

NORTHERN ILLINOIS UNIVERSITY

***The Information Age: America's So
Free They Are In Bondage***

A Thesis Submitted to the
University Honors Program
In Partial Fulfillment of the
Requirements of the Baccalaureate Degree
With Upper Division Honors
Department of Operations Management and Information Systems

by

David R. Beebe

DeKalb, Illinois

May 8, 1993

Student name: DAVID BEEBE

Approved by: William J. Jellen

Department of: Operations Management and
Information Systems

Date: April 29, 1993

Table of Contents

Executive Summary	1
Preface	2
Introduction	5
Personal Information Explosion Changes Value System	8
Power Struggle	12
Big Brother Is Alive	14
United States Law	16
Privacy Defined	17
Credit Industry	20
Example Flow of Information	21
Personal Information Is Easily Accessible	23
Mistakes	27
Clearing a Reputation Is Now Impossible	28
Old and Irrelevant Data	31
Data Out of Context	32
Direct Marketing	39
Consumer Fears	41
False Claims By Businesses	44
Tangible Costs	46
Society at Fault	48
U.S. Government and Law	52
Limiting Characteristics of Privacy	53
Fair Credit Reporting Act of 1970	56

Privacy Act of 1974	57
Computer Matching and Privacy Protection Act of 1988	58
Video Privacy Protection Act of 1988	60
U.S. Constitution	62
Limiting Traits of the Constitution	63
Pass the Principle, Not Just the Words	64
Future	68
Genetic Discrimination	69
Information Age May Even Threaten Thoughts	71
Conclusion	73
Bibliography	76
Appendix	79

Executive Summary

Although many may disagree, the conveniences of the information age do not outweigh the costs that it entails. These sacrifices include personal privacy, individual identity and ultimately the foundation of freedom that America's forefathers laid in the 18th century. Ironically, many do not see this new age as a process of taking away freedom, but actually adding to it. However, this is not the truth. This stripping of freedom is taking place so subtly that most Americans cannot see it happening.

A few methods by which the information age causes this loss of liberty need to be revealed. For instance, the credit industry handles enough information about individuals to monitor them like a dictator. Direct marketers exploit and maneuver people like pawns due to new dominating technology. Yet in defense, the American law system and Constitution can be twisted to become insignificant in light of the raw power of the computer.

The future does not look any brighter if America does not wake up to the deception of the information age. Public and private institutions will increase in power while the precious individual will lose theirs. People will continually become less important while the information they can provide will become priceless. This is not what America was founded for. It is time that temporal values be laid aside and virtues like freedom, liberty, and the love for humanity be revived.

Preface

This paper was not written to take a technical view of the information age, but rather to establish a sociological discernment of American society. It also attempts to take a step back to get the big picture of where society is currently at in respect to personal privacy and individual identity as a result of this information age. Plus, it includes a look into the future to provide some prophetic possibilities.

While this present and future analysis may seem ludicrous, a similar investigation proves its validity. In 1948, George Orwell produced his most famous novel, 1984. In his book, he foretold of a society where public institution had complete control over the personal activities of the people living then. In 1948, this prediction must have seemed unrealistic. However, Orwell knew exactly what he was talking about because hindsight reveals that measures of freedom are diminishing. Even though his prediction was not fully complete by the year 1984, it is evident that American society is well on its way to fulfilling his prophecy.

This paper intends to reveal how the information age has effected these

foundational values of freedom and expose the deceptions of the information age. A mere investigation of current secondary sources quickly displays these dangers to freedom. Consequently, this paper also strives to be as credible as 1984 in surveying past, present and future dangers of American independence.

The three main sections of this paper that uncover the dangers of this information age are the credit industry, the concept of direct marketing, and U.S. Constitution and law. The credit industry could be considered the hub for personal information gathering. As a result, intimate information about individuals is now public. Direct marketing is a concept that takes this personal information and unjustly manipulates consumers with the new power of technology. This may exploit their buying habits, political preferences or other personal dimensions of identity. Sadly, the U.S. Constitution and law may have even become moot and provide no deterrence to the power of the computer. This report will use these three sections and their subsections to prove Orwell's insight of the deterioration of American privacy, personal identity, and ultimately the cornerstone of freedom itself.

Obviously, a clear purpose of this paper is to inform and enlighten the reader about current technology and how it is being used unjustly. However, its motive goes much deeper than this. Because it questions some of the

temporal values that American society has placed on what this new information age has to offer, hopefully in the end, this paper will force the reader to reevaluate and change some of these value choices that he or she has established with respect to the information age.

Introduction

As the world stands on the edge of the 21st century, waves of optimism for the future spread due to technological advances. Computers are processing faster and more efficiently, automatic teller machines conveniently enable consumers to have more flexible finances and various other technological advances have given more power to the individual. In fact, the new opportunities of the information age will continually enhance the value of life well into the future. Is this true, or are people just focusing on the opportunities of this age and not comprehending the threats it can entail? Is it possible that the world is deceived and that the real truth is that the power of the individual is actually decreasing? More specifically, is the information age adding new freedoms to the American people, or is it depriving them of the freedom they once had? Technological advances definitely add to the efficiency of living, but are these new capabilities worth the cost? For example, a case in St. Louis may help illuminate this phenomena.

A journalist from Washington D.C. recently moved to St. Louis. Shortly

after receiving auto insurance his policy was revoked due to information revealed about him in his credit report. Since he had never been in an accident and he did not have a bad driving record, he began to investigate. Much to his surprise, the reason for his disqualification was comments that were corroding his personal file. This interesting file revealed that he was disliked by his neighbors, suspected of being a drug user and was considered to be of the "hippy type". As it turns out, all of the information in his file was from an old neighbor, an elderly woman who had held a grudge against him for his sympathetic, antiwar demonstrations and because his children occasionally ruined her flower beds (Linowes 130).

In a similar case, a woman was continually turned down for jobs that she was quite qualified for. After examining her personal file, she too uncovered the reason of her problem. Her file included critical remarks about her that were made from her third grade teacher over thirty years prior (Linowes 199).

Karen Hochman certainly knows how technology can violate a person. Recently, she talked to an ITT salesman that was selling long-distance services. She mentioned, however, that she did not make many long-distance calls. "I'm surprised to hear you say that," the caller responded. "I see from your phone records that you frequently call Newark, Delaware, and Stanford, Connecticut."

As expected, Karen was shocked that he knew this information about her. "If people are able to find out who I call, what else could they find out about me (Rothfeder 76)." The fact is that many people do not realize the immense information that numerous agencies and organizations know about them. Many, like the victims in these cases, though, are being quickly awakened and welcomed to the enticing trap known as the information age.

There are many obvious threats to privacy nowadays. Actually, two main types can be identified. "One is the growth of information technology, with its enhanced capacity for surveillance, communication, computation, storage, and retrieval. A second, and more insidious threat, is the increased value of information in decision-making (Dejoie 47)".

In the past, surveillance was used mostly on criminals to monitor their activities. But with today's technological power, government and private agencies can do sweeping surveillances of large segments of the U.S. population. For example, employee surveillance has caused much conflict lately. These systems can track the number of minutes spent on the telephone or even the number of strokes on the computer that the employee is pushing per hour. "But by far the most important high-tech threat to privacy is not an exotic surveillance device but a familiar storage system: the computer.

Computers permit nimble feats of data manipulation, including high-speed retrieval and matching of records, that were impossible with paper stored in the cabinets (Lacayo 34)."

