject. These false positives can be caused by many medications and even the passive inhalation of marijuana smoke (DeCew 130).

Laboratories and the people administering the test are also cause for concern to privacy advocates. Human error and the limitations of technology can cause false positives. Many testing procedures use a threshold level to establish drug use. Threshold testing sets a level for drug use and any test that exceeds the set level causes a positive result. The downfall of threshold testing, according to DeCew, is that it doesn't differentiate between isolated incidents and drug abuse. The results don't tell if the subject was impaired at the time of the test or when the drug was used. Threshold testing fails to determine if and how much drug use impairs the individual (DeCew 131). She writes,

> There is general agreement in the scientific community that testing does not discriminate between drug use that impairs performance and drug use that does not impair performance. It does not even determine impairment at the time of test.

A positive test only reveals traces of the illegal substance in the body that would indicate prior use.

The most common drug test is urinalysis because it is less expensive and less intrusive to the individual. A shortcoming of urinalysis is that it is only designed to test for a certain drug or similar drugs. DeCew states that many positive urine tests have been obtained from people who have taken over-the-counter anti-

inflamatories like Advil, Motrin, and cold remedies, including Sudafed and Contac.

Many critics of urinalysis agree that testing fails to provide vital information concerning the amount of drugs ingested and behavioral effects to the individual (DeCew 132). Privacy advocates call for stricter testing methods and the guarantee that test results will be checked a second time. The cost to administer and the time required, a re-test is not seen as a viable option for employers. Drug users have also come up with tactics to defeat the testing procedures. DeCew states,

> Those who practice timed abstinence or who ingest large amounts of fluid can dilute the concentration of a drug in urine to below the cutoff amount. Adding salt, vinegar, bleach, liquid soap, blood, or other foreign substance can adulterate samples and produce false negative results that hide possible use. (133)

Is Testing Effective?

Many critics note that drug technicians are given little training in administering tests and interpreting the results. In DeCew's findings, private laboratories claim to have a 95 percent accuracy rate, although these same companies fail to support their claims with proof (DeCew 134). Many in the testing industry agree that blood testing is the most accurate way to test for illegal substances. Blood tests can measure performance of the individual better because concentrations in the blood are usually proportional to concentrations in the brain (DeCew 134). Another benefit of blood tests is that the threat of tampering is impossible because blood is drawn directly by lab personnel. The downfall of

blood testing, according to many employers, is the cost and time factors associated with this process.

DeCew's studies claim that many in the medical community believe that drug testing does little to cope with illegal use. Data to support employer's claims that refute the medical community are hard to find. Even after large workplace accidents committed by drug users, little data exist to support the claim that urine testing would have prevented the accident (DeCew 135). Data that can be supported are employee theft, absenteeism, and dismissal. DeCew writes,

> One critic has pointed out that for testing to be fully effective, every worker would have to be tested daily for every drug that might impair performance, the results would have to be available before he started work, and he would have to be under constant surveillance while at work to make sure he did not use a drug while working. (135)

The Courts Interpretation

The first drug testing case to reach the Supreme Court happened as recently as 1988. In National Treasury Employees Union v. Von Raab, the Court held that urine tests are a significant intrusion into a fundamentally private domain (DeCew 136). In cases that followed, the Court ruled that a blood test and urinalysis violate privacy rights found in the search and seizure section of the Fourth Amendment. DeCew writes,

> Courts routinely acknowledge that drug tests also violate the Fifth Amendment guarantee against self-incrimination, the Fourteenth Amendment protection of due process, and constitutional privacy interests protecting choice and bodily integrity. (136)

The Courts have opposed drug testing unless there is reasonable suspicion of drug use or the individual holds a safety-sensitive position (DeCew 137). Safety-sensitive can be defined as anyone in law enforcement or who has access to classified materials detrimental to an organization. DeCew emphasizes that the Court has failed to tackle the important issues of drug testing.

> Many Courts have refused to address the issue of testing error, have avoided discussions of the implications of false positives and false negatives, and have underemphasized the physical bodily intrusion related to constitutional privacy concerns surrounding control over one's body, as well as worries about social control over behavior off the job. (DeCew 137)

Many of the Court's decisions have no bearing on the private sector where most private drug-testing programs have avoided legal challenges. DeCew also notes that little legislation exists at the state level to protect employee rights. Those private companies that fail to address privacy concerns could face the risk of increased litigation by employees (DeCew 138).

Recommendations

For drug testing to be effective, DeCew believes that federal guidelines should be in place to back up sanctions with violations. Test results should combine with follow-up assessments of employee performance to determine job eligibility (142). In DeCew's plan, an employee should only be tested when there is reasonable suspicion of drug use. Factors to support the test could be unexplained

attitude change, perceived impairment, or decreased output of job functions. She writes,

> When reasonable suspicion is required before testing, the program is less vulnerable to constitutional attack, and supervisors are forced to oversee more rigorously the performance of those in their charge. (142)

DeCew recommends that all drug-testing plans be explained to employees in writing stating the procedures and consequences of a positive test. Employees who test positive should have the right to explain the test results and have the right to be re-tested for validity. The final step, according to DeCew, is to create strict guidelines to protect the confidentiality of the test results. She warns the growth of computer databases makes this goal almost impossible to enforce. Test results collected should not be used for any purpose not originally communicated and should not be released to anyone but the tested individual. DeCew states,

> My goal has been to strike a balance between the very real and numerous privacy intrusions involved in drug testing and the need to protect public safety when drug abuse is a substantial threat. Mass testing without suspicion is intrusive, inefficient, often inaccurate, and a waste of resources. (144)

Rounding out the literature review is The Limits of Privacy by Amitai Etzioni. Previously he has taught at the prestigious institutions of Harvard and Columbia University. He is currently a professor at George Washington University. He is the author of eleven books, many dealing with societal concerns such as the economy, political corruption, political processes, and organizational structures. Etzioni also served his country as a political figure when he was a senior advisor to the White House during the Carter Administration. He brings a unique

perspective because of his previous political background and his current status as a private citizen. He presents the arguments of those both for and against privacy reform.

Etzioni's book questions topics such as: Under which moral, legal, and social conditions should this right to privacy be curbed? What are the harms that befall us when we do not allow privacy to be compromised (3)? Etzioni decided to write this book after he read a 1996 Harris/Equifax poll of more than a 1,000 Americans. This poll found that nearly eighty percent of Americans were somewhat or very concerned about privacy issues.

Identification Cards and Biometric Identifiers

A national identification card is one of the hotly debated topics concerning privacy reform. One form of the ID card would contain the person's name, age, address, and any other distinguishable information. The ID card is so feared by opponents that the discussion of its merits is not even considered. The proponents of the ID card are usually vilified almost immediately at the mention of this subject (Etzioni 103). The discussion usually begins in a subtle manner concerning ways to track criminals, deter credit card fraud, enforce child support for parents, and monitor illegal aliens. Etzioni writes that ID cards and identifiers are standard practice for many European countries. The Europeans don't even talk about the subject because it is a non-issue to them. Etzioni writes, "Do the benefits to public safety and other public goals of ID cards or biometrics outweigh the cost to privacy?" (104)

Forgotten Cost

Etzioni has named several areas where cost to the public could be reduced if identifiers existed in the United States. Each year there are over half a million criminal fugitives that avoid incarceration or fail to serve their full sentence. Many times these individuals commit more crimes while loose. Etzioni writes,

> Fugitive criminals also contribute to Americans' fears about crime and to the loss of public confidence in the law enforcement caused by the success of notorious fugitives in maintaining their covert status. (105)

With a national ID card that tracked criminals, Etzioni states this number could be reduced and a restored confidence in law enforcement.

Sex Offenders

The taboo subject of child molestation is finally receiving the attention it deserves. Etzioni writes that in 1990, six states identified more that 6,200 people convicted of criminal offenses including sex offenses, child abuse, violent crimes, and drug charges attempted to acquire jobs as child care providers. One reason these criminals infiltrate the lives of youth is the lack of information needed to screen applicants thoroughly. Even if background checks are done many criminals escape detection because they use fake identification. The September 13, 1999, issue of Sports Illustrated ran a cover story on child molestation in youth sports. Their research found that the average molester, the kind most common in youth sports, victimizes about 120 children before they are caught

(43). Etzioni believes a national ID or biometric identifier would keep criminals in check. He writes,

> A report by the state of California to a U.S. Senate hearing concerning the National Child Protection Act revealed that in a single day in 1991 a convicted murderer, a convicted rapist out of jail for fifteen months, and a convicted drug dealer all applied for jobs caring for children. (105)

Identity Theft

Identity theft, according to Etzioni is the misuse of personal identifying information used to commit various types of financial fraud (109). Identity thieves usually start with acquiring someone's Social Security number, which allows them to get credit cards, driver's licenses, bank loans, and to file false tax returns. Some criminals commit crimes and pass the blame onto their unsuspecting victims. In 1997, the General Accounting Office estimated that identity thieves stole at least $750 million (109). The Internal Revenue Service reports that an even more disturbing amount of money is lost due to identity theft. It is believed that $1 billion to $5 billion per year are lost due to people who fraudulently file for multiple refunds using false identities. In most cases, the victims of identity theft are left with a shattered financial record and little recourse to help their cause.

Child Support

Many separated parents escape financial responsibilities for their children when they move or change jobs. Etzioni believes the outstanding debt owed to

children could be greatly reduced if there were better ways to track non-paying parents (106). Etzioni writes, "In 1992 Senator Joseph Biden testified before a Senate subcommittee that 16 million children in America today are owed $18 billion in back child support payments" (106). As recently as 1994, Etzioni reports that 18.6 million cases of non-paying child support parents were reported.

Gun Control

The growing number of shootings in our school systems has many demanding tighter gun control. Limitations in current legislation make it difficult to keep felons from obtaining guns. The inability to pinpoint felons because of false identifications renders current gun buying procedures useless (106). Former Senator Richard Velde stated before Congress, "Without physical or biometric verification of identity the Brady check is only as good as the paper that is presented to the dealer" (106). Current checks rely heavily on the accuracy of information that is given to law enforcement officials. If the buyer information is false, nothing stops criminals from obtaining guns in a legal manner. Etzioni writes,

> A twenty-three year old man was rejected by a gun store for having an expired driver's license when he tried to purchase two semi-automatic weapons for two juveniles; he left the store, bought a fake Colorado ID card for $3.50, returned two hours later, and bought the guns. A week later one of the weapons was used to murder an out-of-state tourist during a robbery attempt. (107)

Illegal Citizens

Etzioni also points out the growing concern of illegal aliens living in the United States. Recent estimates state there are between 4 million and 8 million illegal aliens living in the United States. These aliens collect an estimated $18 billion in government benefits by using fake identifications (Etzioni 107). These people can account for as much as 12 percent of the population growth in the United States. Once again, the inability to effectively track certain people may lead to an increase in crime rates. The inability of deserving Americans to secure employment because illegal aliens take jobs is another reason for tighter identification procedures. Robert Kuttner states in Etzioni's book,

> Hard-won benefits to American workers, minimum wage, the eight hour work day, pensions are undermined by the enormous underground economy created by employed illegal immigrants, who often work longer hours for lower pay than most legal American residents and citizens will tolerate. (108)

Public Response to National Identifier

It is widely believed that many Americans don't fear a national identifier as once was believed. Little protest ensued when airlines mandated that valid identification be shown in order to board planes after the TWA Flight 800 disaster. Etzioni believes that the driver's license and Social Security number have become de facto identifiers already. He writes,

> We are routinely asked to identify ourselves by producing a drivers license when we want to pay for a transaction with a personal

> check, purchase alcohol, obtain credit, apply for a public library card, secure government services, or rent an apartment. (118)

The main problem with relying on these de facto identifiers, according to Etzioni, is the need for this information to be linked to a central database. This database would contain extensive information about the individual. Currently, a routine check of someone's Social Security number would fail to reveal if the police wanted someone, owed child support, or was an illegal alien (Etzioni 118). It is inevitable that private and government databanks will merge information to create a clear, concise picture of an individual.

Most objections to a national identifier have come from libertarians and civil libertarians. They believe that national identifiers are not what the Constitution grants us as free individuals. The Cato Institute comments, "The history of government programs indicates that privacy rights are violated routinely whenever expediency dictates" (120). The ACLU believes problems may arise when government and corporate databases share information. Personal traits like unlisted phone numbers, medical history, voting information, and credit histories could be accessed without a person's awareness. Senator Alan Cranston of California warns,

> Don't we remember the Nazi experience in Europe, where identity documents listing religion and ethnic background facilitated the roundup of Jews? Don't we realize the dangers of allowing Government to establish identity and legitimacy? Isn't it, in fact the responsibility of the citizenry to establish the legitimacy of Government? (121)

Many groups, including the ACLU, believe the creation of a national ID may cause a society of outcasts. Those who refuse to use the ID will be forced out of society (Etzioni 123). These groups believe a 1990 study done by the GAO that poled employers and asked them if they had discriminated in hiring practices. Many employers admitted they discriminated against some applicants that looked or sounded foreign. Etzioni believes that universal identifiers may help to eliminate discrimination practices. All job applicants, including people who look or sounded foreign, would have proper identification to prove their citizenship. Studies show that a majority of legal immigrants are in favor of national identifiers to distinguish them from illegal immigrants (Etzioni 132).

National Identifiers: Nothing New to the Rest of the World

Etzioni reports that national identifiers are common in many European countries. These identification systems have been in place for many years in Germany, Spain, Greece, Belgium, and Portugal without hurting personal freedom (126). It has become automatic for Europeans to carry a card with their picture, date of birth, address, and passport information. A British citizen speaks of his experience with a national identifier,

> For nine years I have lived in societies which have required me to carry their own identification papers. ID cards ensure a swift passage through immigration, facilitate bank transactions, produce registered mail from behind post office counters, and smooth relationships with the taxman. ID's offer evidence of legal entry and authorized residence, and satisfy policemen who use spot checks to discriminate against criminals, drug traffickers, and illegal immigrants. (127)

Etzioni found research on this subject difficult to uncover because no one writes on the subject. The ID is accepted and understood in European countries. Etzioni believes that Libertarians' concern over the National Identifier is unfound. He believes that totalitarian governments come to power because of breakdowns in social order. When society fails to respond to social concerns is when people call for stronger government control to bring order (127). Etzioni writes, "By helping to sustain law and order, universal identifiers may thus play a role in curbing the type of breakdown in social order that can lead to totalitarianism" (127).