Therefore, the most dangerous threats are the subtle ones that go unnoticed. "Much attention has been focused on drug testing and polygraph testing as potential invasions of privacy. But there are far more serious - and widespread - privacy invasions taking place every day, so hidden from view that the victims may not even know that their privacy is being invaded (Marshall 30)." These threats come from collecting and disseminating personal information in order to indirectly shape an individual's life. Consequently, they come directly from the new discovery of the computer because these kind of invasions would not be possible without the power of the computer. The innocent individual is left with a life that he thinks he has total control of, but actually he is being so subtly manipulated that his life may not be only his.

Personal Information Explosion Changes Value System

The methods of data gathering seem to go unnoticed nowadays. Anytime a person applies for a job, insurance, hospital services, or even school, his or her personal file is being constructed. "What compels concern here is not any

single privacy-invading error in judgement. Instead, it is the steady growth of systems for generating, storing, and communicating personal information on vast scales (Rule 14)." Airlines know where people vacation and with whom, banks know much money people spend and where they spend it, and credit card companies know a consumer's buying habits in distinct detail. However, this is just the tip of the iceberg of the information that is known about everyone living in the civilized world, and there's no question how it is gained.

"Every person fills out quite a few forms in his life, and each form contains an uncounted number of questions. The answer of just one person to one question in one form is already a thread linking the person forever with the local center of the dossier department. Each person thus radiates hundreds of such threads, which all together run into the millions. If these threads were visible, the heavens would be webbed with them, and if they had substance and resilience, the buses, street cars and the people themselves would no longer be able to move (Dejoie 48)."

-Aleksandr Solzhenitsyn

Individually speaking, it is therefore obvious the information age has and will continue to have an enormous impact on people because more and more decision-making is done by what is revealed in these personal files. Plus, in this new technological age, information is power. An anecdote to explain this is that of war. The more information an army has about their opponent, like where their ammunition is or when their next attack is planned, the more power

they have over the enemy. This is precisely the kind of power that the government and private institutions have received due to the information age.

"It is widely believed that the balance of power in our society is becoming more and more dangerously weighted in favor of large institutions - government and business alike. The chief reason is they are the ones with the personal information about people and the people don't know it (Linowes 1999)."

The impact on society as a whole is quite relevant as well. After thorough examination, it becomes quite evident that the computer and related technology have changed the world more socially than technologically. The centers of power are no longer in the hands of the American people, a belief that the U.S. was built on. Instead, it is in the hands of the government and private organizations that can mobilize any data on any citizen at will, for any purpose.

Technology has also directly affected society's perceived values, and remarkably has changed how people view the world. For instance, large amounts of the personal data just mentioned is readily available to just about anyone seeking this information. This kind of sociological change was not considered when the computer was first invented. As recently as World War II, most of this detailed information would not have been collected in the first

place. This is simply because the computers that the world knew then did not own a fraction of the power that computers have today. The retrieval and exchanging of information is now a process of seconds. Detailed information can travel from coast to coast in the blink of an eye. The ultimate consequence of this new found power is that critical and important decisions can now be quickly made on the basis of this data. This puts many Americans quite vulnerable to this information. The result is a distinct change in the way American society's value system develops.

"The computer has wrought a fundamental change in American life by encouraging the physical migration of information about the most minute details about our personal and public lives into the computerized files for a large and growing number of corporations, government bureaucracies, trade associations and other institutions (Marshall 35)."

-David Burnham

No other place in society's value system has miraculous changes taken place more than in the respect to individual privacy. The loss of privacy is just one of the key symptoms of America's fundamental social changes from the information age. The power of public and private institutions has been growing much quicker than that of the individual citizen, while there is little flow of information about these institutions going back to the people. The computer has enabled this kind of power change. "The invention of computers gives rise

in our time to a situation somewhat analogous to the discovery of iron in prehistoric times, for as the weapons fashioned of the new metal must have been a key element in the ancient power structures so the computer's ability to store, manipulate, and transmit data makes it a key component of power today (Department of Communications/Justice 19)."

Power Struggle

It is assumed that it was people who originally invented the computer and so naturally they would have power over it. However, if humans have become so dependent on the computer for the information they provide, then who really is in control?

"Progress imposes not only new possibilities for the future, but new restrictions. The simple faith in progress is not a conviction belonging to strength, but one belonging to acquiescence and hence to weakness (Burnham 10)."

-Norbert Wiener

This is much like the concept of money. Typical Americans spend most of their adult lives trying to gain money. In this search, they become so dependent on money that they cannot live without it. The question is when people become so dependent and vulnerable to the amount of money they have,

then who is really in control? Is it the money or is it the person being controlled by money? Although this is not perceived by the person, the money is the one in power over the individual. The person thinks he has power over the almighty dollar, but in reality that love for money twists and puppets him around to wherever it leads. This love for money is much like the love for information in the information age. Consequently, because humans have become so reliant on the computer, they have lost their original power over it.

Although the human mind transcends the computer's intelligence, the raw processing abilities of the computer enables it to perform tasks that the human mind would never be able to attain. It seems that humans have become slaves to their technological improvements, and because of this total dependency on the computer's power, they have lost all of theirs. "By the very slowness of our human actions, our effective control of our machines may be nullified (Burnham 10)." Sadly, this power of the computer migrates right down to the individual. "Computers, as a consequence of their own efficiency, break down many of the protective barriers of inefficiency which in the past helped to shelter privacy (Department of Communications/Justice 111)."

Big Brother Is Alive

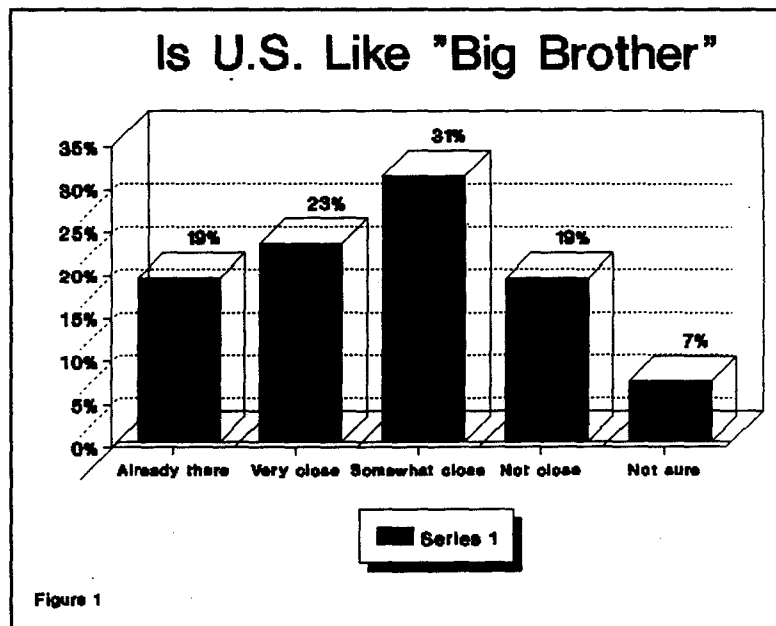
In 1948, George Orwell wrote what turned out to be his last work, the classic 1984. It drew the chilling picture of how a totalitarian government had stripped all traces of privacy, dignity and ultimately liberty away from all the individuals living at that time. The infamous Big Brother signs were posted in numerous places reminding people "Big Brother is Watching You". People were constantly being watched through video cameras and information was twisted to meet governmental needs. In this prophetic society, the people had become mere chess pieces that the government moved around where they pleased.

"And yet Orwell, with his vivid imagination, was unable to foresee the actual shape of the threat that would exist in 1984. It turns out to be the ubiquitous computer and its ancillary communication networks. Without the malign intent of any government system or would-be dictator, our privacy is being invaded, and more and more of the experiences which should be solely our own are finding their way into electronic files that the curious can scrutinize at the punch of a button (Burnham vii)."

As Figure 1 on the next page shows, many people agree that current American society has become a resemblance of Orwell's form of humanity (Katz 138). This chart shows that approximately 73 percent of American people in 1989 thought that the U.S. society had become at least "somewhat

close" to the resemblance of 1984.

In the world today, information is power. As already mentioned, the computer has enabled the government and private institutions to gather hoards of information about individuals.



"Always the eyes watching you...asleep or awake, working or eating, indoors or out of doors, in bath or bed - no escape. Nothing was your own except the few cubic centimeters inside your skull (Thompson 132)".

When this clip was written from Orwell's book, it must have seemed ludicrous to actually believe. However, with the enormous amount of intimate information known about individuals today by outside organizations, this quote is alive and quite applicable to the present world. Though Big Brother's methods were quite brash and disturbing, equal or even more powerful ways of surveillance are now in place. Although much more subtle than 1984, today's information systems do not place second for their ability to effectively monitor

and control society. "Technology has enhanced the power of social control. The information-gathering powers of the state and of private organizations have torn asunder many of our conventional notions of privacy (Marshall 31)." The ramifications of this social control also promotes a society where people become like robots. Therefore, the only logical conclusion is that the computer and related technology have not only triumphed over personal privacy, but it has and will continue to destroy personal identity as well.

United States Law

Where does U.S. law fit into this mess? It should have a significant impact since a recent survey concluded that 93 percent of Americans think that companies that sell information to others should be required by law to ask permission from individuals before making the information available (Lacayo 36). Sadly, though, law is far behind the information age's pace of technology. The law system of the United States is far too bureaucratic to keep up with the new and always changing demands of the almighty computer. In other words, U.S. law and even the Constitution fall prey to the power of the information age. Can the principles of a document that was written over 200 years ago have any chance of fulfilling its original purpose now that society has been

totally transformed due to the computer? Can personal privacy be protected by a Constitution that was written when intimate information could not be processed and stored as quickly and easily as it can be now? These questions will be discussed later but first a concrete definition of privacy needs to be established.

Privacy Defined

Before examining the current status of privacy in America, it is essential to understand what privacy is, where it comes from and why it is so important. How can an individual think his privacy is being violated until he has a clear perception of what is being taken from him. First of all, a precise definition is needed. Webster's Dictionary defines privacy as having a "withdrawal from company or public view (Newfeldt 1071)." It's evident from the information age that this kind of privacy may be prehistoric. Still, a broader definition of privacy is needed.

"Privacy - The social expectation that an individual (and by extension, a group of individuals, or an institution, or all society) must (1) be able to participate in determining how information about him is used or communicated to others, be assured that such information is properly protected against inappropriate use; (2) be assured of openness, forthrightness, and fairness in relations with any record-keeping organization that maintains data about him; and (3) be protected against

unwelcome, unfair, improper, or excessive collection or dissemination of information or data about him (Hoffman 10)".

This definition still seems to only touch the service of the essential commodity that most Americans hold sacred. Undoubtedly, there seems to be a deeper question which is at the heart of the debate. That is, does privacy really matter? This question raises two schools of thought. The one holds that the world would be a much better place if no one had any secrets. Freedom of information would be the norm in order for businesses, banks, hospitals and even the government to serve its citizens much better. However, consider the second school of thought that seems to be the original idea of democracy in the first place.

"The last remaining area of true humanity for all of us is that in which we can be ourselves, do what we like, waste our talents and time - and perhaps discover new truths - without having the rest of our community breathing down our necks, expressing its disapproval of our ways, and pressing us to conform. Only in this way, the argument runs, can we develop our full potential as unique individuals (Sieghart 25)."

It seems to be part of human nature to be left private and reach an individual's capabilities on their own. However, this is the exact desire that is being destroyed by the information age. Consider this quote from Adlai Stevenson:

"If I were asked what the greatest danger is today in the conduct of democracy's affairs I suppose I would think first of war - but second, and immediately - we in America are becoming so big, so organized, so institutionalized that there is increasing danger that the individual and his precious diversity will be squeezed out completely (Linowes 1)."

-Adlai Ewing Stevenson

Mr. Stevenson strikes a clear chord when he says the United States is losing the "precious diversity" that it once entailed. This loss of identity of the individual is directly correlated to the fact that the computer has revolutionized America's social value system. It has put the power into the hands of institutions and no longer in those of the people. Remarkably, this was a foundational idea of America's democracy when it first began. This idea is now becoming obsolete because of the almighty computer. No other warnings prove this point more directly than the credit industry, the direct marketing concept and obviously the ramifications this information age has on the U.S. government, law and the Constitution.

Credit Industry

The credit industry holds an intricate part in the data explosion of the information age. They seem to be the cornerstone of information use in the world today. How the computer is changing banking, insurance and other industries are filed under the credit industry because most of the information sought from these other businesses comes directly from the credit agencies. Although their original motive of gathering thorough information about credit seekers is substantiated, to loan credit without financial information about the individual applying would be ridiculous, their uses of that information after it is gathered seems to be not only unethical but also demeaning to the original individual.

It is the credit industry that seems to control the hub of personal information about people in the private sector of society. Sadly, it is also the credit industry that sells this information to businesses and other institutions that ultimately destroys any hope of personal privacy. Not only does this information include the intimate data that a consumer fills out for the application of a credit card, it also includes detailed reports on their buying habits which come from the statements of their credit card. These habits will

reveal his or her lifestyle, travel exposure and other interests, such as magazine subscriptions to reveal hobbies or even the political party he or she supports.

This kind of information is very beneficial to any organization looking for potential customers or voters. In fact, this political persuasion technique may be the scariest potential power that the information age has given to the government and organizations.

Example Flow of Information

Examine this chain of events to clarify just one example of thousands of how a flow of information could go:

(1) A typical consumer applies for a credit card and reveals information such as his social security number, bank account numbers, address, average yearly income and other personal data. Thus, he has allowed the credit company to virtually use vast amounts of information about him that they may see relevant for his approval of credit.

(2) A year later, the consumer applies for a loan from a mortgage lender revealing even more information about himself. The mortgage lender, to see if he is reliable for their loan, checks with the credit card company to see if he has been faithful in paying his bills. For a small fee they can

receive a full report of his credit history with them.

(3) Seeing the profit potential, the credit company pursues gathering more information about the original credit seeker. So they buy more information from the federal government, state and local courts, motor vehicle bureaucracies, hospitals, banks, employers, estate and insurance companies, and other organizations holding information about this consumer.

For example, checking accounts are like financial diaries of a person's life. Plus, a survey done at the University of Illinois found that 80 percent of Fortune 500 companies give personnel information to credit grantors, while over half do not even tell their employees about it. This is probably because 38 percent of these companies do not even have a policy concerning which records can be disclosed to others (Linowes 200). For a small profit, the credit company then sells this entire consumer profile and credit record to any institutions who may find use of it.

(4) For instance, private businesses especially find great use out of this information and are more than willing to pay a small fee for it. This information enables them to directly target at the market that their

product's adhere to. Because this consumer profile report holds personal information such as age, income, buying habits and other useful demographic material on a consumer, they can better target at the market to which they are selling. For instance, a car company selling an expensive, sports car would find some information quite useful. They would probably want to send their advertisements to the young or middle age group, to those who's incomes could afford it or to those whose buying habits indicate that they would spend \$30,000 for a car. This direct marketing will be discussed in further detail later.

Just from this simple example it is easy to see how vulnerable consumers are to the information that institutions hold about them. Technology has not given them more power, it is draining it from them and giving it to those who hold this information, like credit companies. Plus, since the invention of the personal computer, this kind of personal information is now available to anyone who wants it.