Chapter IV

PERSONAL EXPERIENCES AND INTERVIEWS

Personal Experiences

My interest in privacy reform started a little over a year ago. I was in the final stages of closing on my first home. To secure the mortgage, I had my parents co-sign on the home. It was a very exciting and stressful time in my life. I found the whole home buying experience to be exhausting. I was amazed at how much information my parents and I had to reveal to credit bureaus, lenders, real estate agents, and title companies. I bet we signed our names on a hundred different documents. What I soon came to realize was that every time my parents and I gave personal information about ourselves, we were compromising our privacy.

Not long after closing on my home the flood of junk mail and phone calls began. My parents started receiving mail to my address because they had cosigned on my loan. Solicitations for roofing, siding, windows, landscaping, furniture, bottled water, and security systems filled my mailbox. A popular piece of junk mail that I currently receive is the pre-approved application for credit cards and loans.

My listed phone number has also been a source of privacy invasion. I made the mistake of having my number listed in the phone book and caller assistance. On previous occasions when I signed up for phone service, I never thought I needed an unlisted number. The calls begin around 11:00 A.M. and continue until 9:00 P.M. The phone calls come from many of the same companies that are

sending me the junk mail. My parents were also very popular with the telemarketers until callers finally figured out my parents don't even live in St. Louis.

After I started research for this project, I began to chart the number of unwanted calls that I received in the evening. I decided to have my brother, who is also my roommate, help log these calls. I placed a note pad and pen by every phone in my house. Each unwanted call received a hash mark. I performed this study for a period of two weeks. For this two-week period, I received, on the average, of five to seven unwanted calls per evening. I began to tell the callers that I wanted my name taken off their call list. This tactic did little to stop the flood of bothersome calls. On a few occasions, I even told the callers that asked for Darren Bax that he had recently been killed in a car accident. The callers were so caught off-guard that they said nothing and hung up the phone. Enough was enough and I finally called the phone company to get an unlisted number. Nothing could be done about my number being in the printed phone directories that were in distribution, but my name and number were now out of caller assistance. I knew that until the printed directories were out of circulation, the calls would not completely stop.

While in college, I had a job where I did telemarketing for a company selling circus tickets. Our method of getting individual's phone numbers was very simple. We just opened the phone book and went right down the page. There was nothing scientific about the process and I knew many of my callers were doing the same thing. To my surprise, the phone company told me that I would

be charged one dollar extra each month to have an unlisted phone number. Apparently, it is a big hassle to take someone's name and number out of their database.

As a way to supplement my income, I buy and sell used cars. I have a friend of mine purchase the cars at the wholesale auto auction in Kansas City, Missouri. I normally drive the car for a few months and sell it through the newspaper. Since I keep the car for a while, I have to license and title the car in my name. A few weeks after my monthly trip to the department of motor vehicles, I receive mail from car dealerships that sell my type of car. The dealers know the make, model, and year of my current automobile. In their letters, they let me know about any specials like oil changes, checkups, and detailing. Someone was giving this information to these businesses without our knowledge. Last year when I went to renew my driver's license, the attendant asked if I wanted my personal information kept private. I told her that yes; I did not want any of my personal information sold to organizations.

My family members reported similar experiences. After a trip to the department of motor vehicles for license renewal, my sister started receiving Victoria's Secret magazine. My mother receives literature and enrollment forms from Weight Watcher's. My father, who is an avid outdoorsman, now receives Field and Stream magazine because he purchases hunting and fishing license. Much of they junk mail they now receive can be attributed to vehicle records. I have come to the conclusion that whenever I release my personal information, the

phone calls and junk mail multiply like the story of the loaves and fishes in the Bible.

I recently received a piece of mail from St. Louis Acura. The letter was congratulating me on the purchase of a new Honda. They were sending me coupons for service on my new Honda. Yes, St. Louis Acura was correct in sending me the letter because in fact I did recently purchase a new car. I wondered how they had received this personal information. I called the service manager for an explanation. Before I interrogated, the man I told him that I was doing research on the subject of privacy. Ron Ribolzi stated the information is purchased on a monthly basis from the Department of Revenue. This list is called the Cross-Sell and it contains the car's year, make, and model. Most attractive to the car dealership is the owner's name and address. Ribolzi defended the list by stating the information helps his company serve the public.

Presently, St. Louis Acura is in no violation for the use of this personal information. The state of Missouri gladly sells this personal information to anyone who wishes to pay.

Privacy Compromised

Last year when I moved into my new home, I had to purchase a washer and dryer. Best Buy was running a promotion for six months interest-free financing. To be eligible for this promotion, I had to get a Best buy credit card. The card gave me buying privileges at any Best Buy store in the country. A few months later, I paid the balance on the washer and dryer. In April of 1999, I received an

invoice from Best Buy for $335. The only purchase I had made with the Best Buy card was for the washer and dryer. Somehow, someone had obtained a copy of my account number and had another card made. I called their customer service department and found them to be less than sympathetic. I told them I had not used the card in several months and it must be a mistake. The representative told me I had to write to their claims department for further help. I wrote a letter stating that I did not make the purchases. I asked Best Buy to manifest a copy of the credit card receipt. The copy that was given to me indicated someone had made the purchase in Houston, Texas. The imposter had not even bothered to sign my name to the receipt. Even with this evidence, Best Buy was reluctant to take the charges from my account. I wrote a second letter stating that I had never been to Houston, Texas and the signature was not mine. A third letter was written to state that I would not pay the charges and would never shop there again. Since this incident, I always check the accuracy of statements and properly discard ones with account numbers shown.

Interview with State Rep. Rich Chrismer

I recently had the opportunity to talk to Missouri State Representative Rich Chrismer of St. Peters. I first became aware of Mr. Chrismer when I read an article in the Jefferson City News Tribune in February, 1999. Chrismer was supporting a bill that would make it illegal to require fingerprints, retina scans, voiceprints, or DNA tests as a condition of employment or doing business (AP 5). The bill was created because of the increasing number of businesses that are

asking for a thumbprint when writing a personal check. Chrismer and other proponents of the bill are also worried because DNA tests can show who has a high potential for certain diseases. Chrismer asserts,

> I understand where the businesses are coming from. They want to protect themselves from people bouncing bad checks. But evidently with a thumbprint, these businesses can get a lot of information that they don't need.

I asked Chrismer if he thought that privacy reform was needed at the federal level of government. He believes that there are enough laws on the books that are not being enforced. Using these laws or getting rid of them is needed before more legislation is written. Chrismer, a Republican since 1978, had little trouble expressing his dissatisfaction with the Clinton Administration. Chrismer said, "The Clinton Administration would like more legislation. When you see more legislation, a lot of times that's to let someone in on your private life." Chrismer is also an avid believer in "government by the people, for the people." He believes that people have come to blindly recognize the government as a mysterious godfather who will take care of them. He states,

> This particular administration believes that government can do best for everyone. We need to take care of ourselves because we are the government. It may sound harsh but this man may be the best politician I have ever seen but he is no servant of the people. He would really want to take away people's privacy because he really believes that government is best.

I asked Chrismer to comment on the groups who believe privacy is not protected by the constitution. Chrismer made his stand on the ongoing issue

abundantly clear. He stated he is a pro-life activist and feels strongly on the issue. He noted that in Roe v. Wade, the Supreme Court found a right to privacy in the Preamble to the Constitution. Chrismer stated,

> I think the Supreme Court justices were stretching to find a right to privacy. If anyone tells me the right to abortion is constitutional. No! It was the opinion of seven men.

He believes the right to privacy exists in the Constitution by granting us life, liberty, and the pursuit of happiness. "That is as close to a right to privacy as you will find in any document the founding fathers came across," said Chrisner.

I asked Chrismer how Missouri ranked among other states trying to pass legislation for and against privacy reform. I was shocked to discover that Missouri is one state, according to Chrismer, that is always trying to diminish privacy. He believes this has come to pass because the Democrats have controlled the Missouri legislature since 1945. He stated,

> The way you hold onto power is you make sure people are dependent on government. In the last seven years, I have seen our legislators propose legislation to get into our pockets.

I was curious to find out what, if anything, Missouri is doing to inform the public of their privacy rights. "Absolutely nothing, they are not assisting the people of our state in any way, shape, or form," asserted Chrismer.

I ended our conversation by asking Chrismer what citizens can do to protect their privacy. He became very animated when I posed this question. He states,

> If you think flashing a $500 dollar bill will attract attention. Your personal information is just as valuable. If you tell one person, you have just told a thousand.

Interview with Denise Lieberman of the ACLU

Throughout this research, the American Civil Liberties Union has been a source that I have used extensively. I knew that interviewing to someone from the ACLU would be an important asset in my studies. I contacted Denise Lieberman of the local chapter of the ACLU. Lieberman is Legal Director for the ACLU of Eastern Missouri. She recently joined the ACLU after starting her career in the private sector. She grew up in a family that was politically active and involved in the civil rights movement.

Creating public awareness concerning the rights of citizens is a primary task of the ACLU. This push for privacy awareness begins with the distribution of literature, helping companies write policy, filing suits, and writing letters to privacy abusers. Much work is done at the state and national level of legislature. The ACLU branch of Eastern Missouri employs a full-time lobbyist in Jefferson City to support privacy reform. The ACLU is a private organization so it receives no government funding and is supported entirely by memberships and private donations.

Our conversation began with the question of her definition of privacy. She mentioned that was a very broad question to answer because privacy could cover many areas, "The right to be left alone." Lieberman stated that the ACLU handles a variety of cases, including bodily integrity, privacy of documents, and the

protection of Social Security numbers from government organizations. She stated,

> Every form, from jury service to checking out library books, often ask people to disclose their Social Security number without making the required disclosures.

Government organizations are required to explain how they will use this personal information. Lieberman noted that the ACLU has been very successful in getting government agencies to change certain forms. A government form that the ACLU has targeted as an abuser of personal information is the voter registration form. According to Lieberman, this form requires a spouse's name, mother's maiden name, occupation, and employer.

In October of 1999, Lieberman and the ACLU wrote the City of Affton, Missouri Fire Protection District for perceived privacy violations. Lieberman had received reports from concerned individuals regarding the fire district's employment applications. In a letter to Assistant Chief Buehne of the Affton Fire Protection District, Lieberman wrote,

> Courts have recognized that government employers have a valid interest in knowing a good deal about the people it hires, and can question applicants on many aspects of their lives. However, there are important limits on the extent to which agencies can probe into the private lives of their applicants.

Many of the questions in this form inquire about the political affiliations of the applicants. These types of questions are specifically protected by the First Amendment. The Affton Fire Protection district questionnaire asks,

1. List all civic or social organizations, fraternities, clubs, or groups of which you are or have been a member or associate. Also furnish its location.
2. Are you now or have you ever been a member of any activist group (refers to KKK, Communist Party, and Black Panthers)?
3. Have you ever participated in any demonstration, strike sponsored by any group or organization?

Even more troubling were the evasive questions regarding the spouse of the applicant. The questionnaire wanted to know what the spouse thought of their mate becoming a fire fighter. It asked the applicant what they thought of their in-laws and whether they got along. The fire district wanted the full names of the spouse's immediate family, including their address, occupation, and date of birth. Financial records of the applicant were also requested, including account numbers. Lieberman wrote,

> Only information that is reasonably necessary to make a determination about the applicant's fitness for the particular job can be sought. There must exist a rational relationship between the questions and the nature of the employment. Moreover, inquiries into applicant's participation in political activities are prohibited by the First Amendment.

Lieberman has offered her services to the Affton Fire Protection District to review and revise their current employment application.

Lieberman noted that a new area of concern for the ACLU is the administering of DNA tests to law offenders. This bill would allow law enforcement to take DNA samples of certain offenders for possible future use. Problems with the bill, according to Lieberman, include the pettiness of some offenses where DNA could be taken from the offender. She stated that someone

who is convicted of filing a false report of elder abuse is subject to DNA removal. Lieberman said,

> The state of Missouri doesn't have any regulations accompanying it. Most states have regulations that modify or explain the boundaries of the statute. The statute also allows that state to collect the sample by using force if necessary.

Many clients of the ACLU are worried how a DNA test could effect their children and grandchildren. Any genetic predisposition for disease will be discovered in their DNA and this information may stigmatize their offspring. The concern of the ACLU is how this DNA file will be used and stored. If used improperly, the DNA file of an offender could cause discrimination against an innocent family member.

When asked what Lieberman would say to the person, who believes privacy is not guaranteed by the Constitution because it's not explicitly mentioned, she stated:

> There are two schools of thought on the privacy issue. One is the strict constructionist kind of approach like a Justice Scalia who reads the Constitution to govern things explicitly mentioned. Bowers and Roe were the two cases that really brought the issue to the forefront. In those cases, the court said the notion of privacy, although not explicitly stated in the Constitution, is in the penumbra of the Fourteenth Amendment.

Lieberman believes the "notion of privacy" is found throughout the Constitution. Not found in any particular amendment, privacy can be said to apply to many instances the Framers of the Constitution never envisioned. According to Lieberman, the Constitution is not a comprehensive document that covers all

aspects of society. The Constitution can be taken and applied to many situations where interpretation is needed.

Lieberman believes DNA testing, wiretaps, and the illegal use of database information are some instances where the government abuses privacy. She stated, "That's today's equivalent of the soldiers busting in your door and going through your papers."

Drug testing in the workplace is also a concern for Lieberman and the ACLU. The ACLU believes obtaining the sample can be degrading because observation is required by the testing facility. The lab procedure is the second invasion of the employee's privacy. In addition, the test reveals much more than the presence of illegal substances. The identification of pregnancy and genetic predisposition to certain diseases are primary concerns of the ACLU. Although testing for pregnancy is illegal, in 1988 the Washington D.C. Police Department openly admitted it used urine samples to test female employees for pregnancy (ACLU). The screening for pregnancy was done without the consent of the individuals. Human error and the inability to differentiate between illegal and legal drugs often cause several false positive test results (ACLU 1). The ACLU writes,

> In 1992, an estimated 22 million tests were administered. If five percent yielded false positive results (a conservative estimate of false positive rates) that means 1.1 million people could have been fired, or denied jobs – because of a mistake. (ACLU 1)

Lieberman believes that drug testing is a way of making judgements about people because of activities in which they engage in while not at work. This harsh judgement could hurt employees for activities they engaged in years before.