Personal Information Is Easily Accessible

"For very little cost, anybody can learn anything about anybody (Rothfeder 74)." For instance, as just an experiment, an editor of Business

Week sought to find out how much personal information he could find and how easy it was to get it. For a moderate fee, the editor got access from his home computer to a superbureau's database. He was then able to rummage through names of millions of Americans at will. At about \$15 per report, he could purchase a report that included the individual's information like bank balances, buying habits, possible abortion data, driving records, potential divorce records and other intimate details. Ironically, two of the names that he pulled out were those of great prominence. One was a Democrat Representative from Illinois named Richard J. Durbin, and the other was Dan Quayle. "The Vice-President charges more at Sears, Roebuck & Co. than at Brooks Brothers. He has a big mortgage. His credit card number at D.C. area Merchants bank is... Sixteen digits long (Rothfeder 74)."

What's even worse is that many important decisions are determined because of this information. For instance, a person may no longer get a job, acquire a loan, get accepted into school, or even receive hospital care before their profile is investigated. Many times the use of these types of databases becomes controversial.

An example of this kind of fraudulent database is Physicians Alert. This database was set up to provide doctors with the names of patients who had filed

for malpractice suits, whether their suits were appropriate or not. Obviously, these patients were blackballed and would have difficulty finding medical assistance, even in times of emergency. Fortunately, because of media attention and public complaints, Physicians Alert closed down. However, there are many other databases like it that still exist.

There are many similar databases that are utilized by landlords. The landlords consult these databases when considering a potential tenant. These databases list those tenants that either did not respond to legal action by a landlord or who lost their case in court. Obviously, if potential tenants have had problems with landlords before, they too will get blackballed. This is true of a woman in Los Angeles who kept getting turned down in her search for an apartment because of a legal dispute with a landlord (Marshall 30).

A clear problem with this database is that if a tenant does not stick around to fight an eviction in court, something which he is not legally obligated to do, he could end up in the database. His consequence is getting blackballed. The problem is that these kind of inconsistencies with databases are very frequent. As can be expected, this results in many innocent people paying for the flaws of the information age. Again, because American society has become so totally dependent on the personal details now being kept by the tyrannical

computer, it has set itself up to reap the burden of the information age. If it is not scary enough that lives are shaped on the basis of this information, further investigation reveals that much of this data is bogus. Plus, some of this information is just old and irrelevant or like the landlord database, it is simply taken out of context.

Mistakes

There are three main credit agencies in the United States that hold the majority of the information available. These companies include Equifax, Trans Union and TRW. Together, the number of credit bureaus controlled by the Big Three has doubled during the 1980s to more than 200, giving them information on over 90 percent of the United States's adult population. Plus, it is no wonder why they are in this business. In 1988, Equifax's operating income from sales of credit and marketing data was \$61.5 million with an equally impressive mark in revenues of \$259 million. TRW's revenues in the same categories that year were \$335 million while Trans Union's was \$300 million (Rothfeder 80).

Every month these agencies purchase computer records, mostly from banks and retailers that detail the financial activities of virtually every adult American. In return, these reports are sold to credit card companies, mortgage lenders and anyone else who shows a "business interest" in them. These companies contain approximately 150 million individual files each (Lacayo 37)!

Plus, one estimate is that each American has approximately 50 files from private organizations and nearly 25 files from the government (USA Today 11). The terrifying truth is that Consumer's Union recently reported that nearly half the credit reports it studied from the nation's largest credit bureaus contained some inaccuracies. As can be imagined, this can produce some pretty destructive outcomes to many innocent lives.

Clearing a Reputation Is Now Impossible

Eugene N. Wolfe, a retired speech writer who lives in McLean, Virginia, realized the consequences of a data error. In 1986, he was puzzled when a local bank turned down his request for a loan. Ironically, he discovered that for years an Equifax subsidiary called Credit Bureau, Inc. had merged his credit history with another person named Eugene N. Wolfe. However, this Eugene N. Wolfe had many debts. "At one time I had to pay the highest interest rate on a car loan because the dealer was looking at bum debts that were erroneously listed in my name, but I didn't know it," Wolfe complained (Lacayo 38). After weeks of paperwork, Wolfe thought he had cleared everything up. Recently, however, he was turned down for a credit card and rediscovered that information about the other Eugene N. Wolfe had found its

way back into his life.

This case introduces a further problem with the use of personal data by credit agencies. Once a person's file becomes sour, it may be virtually impossible for that person to catch up with it. The reason has already been mentioned: information on individual travels faster than the individual can keep up with it. Because all businesses are not linked up with a central database, the individual would have to correct his file with all the organizations that have it. What often happens, though, is that the reports are circulated to a wide variety of users' data banks before the mistakes are detected. As already seen, tracking the footprints of this information and finding out who has it can ultimately be impossible. Sadly, even if the individual can catch up to the mistakes and correct them all, his problem still may not be over.

"A reputation once broken may possibly be repaired, but the world will always keep their eyes on the spot where the crack was (Linowes 23)."

-Joseph Hall

Therefore, the spreading of this personal information becomes like a virus out of control. If, for a moment, the victim thinks he has caught up, in reality he really has not. As in the case of Eugene N. Wolfe, this further adds to the vulnerability that people have toward the almighty computer.

Similarly, in New Orleans a computer was doing a routine background check on a woman named Shirley Jones. The computer revealed that a woman named Shirley Jones had an arrest warrant out for her. The innocent Shirley Jones was arrested twice, spent time in jail and had three court appearances before the mistake was corrected (Linowes 21).

These errors are not limited to the computer. Human error can also be recorded for many years without people knowing. Unfortunately, the use of the computer does not let these errors be forgotten, it rather magnifies it. In one case, an innocent teenager visited the doctor at the same time other youths were there for the treatment of drug addiction. At one point, one of the teenager's neighbors came in and noticed him in the waiting room with the teenagers there for their drug problem. However, the innocent teenager thought nothing of it at the time. Years later, though, when he was married, employed and living comfortably, the incident surfaced. While expecting his first child, he applied for life insurance. His application was denied. Amazed, he consulted his file and was told that adverse information was in it. Tracking the information down, he found out that on that day years before in the doctor's office his neighbor had told an insurance investigator that he assumed that the innocent teenager was on drugs because of the other youths that were in the office that

day (Linowes 166).

Old and Irrelevant Data

This case reveals another fundamental change in American society due to the computer. In the pre-computer years, old and irrelevant information was discarded because of the paper dragon, a fictional character representing the mountains of paper that would be needed to store on-going information about many customers. Now with the computer, however, this aged information can be kept on computer file instead of paper. This entails tremendous consequences on everyone in the United States. One missed payment, one accident or even one bad grade in high school will go down in the annals of that person's personal file forever. For example, the American Business Conference and the National Alliance of Business have joined with the Educational Testing Service in creating a program for a nationwide database of high school records. It would give employers access to a job applicant's grades, attendance history and even the evaluations of teachers (Lacayo 36). In other words, just like Mother always warned, a poor report card in the sixth grade could follow an individual for life.

It is to the point of to err is human, but the recording and remembrance

of that err is utilized by the computer. Sometimes, though, these computerized memories were never human flaw in the first place. For instance, if someone applies for workman's compensation, it is recorded and put on a list. Potential employers may take a look at this list and not hire this person because they are fearful of injuries or more claims of workman's compensation. The Employers' Information Service, a company in Gretna, Louisiana, is one company that sells this information about prospective employees (Lacayo 34). Therefore, Big Brother not only is watching, but he's remembering every questionable move someone makes. This is a scary contradiction to what America defines as freedom. But this redefining of terms seems to be the norm of the information age.

Data Out of Context

Another type of data error is when information is taken out of context. These kinds of errors do not deal with misplaced digits or other errors in the data. They deal with the encoding and decoding of information. That is, the dangers of the different interpretations of data. For instance, the youth's neighbor in the doctor's office definitely misinterpreted that the boy was a drug addict. However, data interpretations can get much more complicated when

even more people are interpreting a single piece of information.

"A major problem created by the widespread application of personal-data record-keeping is the inability to anticipate and control future uses of information. Systems evolve on the basis of immediate need, often with little or no explicit consideration of their long-term consequences for individuals of society as a whole (Hoffman 155)."

No longer is information gathered for a single purpose and therefore standard for interpretation. Different uses for the same piece of information can produce serious problems. These numerous interpretations of a single piece of data result in numerous pieces of different data, much of which adhere to a given organization's exploitation of it. Since data travels around the world in seconds, most of the time the data receiver has no idea who generated the data or the foggiest notion of its original purpose. As a result, a person's actions and personal information is often misinterpreted. This is one of the biggest threats caused from the information age. That is because data out of context has a missing link in the communication process. Feedback is not available simply because most of the time the receiver does not know who developed the data in the first place. Therefore, the receiver is left with the task of interpreting the data, which can result in quite a bit of data inconsistency.

Standardized data is imperative. The problem is that standardized data may be only a dream in the world today because of differences in environments

and culture. In the United States alone there are hundreds of subcultures. Once again, the average, innocent citizen is the one who reaps the problems of technology. This time, however, not only is his privacy at stake, but it seems he is shaped like clay with whatever translation that the interpreter may have.

A perfect example of this data out of context is arrest records. The National Crime Information Center (NCIC) is a computer system used by the FBI to track criminal information. They hold information on Americans who have been arrested, which means nothing until conviction according to federal law. However, why is it that many employers in the U.S. want to know if prospective employees have been "arrested"? The statistics show that 40 percent of the data in the NCIC are only arrest records, no convictions (Dejoie 124). Yet, many pre-employment credit checks and insurance inquires want this information to make decisions. In other words, they want to stay away from people who have been arrested as much as they can. However, the arrest means nothing because many people were never guilty in the first place. Yet, the FBI is creating a database on 25 million Americans who have been arrested, even if they were not convicted (Lacayo 40). Because data is taken out of context, though, they are considered guilty anyway.

Similarly, many insurance companies turn down an applicant if his or her

file reads that another insurance company has rejected them. In fact, one out of five insurance companies participate in this refusal policy (Linowes 115). In some cases, though, an applicant may be declined simply because he or she happens to live outside of the first insurer's preferred area of concentration. However, the second company who declines the applicant simply because they have been declined before does not know this. This could make it very difficult for people to get the proper insurance that they need. This is data out of context.

Another example of this is when someone's file reads that he was convicted of criminal trespass, convicted, and sentenced to six months probation. Prospective employers might think this person is one of those violent vandal kids, which results in no job for this applicant. What it turns out to be, though, was a civil rights demonstration and the conviction was even reversed on appeal because of impermissible intrusion of the First Amendment (Dejoie 125). In cases like this, data out of context occurs simply because the data was incomplete. Nevertheless, how is the receiver to know that? This is the danger of relying on data without truly knowing what it means.

There are some illuminating statistics that are produced when this kind of information is taken out of context. If someone is a late teenager who is a

black male living in Harlem, the odds are between eight in ten that he has an arrest record (Dejoie 125). This is not a conviction record, just an arrest record. This high arrest percentage comes from inner-city police who know how to keep a lid on the problems in cities like Harlem. If they see kids doing anything suspicious at all they will take them into the station to keep them off the streets in order to keep them out of trouble. Their motive is that it is better to be safe than sorry, but this may be just the beginning of the teenager's trouble. They may have many problems getting a job, a loan, or having a normal life now that their file says that they have been arrested. What has happened to equal rights? Is this to say that the technological capabilities that are now available in the information age have actually promoted the use of discrimination? The bottom line is yes, but this is a norm of the information age. Discrimination is more subtle and obviously easier to spread when much of this information is racial, religious or pertaining to other traits that are supposed to be protected by law (Department of Communications/Justice). The computer's deceptive ways have conned Americans to think that it is adding to their freedom, but the truth is that it is taking it away. The right hand clearly does not know what the left hand is doing.

Where does it end? If someone calls an AIDS Hotline, does a computer

track their phone number to their address and name and put it on a computer list? Do people scan this list thinking that this caller is either HIV positive, has AIDS or a concerned homosexual? This may seem like an extreme case, but since the technology is available some insurance companies may want a copy of these lists for future reference. This is how abused personal identity has become in the United States.

The most terrifying thought concerning the different forms of database errors is when the number of errors that go undetected is considered. How many errors could be eroding peoples' files and they do not even know it? How many Eugene N. Wolfe's are out there that are paying more interest than they have to? How many people are paying higher insurance bills than they have to? This could be quite a few because the Medical Information Bureau furnishes information of all kinds to approximately 800 insurance companies throughout the company, while much of this information is not verified (Linowes 198). How many other people are getting turned down for jobs, loans and credit cards when they do not have to? How many people's lives are being totally altered because of unknown mistakes in their personal files? It seems impossible to measure the amount of impact computers have on people and they do not even realize it. With mistakes, this impact balloons and goes

to prove that people are not empowered over the computer, the computer has reign here.

It has become evident in the information age that people are no longer important, but rather the information about them is what is important. Consequently, the more information the computer holds on a person, the less power the individual has over the computer. Thus, personal identity becomes obsolete. With all this information about people in files, organizations can manipulate that person with the data they have. No other way of business exemplifies this more than direct marketing.

Direct Marketing

Following a visit to her doctor's office, a young wife found out that she was pregnant. Soon after, the expectant mother was deluged with mail from suppliers of items ranging from diaper services and baby carriages to insurance and furniture. Since she had not informed anyone of her pregnancy, she assumed it was her doctor and accused him of breaching the confidential relationship between physician and patient. After investigation, however, it was revealed that while she was in the doctor's waiting room she had filled out a card offering free literature on prenatal and postnatal hygiene. What she did not know was that by filling out this card she had placed herself on many companies' mailing lists (Linowes 140). As a result, these companies were using direct marketing to enhance their probabilities of sale.

Placing individuals into categories has become big business. Compiling data on an individual's personal life style is very helpful to marketers seeking to target a niche market of specific personal interest. Due to the new power of the computer, the possibilities of direct marketing are endless. For instance,

companies can buy the results of the entire 1990 U.S. census. With this census, they are linked to a street-by-street map of the United States. Citicorp and other data merchants are even piloting systems at supermarkets that will record every purchase because of the new use of UPC symbols. "Folks who buy Mennen's Speed Stick could get pitches and discount coupons to buy Secret instead (Schwartz 41)."

Through today's technology, it is possible to store every transaction people engage in into somebody's computer. It is almost impossible, except for becoming a hermit, to not be placed on one of these marketing lists. By merely living at a particular address, subscribing to a telephone service or voting in an election, marketers can form lists of someone. By getting married or divorced, going to school, buying a car or getting a job, marketers can develop even more specific lists on an individual. Virtually any activities that humans do can construct lists of their interest.