If the employee has been drug free for several years, how does a positive drug screen assess their current job performance?

The Tin Drum

In 1997, several Oklahoma City, Oklahoma residents claimed The Tin Drum, the 1979 Oscar-winning German film, violated state obscenity laws and was, in fact, contraband (Romano 1). The scene in question is of a young boy engaging in oral sex with a teen-age girl. Bob Anderson, Director of Oklahomans for Children and Families, heard a radio announcer state the film could be considered pornographic. Within three days and before even viewing the film himself, Anderson had gotten a judge to rule the film violated state obscenity laws.

What transpired in the following days was nothing but numbing to personal privacy. Police raided several Blockbuster Video stores and seized all remaining copies of The Tin Drum. Even more alarming, the police wanted to know all the people who had a copy in their possession. Michael Camfield, Director of Development for the state ACLU, had picked up a copy from Blockbuster when he heard of Anderson's crusade. Shortly after, three police officers came to Camfield's home and demanded the tape. Camfield obliged and then filed a complaint with the ACLU. Camfield claims that Blockbuster gave his name and address to the police. Camfield and the ACLU maintain that Blockbuster and the police violated the Video Protection Act of 1988. The act states, "it is a violation of federal law to acquire the records of a customer at a video store without a court order or search warrant." Michael Salem, an ACLU attorney remarked, "No one

disputes that child pornography is evil, but we cannot turn our cultural decisions over to people who would put a fig leaf in front of a Michelangelo statue."

On October 21, 1998, the U.S. District Court for the Western District of Oklahoma ruled on the case of Camfield v. the City of Oklahoma City. The ACLU wrote, "A federal court ruled that The Tin Drum is not child pornography and therefore may not be subject to criminal penalties imposed by Oklahoma's child pornography law." To date, this is the last ruling on the case. However, several issues still remain, such as prior restraint, unreasonable seizure, due process of law, and whether the seizure was a violation of a federal privacy statute (ACLU 1). "I'm thrilled that The Tim Drum has been exonerated of the child pornography label attached to it by potential censors, " Camfield said. "Although this ruling is a victory, we definitely have more work ahead of us."

Book Flagging?

In the recent motion pictures Seven and Enemy of the State, references are made to a term called book flagging. In both movies, law enforcement is able to access library records to find out who had checked out certain books. The question of whether book flagging really happened was an issue I resolved by calling the St. Louis Public Library. Dan Wilson, Director of Library Services, shed some light on this ominous notion. Wilson stated that a form of book flagging does indeed take place. He stated that the FBI has been using the library system as a source to track suspicious persons for several years. To ascertain the information, the FBI has to have a court order to search individual library records.

Most electronic library databases allow one to retrieve the list of books that a person has checked out. To do this, according to Wilson, one must have the name of the person. A search of a particular book will not inform one of the individuals who have checked the book out. No history is maintained from book to person. Missouri law prohibits public libraries from disclosing this type of information.

My firsthand experience with privacy loss was the motivation behind this research project. Little does one know that every time a warranty card, sweepstakes, or credit application is filled out privacy is endangered. The mounting junk mail and incessant nightly calls led to a realization that one must take charge of their personal information. Calling on experts in the field gave the researcher a perspective on the problem, possible solutions, and hope for positive changes.

Chapter V

INTERPRETATION AND RESULTS

The issue of privacy confronts humans from birth until death. By the age of two, Americans are required to obtain a social security number. In grade school, children receive their first library card requiring their name, address, and phone number. When teenagers apply for their first driver's license it marks the beginning of the end to real privacy. That small card contains enough information to cause organizations to pay large sums of money to secure its contents. Once this process begins, it is almost impossible to reclaim this information. When a child starts his first after-school job, the Social Security number begins to build a dossier on that child. Once college begins, for many, their social security number takes on a new role in their lives. It now becomes their school identifier as a way to track attendance, grades, meal programs, housing arrangements, and financial aid account information.

In college, young people are bombarded with pre-approved credit card applications. Armed with the student's social security number, the company adds to the growing dossier. This personal information is now sold to another company, who does the same. Stopping the flow of personal information is like trying to stop a moving train; it doesn't happen easily.

Government Legislation

The United States government has been trying unsuccessfully for years, to create a national identifier. The time has arrived for one, true, identifier to be

used by the United States. National identifiers have been in use for many years in Europe. The majority of Europeans believe the identifier has been a great benefit. All their government transactions are processed efficiently and in a timely manner. Armed with biometric information, it would take identifiers to another dimension.

No longer would individuals be able to impersonate someone for the purpose of committing fraud. The biometric identifier would curb the mass influx of illegal aliens into the United States. True citizens and welcome guests would have nothing to fear. In turn, the biometric identifier would hinder employers from hiring illegal aliens at lower wages. Criminals hiding from the authorities would be very fearful of a biometric identifier. No longer would they be able to impersonate others. Any time they went to cash a check, obtain a loan, or go to the doctor, they would have to prove their identity. Criminals, illegal aliens, and people who fear being recognized are the ones who oppose any form of identifier (Russos 5).

Even with a biometric identifier, many questions surrounding the management of this information remain. What organization would be responsible for assimilating the biometric data? Would this be a government-appointed organization or a private company contracted by the government? For Americans to agree on the usefulness of a biometric identifier, this private information must be protected from outside organizations. This valuable information must not be sold to direct marketers and companies who will invade our privacy (Brin 3).

If, and until biometric identifiers are used in the United States, reform is needed to secure privacy. One priority is the immediate removal of the social security number as the national identifier. Originally, the social security number was created to track workers' contributions to the program. Since its inception, the Social Security number has been used for over forty congressional functions not associated with the original program (Paul 1). People need to be educated on the dangers associated with allowing a social security number to be known. The mere knowledge of this number could allow someone to obtain a social security card, driver's license, credit card, loans, buy a car, and commit a crime while impersonating someone.

According to the ACLU, the Clinton Administration, with the aid of the Federal Communications Commission, has been a major supporter of privacy invasion tactics. Recently, presidential legislation has focused on adding surveillance devices to home and mobile phones. The purpose is to allow law enforcement the opportunity to track criminal or suspicious activity.

A similar plight exists regarding the design of software products. The Clinton Administration is requesting that all encryption software have a back door for law enforcement if needed. This type of government surveillance poses a greater threat to individual privacy than a national identifier. Problems exist as to who determines when surveillance tactics are used? If and when this technology is being used, will law enforcement need a court order to activate the tracking of backdoor encryption devices? Enough technology is already in place that allows

law enforcement to track individuals. This type of damaging legislation that calls for increased surveillance tactics must be stopped (ACLU 1).