Private businesses can buy these lists from the credit agencies already mentioned or from any other organization that holds information on individuals. This is done primarily to construct these lists. These lists are created for a simple reason. They automatically and at mind-boggling speeds identify people who are most apt to respond favorably to solicitations for vacations abroad,

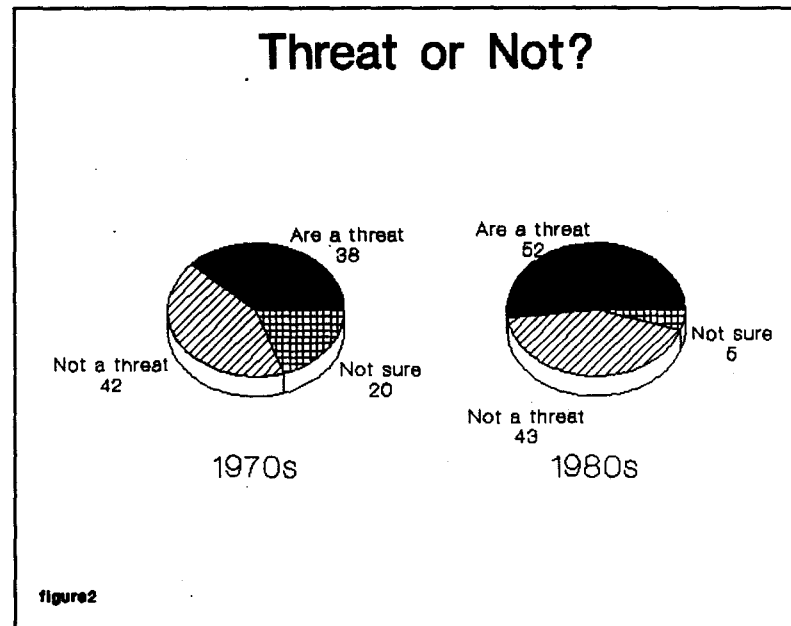
home furnishings, car rentals or any other consumer needs. "When it comes to direct mail merchandising, the key factor is selectivity (Linowes 141)." Many times these lists start with finding out where these people live.

Since 1985, the United States Postal Service has been licensing an extensive, computerized list of American addresses to direct marketers, insurance and credit companies. This list greatly benefits private businesses in their search for selectivity. "Currently, 23 direct-mail marketers, credit bureaus and insurance companies buy the list for an initial licensing fee of \$80,000 and a yearly charge of \$52,000 (New York Times A17). By law, though, selling these lists would be illegal for any governmental agency. Nonetheless, the Postal Service claims that they are just licensing computerized access to this list. However, marketing companies can access this information and then turn and sell the updated lists to other businesses, and that is exactly what has been happening. This ability to track where individuals live definitely aids in the process of consumer supervision.

Consumer Fears

Many consumers are outraged by the subtle manipulation process that happens to them during direct marketing. Figure 2 on the next page reveals

how the percentage of people seeing computers as this kind of threat is rising (Katz 138). However, as can be seen by the charts, this is still not a universal belief. The complaint of many is that consumers do



not have a choice of which lists they are put on. That is, if they even know they are on a particular list and are being indirectly exploited. However, in business's point of view this has been going on for years.

A common practice for business survival is finding customers that will buy their product or service. Through the new advent of the computer, though, it seems these businesses have stepped over the line of just finding customers into destroying personal identity. Again, businesses are not interested in the consumer, but rather the consumer's buying habits. So what does the actual consumer become? He or she becomes an object of manipulation because of the new data gathering abilities of the information age. Thus, they too have become pawns in the game of big business because most of the time their being

manipulated they do not even know it.

Many direct marketing firms have become aware of the rising tide of privacy fears. They have also calculated the cost if they do not adhere to these fears. "We have to address consumer expectations and consumer concerns. Industry should be giving consumers more control before we get horribly restrictive legislation... (Fost 18)." Direct marketing companies have attempted to deter these fears by persuading consumers that their practice is beneficiary for both the companies and the end consumer. Their argument is that they can better serve customer needs if they have this personal information in the first place. However, the truth behind their enticement is that they are quietly and subtly raping individual identity and autonomy.

Lotus Development Corporation had plans to release on the market their compact-disk database called Lotus Marketplace: Households (Huber 136). This database included detailed profiles of the buying habits and life styles of 80 million U.S. households. It even provided categories such as "cautious young couple" or "intercity youth". Plus, it encompassed the power to identify and target an elderly, rich widow on Chicago's north side (Linowes 199). Thus, this would quickly enhance the abilities of today's direct marketers by developing these specific consumer lists. This information power would now

be accessible to anyone with a personal computer. However, specific lists like this have been available for years to large corporations. Marketplace would have just let anyone with the right PC to tap in. Recently, though, Lotus had to halt the whole program because of 30,000 letters of complaint from consumers about the invasion of their privacy (Schwartz 41).

False Claims By Businesses

The problem is that many businesses do not see these actions as a loss of privacy to the consumer. They feel the only thing consumers have to do is turn down their advertisements and the result is just junk mail. In fact, Alan Westin, a Columbia University law professor and privacy expert said, "Privacy advocates have been so busy fighting for privacy that they don't always realize that the most this will result in is an extra bit of junk mail (Seymour 89)." However, this is clearly not the only cost to the victims of direct mail. Mr. Westin may be only seeing the symptoms of the problem and not the ultimate sacrifice to the average American. In fact, a recent survey by Louis Harris and Associates revealed that approximately 30 percent of Americans do not apply for something like credit, insurance, or even a job because they are scared of the consequences of revealing personal information (Linowes 199). That sure

does not sound like "the land of the free and the home of the brave".

At the core of the new abilities given to direct marketers from technology is a stripping of human identity. This ultimate tool of control has tremendous power that people do not realize. "It's just a short step to 'behavioral manipulation,' says George B. Trubow, a privacy expert... (Rothfeder 76)."

Purchasing details have gotten to the point where marketers can predict when a consumer will need a certain product, like a pair of gym shoes. They know the date the consumer bought the shoes from a credit report. By taking the average time use of shoes, they can send the consumer advertisements at the precise time when they will be in need of another pair. Surfacing, is a reality where consumers are no longer making decisions for themselves, but organizations are making them for them. "In 1984, the George Orwell classic, *Big Brother* was a political dictator. In 21st century America, he may be a marketing whiz (Phillips 81)."

Some other incorrect assumptions by businesses include those that claim that the individual has control over this transferring of information about himself. They think all they have to do is just not give out this information. However, these people need to realize that intimate information is stored about them anytime they apply for school or a job, use a bank account, get a driver's

license or many other activities that Americans must do to live a normal life. These people need to face it, Americans are trapped and vulnerable to the information age. "There are avoidance schemes, such as guarding your Social Security number. But only one strategy really works: Pay cash. Avoid credit. Don't sign up for government programs. Walk, don't drive. Live under a rock. In short, for most ordinary people there is no way out (Phillips 81)."

Tangible Costs

Not only is the ultimate cost the loss of personal identity, but under certain circumstances, individuals can suffer tangible damage because of their appearance on certain mailing lists. For example, individuals listed as having rare coins or stamp collections may feel more vulnerable to burglary because of these lists. One security company even sent a form letter to 5,000 people on lists they believed to have art, gem or coin collections. In the letter, the company pointed out how vulnerable these people were to criminals because the thieves could easily buy these lists as well. Consequently, they tried to persuade these consumers to protect themselves by buying one of their security systems (Linowes 151). What has happened to America the Beautiful? Is this the kind of freedom that America's forefathers wrote of or is this just a

revelation of the subtle manipulation that goes on everyday because of these database lists? What is ironic is that these manipulation tactics and loss of identity are growing more fierce all the time and society is just letting it happen. Consequently, society as a whole may be the problem for their own loss of privacy and identity.

Society at Fault

The conflict between personal privacy and the freedom of information may be in the hands of society. Their hypocrisy is revealed because many consumer's beliefs and actions do not match. "In theory, Americans think modern technology is invading their privacy. In practice, many Americans don't hesitate to reveal detailed information about their shopping habits, personal lives, and finances - if they get something in return (Russell 2)".

It is evident that America's society as a whole is very individualistic. Therefore, they feel they have the right to be left alone and not have their personal information readily available to anyone who wants it. However, these same people readily share their information if it can somehow benefit them. In other words, what they say and do are totally opposite of each other. A recent survey points out this inconsistency within the American people. The survey concluded that Americans believe that their privacy is threatened by the advancements of the information age. Figure 3 on the next page represents individual categories of concern (Lacayo 36).