Work Place Privacy

Monitoring of an employee's performance is nothing new in today's society. The monitoring of employee phone usage has been standard practice in organizations for decades.

Employees should be guaranteed limited privacy while at work. According to Joseph Garber of Forbes, American companies spent over a half a trillion dollars in computer-related products and training in 1998 (Garber 297). Employers have a right to make sure they are getting a return on their investment.

If organizations are going to monitor employees, they should make this known. Any employee is less likely to break rules if they know someone may be watching. The threat of being caught is just as effective as the punishment. Those who oppose any form of employee monitoring are the unproductive ones. With the aid of monitoring software, keeping tabs on an employee's productivity is simplified. Even without monitoring tactics, productivity can be measured in other ways.

Workplace Drug Testing

I agree that drug testing in the workplace is a privacy violation. I oppose the testing, not because I am in favor of drug use in the workplace, but because of the inaccuracy of the test. Employers do have a right to a drug-free environment, but

many fail to state the true goal of testing. A main stumbling block associated with drug testing is that current techniques can't detect impairment at the time of the test. In reality, all that drug testing reveals is that substances have been taken in the past. Should a possible or current employee be held responsible for taking illegal substances years past or on their own time? Even if a positive test is revealed, this does not determine job performance. A current or former drug user may be the model employee; although research does indicate a direct correlation between drug use and illness, tardiness, theft, increased health insurance, and lost productivity. Even the non-users suffer from standard drug testing procedures. The non-user is forced to pay the rising cost of healthcare caused by the habitual users.

The disturbing aspect of drug testing is the vast amount of bodily information that can be ascertained. Through a simple urine test, employers can discover AIDS, pregnancy, epilepsy, manic depression, and predisposition to other illnesses. An employer, armed with our genetic makeup, could decide it might be too expensive to hire or retain someone with cancer or depression in their family history in their workplace. Just because a predisposition for a disease exists, does not mean the disease will materialize. The drug test that employees take today could be used to prejudge their children years later. The genetic predisposition for certain diseases that offspring possess could prejudice them even without their taking of a drug test.

In all reality, drug testing in the workplace is not going to end. So with that in mind, the goal should be to strengthen the procedures in place. Historically,

the courts have opposed drug testing unless there is reasonable suspicion of drug use or the individual holds a safety sensitive position (DeCew 137). Safety sensitive could be defined as law enforcement official, doctor, nurse, or anyone with the lives of others in their control. All drug testing procedures and consequences of a positive test should be explained to employees. If overall job performance suffers, then a test may be administered. Judith Wagner DeCew believes when a test is given, after probable cause exists, the employer protects himself or herself from constitutional attacks (138).

If a positive test is revealed, the employee should be given the right to refute the findings if he so wishes. Lists of possible substances that may be causing the false positive are reviewed. The suspected employee should then be allowed a second test. If a second test reveals the same and the employee is unable to explain the results, employer discretion is advised. The employer must decide if this person is valuable enough to the organization to retain. This line of thinking is used in the world of professional sports almost on a daily basis. Sports figures are testing positive for drug use at an alarming rate. They are usually suspended for a period of time, forced into a drug treatment facility, and then allowed to have their jobs back. In many cases, the athletes that are caught usually get caught again, and again, and again. What separates the nine-to-five employee who uses from the world class athlete who uses? It is reasonable to assume that both classes of users could have an explained attitude change, perceived impairment, or decreased output of job functions. The difference is that the athletes get warned and everyone else loses their jobs.

Even a greater threat to individual privacy caused by drug testing is the information that exists. The confidentiality of the results should be taken into consideration. If an employee tests positive, and if hey is retained, the results should be kept by the employer for as long as the individual is employed. Positive tests from possible or current employees not retained should be destroyed immediately. DeCew believes, however, that the growing number of databases it makes the deletion of test results impossible.

Internet Reform

In this ever-growing computer aided world, the Internet is vital to our society. The term e-commerce is the new buzzword in the business community. Companies and individuals want the freedom to sit at their computer and shop for goods and services without the pressure from outside sources. For the Christmas season of 1999, economists state that retail business was down but e-commerce was booming. If one is concerned about transmitting personal information to a business via the Internet, the company's policy statement should be consulted. Almost every reputable site will provide a privacy statement. This statement explains how your personal information will be treated. If one has reservations concerning a policy statement, no one is forcing people to use certain Internet sites. The thought of not utilizing the Internet is becoming less likely in the rapidly growing Internet-reliant world. Stephan Manes of PC World writes, "Here as elsewhere, the Internet is merely an extension of the rest of life, where

privacy has become a casualty of a capitalist paradise where we trade personal information for cash, convenience, and goodies" (316).

Computer users concerned about their privacy while using the Internet should be aware of cookies. Joshua Quittner of Time Magazine describes a cookie as a means by which Internet users tell what sites they have browsed. When a user logs on a particular site, the web page records the time spent on that page and what information was important to the person. Quittner wrote, "By the mere act of "browsing" (it sounds so passive!) we're going public in a way that was unimaginable a decade ago" (30). In essence, the cookie enables web site designers to design their pages to what consumers wish to see. The problem is that the consumer doesn't know this is taking place.

There are ways of safeguarding yourself from web site cookies. In both Netscape's and Microsoft's Internet explorer there are built in features to warn users when web sites ask for cookies. In both formats the user can refuse to go any farther into the website. There are also several programs on the market that can mask or disable cookies. The best line of defense from cookies is to be wise when browsing websites. A user can say no to personal questions at any time.

To the dismay of many people, the Internet is similar to a wild animal out of control. With technologies of the past like radio and television, government legislation sets policy on its use. Unfortunately, with the exponential growth of the Internet, government legislation has failed to keep pace. In my opinion, the Internet should be treated the same as television, movies, video games, and music. An advisory board would review the content and the organization of a web site

and then assign it a rating. With the hundreds and even thousands of web sites that go on-line each day, this proposal is unlikely to occur. It would take government legislation to create an organization that would review, rate, and monitor the activity of millions of sites.

In reality, the size and scope of the Internet is too immense to control at this time. The bottom line for people concerned about the loss of privacy via the Internet is simple. If people have reservations, no one is forcing them to use the Internet. With the reliance on the Internet, this may be harder to accomplish in the future.

Medical Records Privacy

A person's private medical history has bearing on many aspects of his everyday life. This file begins at birth and continues to grow with every trip to the family physician. Every broken bone, allergic reaction, prescription, immunization, disease, surgery, and genetic defect is contained in this file. Many organizations claim to posses the so-called private medical histories of over fifteen million Americans. The main culprits of this information hoarding are insurance companies, pharmaceutical companies, and employers.

How does someone's private medical history become public? Very simple, this medical history is a powerful tool for these organizations to pay fewer insurance claims, create new drugs, and screen job applicants. The repercussions caused by the selling of medical records may be felt in many aspects of society. People with a predisposition for a certain illness could be refused healthcare, lose

their job, and be ostracized. This sensitive information could even hinder their children's chances at healthcare insurance and employment.

Any change regarding the current policy of handling of medical records must come from the people. Americans who are truly worried about the misuse of sensitive information should contact their legislators. Many people complain about certain legislation that is passed. But how many people actually take the time to write, call, or e-mail their legislators? The people are the government and have an obligation to speak their minds if they believe injustices are occurring.