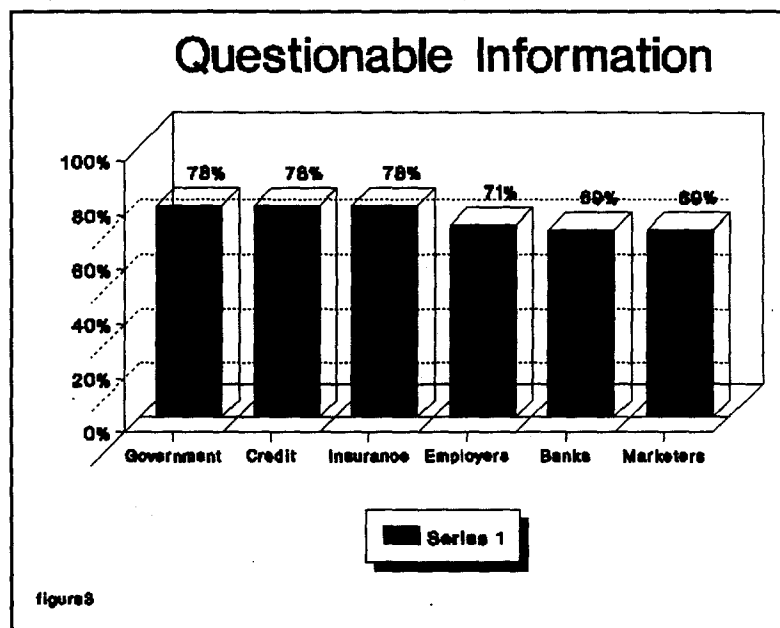
Ironcially, 78 percent of Americans would be upset if they could not get credit based on their previous credit history.

This is the exact percentage of people who said they thought credit companies were retrieving questionable information in Figure 3.

Similarly, about two-thirds oppose direct marketing

companies being able to buy their personal information, but almost the exact same percentage of people support the sale of lists containing the names and addresses of those who might want to receive information about a particular product (Wallich 27). As can be seen here, Americans want the best of both worlds.

Robert H. Courtney, a computer-security expert, discovered this phenomena some years ago. Then a manager at IBM, Courtney sent researchers out on a New York street to ask people passing by if they thought modern technology was invading privacy. Nearly 90 percent said they believed



this was true. However, the next day on the same street his group offered a credit card with a favorable interest rate. The application asked for a Social Security number, information about other credit cards, and bank-account numbers and balances. Ironically again, about 90 percent of the people filled out all the spaces of the application without hesitating (Rothfeder 82).

Sadly, Americans do not understand the power and freedom they are giving up when they release more intimate information about themselves. A temporal value of what they receive from the information age may be a little more convenience, but looking at the big picture, they are slowly giving up their privacy and identity and do not even know it. Plus, as a whole, society is following this pattern and are not comprehending the consequences of their actions. The ancient Chinese philosopher, Mencius, once noted,

"To act without clear understanding, to form habits without investigation, to follow a path all one's life without knowing where it really leads - such is the behavior of the multitudes (All Rapped Up)."

-Mencius

Unfortunately, this path leads to a society the resembles "Big Brother" in 1984.

Some people actually pay money to be on certain lists. The National Consumer Research of Fort Mitchell, Kentucky has introduced a household panel called the Saver Club. "Each household in the Saver Club pays \$199 for

the privilege of having its name, address, and buying habits bought and sold (Russell 2)".

The problem is that the best of both worlds does not exist. Frequently, a prerequisite of enjoying the benefits of new technology is giving up some personal privacy. Nevertheless, Americans do not want to believe this.

While the consumers of America do not have a solid view of where they want the line drawn between personal privacy and freedom of information, the stand of private business is clear. They definitely lean toward the freedom of information side because with more information they have more ability to target customers which ultimately will lead to higher potential of profits.

Consequently, it could be argued that consumers are losing their privacy and identity because their weak stand for it is being overpowered by business's hunger for it. In other words, private business may not be at fault here, but the actual hypocrisy of the people of the United States.

U.S. Government and Law

The idea of the right to privacy grounded in law is a relatively new one. Since privacy in the past was not seriously threatened by something like the computer, it was taken for granted and considered common, unwritten law that was based on custom and precedent. Recently, however, due to the power of the information age, Americans have been looking to Congress and the government to resolve the questions of privacy and identity that the information age has introduced. Ironically, the U.S. Government is the nation's largest data compiler. At last count, in 1982, it possessed more than 3.5 billion files on individual Americans, which has surely risen in the last decade. Plus, much of this data consists of hearsay, which obviously can be potentially damaging to individual rights if it fell into the wrong hands (Lacayo 39).

In the 1960s, the public and Congress were getting concerned about proposals for a centralized federal computer facility into which all agencies would dump their data. The idea generated such fears of "Big Brother" that the proposal was dropped. In response, Congress required the government to have

many different data bases, to make retrieval of information impractical and often impossible. Such fragmented information was "one of the most practical of our present safeguards of privacy (Marshall 35)". However, this protection is no longer pertinent simply because the power of the computer in the 1960s was not even a fraction of what it is today. As already mentioned, data can be transported and exchanged by hundreds of organizations in a matter of seconds.

Some experts think that laws essentially hold no deterrent in the information age. David F. Linowes, a University of Illinois professor and chairman of the 1977 U.S. Privacy Protection Commission stated, "Computers have outstripped our ability and that of our laws to safeguard privacy (Rothfeder 76)." As can be seen again, the rise in power of the computer has resulted in the loss of privacy to the average American. Plus, there are other characteristics of privacy that do not allow it to be protected faithfully.

Limiting Characteristics of Privacy

When considering how law can protect personal privacy, many limitations occur simply because of the nature of privacy in the first place. Because privacy is such an intangible right to protect, an overall privacy policy in the United States would be inapplicable. Therefore legislators must deal with

specific uses of information separately, which becomes very inefficient and hypocritical. Privacy also is very subjective and distinctive to many different cultures. "The subjective nature of an 'expectation' of privacy - an expectation that to a large extent is dependent upon social and technological change - is the major reason privacy-intrusion laws have been slow to develop (Marshall 42)".

In the U.S. today, people disagree about their expectations of privacy. Not only because they live in different subcultures, but technology is always changing before new standards of privacy can be established. As these changes in society and technology take place, so will society's expectation of privacy. "Since privacy is so subjective, it is not possible to come up with a single statute that will protect it, at least not without conflicting with other values our society has found equally as important, such as freedom of information (Marshall 42)." Other important issues, such as drug control, may also outweigh the efforts for privacy protection. Police officers are required to report any suspicions dealing with drug movement. If personal privacy is a cost of this, then that is no concern of the officers. Plus, mixed perspectives of what privacy should be have added to the dominating effects that the computer has had. "Into this volatile mix of half-formed attitudes and sharply felt anxieties, technology has arrived with a host of unprecedented temptations

(Lacayo 34)." This is why the credit agencies and direct marketers have been so successful in stripping the privacy of Americans.

Supporters of the information age claim that technology is not the villain, but it is the people who misuse that technology. While theoretically this may be correct, that does not change the fact that Americans are losing their autonomy. It is true that privacy is not a "computer problem", it is a human and societal one (Seymour 89). However, the current medium that is being used to expound these societal problems is the computer and related technology. In addition, America has become so totally dependent on the computer for its processing power, businesses and other organizations cannot survive without technology anymore. This reliance promotes a vulnerability which can no longer separate societal problems from the computer. Instead, the computer explodes these societal problems into bigger ones than if they were not dependent on the computer. Unfortunately, law does not have a dominant effect on a society that is susceptible to the computer.