It is paramount that legislation be enacted similar to the proposed Medical Records Confidentially Act of 1995. People should have access to their medical history when needed. Access would allow for accuracy and the termination of erroneous information. People should also have the choice if they wish their information to be sold to employers, insurance, and pharmaceutical companies. Those groups who break the rules should be subject to penalties. Concerned people should ask their healthcare providers about policy regarding the sharing of medical records. Expressing concern to healthcare providers is another way to create public awareness. Policy will never change unless citizens air their grievances. Waiting until the loss of a job, health insurance, and dignity is too late.

Identity Theft

According to Gill Klein of Media News Services, identity theft is one of the fastest growing crimes in the United States (Klein 1). Unfortunately, programs to

inform the public of the dangers and ways to prevent identity theft are insufficient. Presently, little recourse for victims of identity theft exists. Law enforcement officials are unaware of the scope of the problem and lack the legislation to protect the innocent victims. Many awareness groups blame the credit bureaus for the inflation in identity theft crimes.

The first step in preventing identity theft is to create public awareness of the dangers that exist. One should contact local legislators and emphasize the public disdain for the lack of refuge for victims. The social security number is probably the most sought-after item for identity thieves. Armed with this identifier, the thief can obtain driver's license, credit cards, bank accounts, loans, and file false tax returns. It is recommend that people go to the department of motor vehicles and have their social security number removed from their driver's license. It is also common for people to have the social security number on their checks. Any organization that takes checks could have an identity thief on staff. College students also run a high probability for identity theft because their social security number doubles as their student identification number. People who carry their social security card in their wallet or purse are also at risk. Memorizing the number and storing the card in a secure place is recommended. Many organizations ask for a social security number as a requirement for doing business. By law, the only organization that can request this number is the Social Security Administration. Unfortunately, many people are forced to give out their number as a prerequisite for doing business. One should be confident in the

organization and their privacy policies before agreeing to the release of their social security number.

Experts recommend that people examine their list of credit cards and cancel all cards that are not being used. When cards are not being used regularly, people will be less likely to notice when they are missing them until it is too late. Beth Givens of the Privacy Rights Clearinghouse believes that credit card companies make it too simple for people to receive credit. An easy way for identity thieves to obtain credit is through pre-approved credit cards. Thieves will sift through garbage cans to retrieve these unopened forms. Even tearing the forms into pieces does not offer people complete safety from theft. Office supply stores like Office Max, Staples, and Office Depot, now sell paper shredders for home use. Shred all pre-approved credit cards, credit cards statements, bank statements, medical bills, phone records, and any other private information. This small time inconvenience could save someone thousands of dollars. When possible, pay for purchases with cash. However, with the growth of electronic commerce, this option is less viable for many people.

The best way to stop identity theft is to be prepared before it occurs. Keep accurate records of all credit card purchases. On a regular basis, review credit statements to insure the accuracy of purchases charged to the account. If identity theft is suspected, cancel as many credit sources as possible. Call the credit agencies to alert them of any suspicious activity. Contacting law enforcement to file a report is advised, but this will help little until legislation acknowledges the problem.

On January 12, 2000, a victory was struck for privacy. The Supreme Court, with all nine justices in unprecedented unison, voted against a dangerous form of invasion of privacy. No longer can state governments sell personal data and pictures of a driver's license to private investigators. Outraged states' rights activists' claim that Congress's right to pass such a law infringes on states' rights to regulate driving. Senator Richard Shelby and Representative Frank Wolf co-authored the bill. Shelby stated,

> The decision will help protect women from stalkers, keep telemarketers from interrupting dinner, and give people peace of mind that private information collected by the government is secure. (3)

In the landmark ruling Katz v. United States (1967), Justice Stewart advanced a new standard for triggering the guarantees of the Fourth Amendment. This Supreme Court had to consider whether individuals have "reasonable expectations of privacy." Concurring, Justice John Harlan proposed a two-pronged test to clarify the majority's holding. Harlan articulated the standard as, "First, that a person have exhibited an actual expectation of privacy and, that the expectation be one that society is prepared to recognize as reasonable." The Court under Chief Justice Earl Warren tended to expand Fourth Amendment protection, while the more recent Burger and Rehnquist Courts have narrowed the scope of "reasonable expectations of privacy." Citizens should be very clear as to what their expectations of privacy are and ensure that others see them as

reasonable. Justices Marshall and Douglas make a telling point in their dissenting opinion, United States v. White. The Justices agreed,

> The concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on. (872)

Can one truly lead a private existence? In today's society, with rapid advances in technology, the other side of the world is only a keystroke away. Unless one chooses a hermit's existence, the likelihood of pure privacy is extremely remote. One can, however, begin the process of taking charge of safeguarding privacy. The first step in any transformation begins with awareness that privacy loss is inevitable. The next step is to take a personal inventory as to what is important in one's private life. By setting realistic goals as to what one has control over to alter, a blueprint for change is required. One can take control by becoming actively involved in the process. One of the most powerful ways to aid change is to support the work of legislators and lobbyists committed to privacy issues. One can continually challenge the establishment by asking, "Why is my privacy being compromised?" Informed citizens should spread the word that private information should remain private.

Citizens should learn the privacy policies of all organizations they contact. Citizens that learn these policies beforehand are able to question the rationale behind the need for personal information. Asking organizations the need for such

information will force them to reevaluate privacy policies. Typically, people only tend to worry about societal concerns when they are effected. Waiting until privacy loss has occurred is the wrong time to become involved. As with the treatment of many diseases, early detection is paramount to recovery. Safeguarding oneself from privacy loss is no different. Citizens should bar the "walls and doors" of their private existence so that no ill-seeking invaders can penetrate the sacred shrine of privacy.

Appendix A

Privacy of Library Circulation Records Policy

1. The circulation records of the St. Charles City-County Library district are confidential regardless of source inquiry.
2. Circulation records shall not be made available to anyone except pursuant to such process, order, or subpoena as may be authorized by law.
3. Upon receipt of such process, order, or subpoena, consultation shall be made with the Library District's attorney to determine if such process, order, subpoena is in good form and if there is a showing of good cause for its issuance.
4. If the process, order, or subpoena is not in proper form or if good cause has not been shown, insistence shall be made that such defects be cured before any records are released. (The legal process requiring the production of circulation records shall ordinarily be in the form of subpoena duces tecum (bring your records), requiring the librarian to attend court or the taking of his or her deposition and may require them to bring along certain designated circulation records.)
5. Any threats or unauthorized demands, (i.e., those not supported by a process, order or subpoena) concerning circulation records shall be reported to the Director of the Library District and to the Board of Trustees of the District.
6. Any problems relating to the privacy of circulation records which are not provided for in the above five paragraphs are to be referred to the Director or Deputy Director of the Library District.

SOURCE: St. Charles City-County Library District. Exhibit from organizational web site (1981)

Works Cited

Alderman, Ellen. , and Kennedy, Caroline. The Right to Privacy.
Vintage Books: 1995

"National Identification Cards." American Civil Liberties Union.
18 Feb. 1999. http://www.aclu.org/library/aaidcard.htlm

"The Presidents Privacy Problems." American Civil Liberties Union
27 Jun. 1996: http://www.aclu.org/congress/html
(16 Feb. 1999)

"Testimony Presented to the Senate Labor and Human Resources Committee."
American Civil Liberties Union. 21 May 1998:
http://www.aclu.org/congress.html (16 Feb. 1999)

"Congress Plans National Wiretap Week." American Civil Liberties Union.
26 Mar. 1996: http://www.aclu.org/congress/op-ed.html
(16 Feb. 1999)

"Stopping the Assault on Privacy in the Welfare Reform Bills."
American Civil Liberties Union. 15 Nov. 1995
http://www.aclu.org/congress/privacy.html
(14 Nov. 1997)

"ACLU Praises Summary Judgment Ruling in Oklahoma Tim Drum Litigation."
American Civil Liberties Union. 21 Oct. 1998
http://www.aclu.org/news/w12299/a.html
(13 Dec. 1999)

"Terrorism Bill Expands Wiretap Powers."
American Civil Liberties Union. 16 Apr. 1996
http://www.aclu.org/congress/wiretap2/html
(10 Jul. 1999)

"Federalizing Driver's Licenses and Birth Certificates."
American Civil Liberties Union. 29 Apr. 1996
http://www.aclu.org/congress.html
(7 Oct. 1999)

"Lawmakers Seek Ways to Protect Public Privacy." The Associated Press
16 Feb. 1999: 1

"Adoption Records Opening Law Upheld." 28 Sept. 1999. Associated Press. America Online. 29 Sept. 1999.

The Holy Bible. "The Book of Genesis." 1st ed. P.J. Kennedy & Sons New York: 1961. Chapter 9, Verses 21-22

Biskupic, Joan. "In Shaping of Internet Law, First Amendment is Winning." The Washington Post 12 Sept. 1999, A02

Bitol, Solage E. "Testimony on Drug Testing in the Workplace." Testimony to the United States Congress on Workplace Drug Testing. American Civil Liberties Union Washington, D.C. 14 May. 1998.

Brandeis, Louis D. , and Warren, Samual. "The Right to Privacy." Harvard Law Review 1890

"Placing the Clinton Administration Administration's Privacy announcement in Perspective." Center For Democracy and Technology. 11 Aug. 1998 http://www.cdt.org/privacy/gore/html (23 Jan. 1999)

Chrismer, Rich. Personal Interview. 20 Nov. 1999.

Cohen, Alan. "Know Your Cyber-Rights." PC Magazine May 1999: 36

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

Dowbenko, Uri. "Patriotic Gamble." National Review 13 Oct. 1997: 30-32.

Dowd, Ann. "Alert: New Threats to Your Privacy." Money Nov. 1997: 30-31

Ducat, Craig R. Constitutional Interpretation. 6th ed. St. Paul: West Publishing Company, 1996

Elizondo, Juan B. "Law Not Assuring Texans' Privacy." Austin 360 Online. Internet. 20 Sept. 1999

"E-mail Can Cause Embarrassment, Legal Woes." St. Louis Post-Dispatch 24 Jun. 1998: C5.

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

"White House Shifts Encryption Strategy." 20 Sept. 1999. Federal Computer Week. Yahoo. 7 Oct. 1999

United States. Federal Communications Commission. Engineering and Technology Action Committee. FCC proposes Rules to Meet Technical Requirements of CALEA. Washington: FCC, 22 Oct. 1998

Gaither, Chris. "Big Brother is Your Friend." Wired News Online. Internet. 20 Sept. 1999.

Garber, Joseph R. "The Right to Goof Off." Forbes 20 Oct. 1997: 297-298.

Givens, Beth. "Identity Theft." National Organization for Victim Assistance. City of Los Angeles. 29 Aug. 1999

Howd, Aimee. "Medical Records are Up for Grabs." Insight on the News 15 Mar. 1999: 18

"Internet Publisher Denied Access to Government Computer Cookies." Jefferson City Post-Tribune 1 Oct. 1998: 23

"Credit Identity Takeover Scheme Linked to Heroin Distribution." Queens, New York District Attorney's Office. 12 Jul. 1999 http://www.queensda.org.press99/07-12-99/html (22 Oct. 199)

Hadley, Jane. "Hearing Draws Passionate Tales of Privacy Woes." Seattle Post-Intelligencer 9 Sept. 1999. D5

Jaffe, Brian. "Why We Need a Bill of Rights for User Privacy." PC Week 27 Jul. 1998: 72-73

Lapham, Lewis. "Shadow Boxing." Harper's Magazine Sept. 1999: 15

Lieberman, Denise. Personal Interview. 5 Dec. 1999.

Manes, Stephen. "How Much Privacy Do You really Have." PC World Sept. 1998: 316

Marsh, Ann. "No Place to Hide." Forbes Sept. 1997: 226

McCullagh, Declan. "Smile for the Secret Service." Wired News Online. Internet. 7 Sept. 1999.

Mitchell, Russ. "Is the FBI Reading Your E-mail." U.S. News and World Report 13 Oct. 1997: 49

Moad, Jeff. "Privacy Issues Surrounding the Internet." PC Week 27 Oct. 1997: 83

Nack, William. "Every Parent's Nightmare." Sports Illustrated 13 Sept. 1999: 42-53.

Nash, Kim S. "Privacy Can be Lost in Background Checks." Computerworld 3 Nov. 1997: 43

O'Brien, David M. Constitutional Law & Politics: Civil Rights and Civil Liberties. W.W. Norton & Company: New York, 1991

Paul, Ron. "Insight on the News." Washington Times 17 Aug. 1998, 28

Quittner, Joshua. "Who's Out There Watching You." Time Magazine 25 Aug. 1997: 1-6.

United States Attorney. Western District of Wisconsin. Defendant Sentenced for Violating New Federal Identity Theft Statute. 24 Sept. 1999.

Rice, Valerie. "Big Brother is Watching." PC Week 13 Sept. 1999: 83

Romano, Lois. "Oscar Winner Tin Drum Ruled Obscene in Oklahoma Ruckus." Washington Post 1 July 1997

Sanstead, Carl. Personal Interview. 17 Dec. 1999.

Saphire, William. "Victory for Privacy." Jefferson City Post Tribune 14 Jan. 2000, Vol. 134, No. 272

"Spring Technologies to Study Iris Recognition Technology." Spring Technologies, Inc. 28 Apr. 1998 http://www.springtech.com/april2898.html (18 Feb. 1999)

Teicher, Stacy. "Breaking Ground on Privacy Rights." The Christian Science Monitor 17 Aug. 1999: 2

Tritz, Gerry. "Rohrbach's Bill to Safeguard State Employees' Privacy Called Anti-union by Labor Leaders." Jefferson City New Tribune 17 Feb. 1999, first ed. : A9.

Vespereny, Cynthia. "Mallincrodt, SSM Monitor employees' use of Internet." St. Louis Business Journal. 16 May 1999: 32

United States. Office of the Vice President. Vice President Announces New Steps Toward an Electronic Bill of Rights. The White House. Washington: Democratic Party, 31 Jul. 1998

Wilson, Dan. Personal Interview. 10 Dec. 1999.