While laws take so long to get passed and enforced, the end result is an abundance of U.S. laws that are so filled with loopholes that they offer no deterrent to the power of the computer. "Changes in technology are making our information dissemination laws obsolete. Most of our statutes were written

in an era when all information was on paper. Today, more information is kept in electronic formats, and this raises new problems that existing laws do not resolve (McMasters 19)". Thus, the information age triumphs over law as well. This can be proven by revealing how some privacy and information laws that currently exist are narrow and have numerous holes in them because they have been twisted and distorted by the omnipotent computer.

Fair Credit Reporting Act of 1970

The Fair Credit Reporting Act of 1970 is a perfect example of this. At face value, it seems quite potent. It gives an individual the right to see and correct his or her credit reports and limits the rights of others to look at them. This Act seems like a good solution to the privacy problem of data sharing in the credit industry. However, this is before the exceptions to the Act are considered.

The biggest one of these exceptions is that credit agencies can share this information with anyone with a "legitimate business need" for these credit records (Miller 42). What weight does this Act hold then? Who does it actually bar from this personal information? Certainly it does not prohibit the direct marketers, mortgage lenders, employers and other crucial institutions in

America. They have a "legitimate business need" for this information. In fact, many of these firms depend on this information for higher rates of return.

These are the same organizations that have initiated this conflict of privacy loss in the first place. Consequently, this Act becomes irrelevant and insignificant in the search for the protection of personal privacy for Americans.

Privacy Act of 1974

In 1974, Congress passed the Privacy Act which was supposed to be the most significant law protecting privacy ever. It was instituted because of the Watergate controversies. A solid law was definitely needed now because the public had become quite aware of the threat to their privacy because of Watergate. This Act was supposed to bar federal agencies from sharing information on U.S. citizens. It also prohibited these agencies from using data for a different purpose than it was originally collected for. However, this Act has a significant exception as well.

It is legal under this Act to share information if the second use of it is consistent with the purpose it was originally compiled for. For instance, the Health, Education and Welfare agency stretched this exception by saying that they need to see federal payroll records so that they can root out welfare

cheaters. Their reasoning is that efficiency is the goal of all federal agencies. Therefore, their need for these payroll records is justified because it agrees with its original intention for collection, which they claim is efficiency (Rothfeder 77).

The problem is that this manipulation of purpose is so frequent that the original intention for collecting the data becomes so watered down that it enables numerous institutions to gather this federal information. As a result, this results in another Act with many loopholes that in the end does not protect the privacy of the individual, but rather adheres to the motives of organizations. Again, these Acts are to give more power and protection to the average American. However, because of their deficiency and the elusive traits of the information age, the power of the government and private organizations is multiplying.

Computer Matching and Privacy Protection Act of 1988

The Computer Matching and Privacy Protection Act of 1988 provides considerable protection of the matching of federal data to data from private institutions. For example, this would again attempt to deter the government from matching payroll records with welfare files. "That might seem justifiable

in a time of tight budgets, but the precedent it set for going around the law could encourage more ominous practices, such as using the records of people in drug-treatment programs to search for possible criminals (Lacayo 40)." It also requires the government to give individuals a chance to reply before taking adverse action. Once again, however, this Act has two major holes in it.

First of all, the Act leaves many potential matches unaffected, such as those done for law enforcement and tax purposes. Plus, a bigger problem is that this Act only applies to federal agencies. The states also maintain databases and conduct the same type of matching programs. "In many respects, the personal information gathered by state agencies is more sensitive than that gathered by federal agencies (Marshall 37)." This is easy to see when the types of information that is gathered and matched is examined.

This kind of touchy, personal information includes tax and driving records, drug and alcohol treatment records, communicable disease and abortion data, treatment records at state institutions, criminal files, educational and vocational training records, licensing (attorneys, beauticians, etc.) information, Medicaid records, reported suspicions of child abuse and adoption records. With this kind of information out, average Americans are quite vulnerable to state agencies. Another danger to this is that state laws pertaining

to this information is far from uniform. See Appendix A (Marshall 36). This is significant when "state governments and the private sector hold the vast bulk of personal information concerning the residents of this country (Marshall 37)."

Video Privacy Protection Act of 1988

Quite possibly, the Act that produces the most protection is the Video Privacy Protection Act of 1988. This Act was instituted because a major newspaper in Washington D.C. published a list of videotape titles that were borrowed by Robert H. Bork, then a U.S. Supreme Court nominee (Rothfeder 77). Called the Bork Bill, it bars retailers from selling or disclosing video rental records without first getting the permission from the consumer. While this is somewhat of a breakthrough, it seems kind of ironic why there is protection of video rental records while more critical records such as medical and insurance records remain unprotected. This is a fine example to see what the computer and related technology has done to the American law system. Inconsistencies have become the norm. With these inconsistencies and the numerous exceptions to these Acts, it becomes evident that law cannot adapt to the changes in the American societal system that the computer has created. What is even more intimidating is the fact that not even the Constitution can

combat the computer. Unless America wakes up and realizes what is going on, even the principles and foundations of morality that America's forefathers laid down in that document over two centuries ago will become powerless and even moot to the immeasurable strength of the information age.

institutions know where the American society has drawn this "expectation of privacy"? It has also been concluded that because technology is always changing this "expectation" and because there are so many subcultures in the U.S., it becomes impossible to measure this "expectation of privacy". As can be seen, however, this is only a symptom of the core problem of the adaptability of the U.S. Constitution.

Limiting Traits of the Constitution

The United States Constitution was obviously written at a time where computers did not exist. Therefore, a distinct characteristic of this document was that it was written for those things which could be measured or comprehended in the physical by any human being. It was written when the United States was not dependent on the computer, but rather human understanding. Consequently, it was simple and direct in nature and the principles it conveyed were easy to perceive. However, the computer has destroyed this simplicity.

For example, before the computer it was easy to put a patent on an invention because it was a tangible object that no one could copy. If someone did, it would be simple to detect and corrective action could be taken. As a

result, protection of that American right was clearly secured. However, with the discovery of the computer this becomes an intricate process that is so complex it is often a hopeless goal.

How can there be a patent on an idea? Since the majority of ideas today never take physical form because of the computer, how can that property be protected by a patent? This becomes complex because deprivation is the essence of theft. However, with the computer, deprivation does not occur because the idea is just transmitted from computer to computer while the actual owner never loses anything. This is just one case on how the computer has changed the way the Constitution applies to society.

The question that can be raised from this problem can be horrifying. When the lines along which the Constitution were drawn up become warped or even vanished, what happens to the credibility of the Constitution itself? Is there law and liberty beyond the computer frontier?

Pass the Principle, Not Just the Words

The bottom-line problem with the manipulation that is going on with the Constitution is that people are allowing new technologies to twist and bend the words of the document until the meaning is totally lost. The key obstacle is

that it seems people are so fixed on the words of the Constitution that they forget the principles that are behind those words. These are the same principles that set the foundation for law and liberty in the United States in the first place. The call for these core values is essential and easy to see why they are needed. "The Constitution's architecture can easily come to seem quaintly irrelevant - or at least impossible to take very seriously - in the world as reconstituted by the microchip (Tribe 17)."

Make no mistake, however, the framers of the Constitution were very discerning. They completed a framework for all seasons, one whose principles are for all technological advances. However, that is the key. Only the principles can be passed on, not just the words of those principles.

This concept is much like parenting. For a child to gain true understanding, parents must effectively pass on to them principles and not just words. If children just hear what their parents communicate in words and do not actually comprehend why they are following those words, then they become like a robot. However, if their parents can effectively pass on the principles of morality, then these principles will be able to adapt and adjust to the many changes in the child's life. Placing a moral foundation on mere words would be disastrous because as soon as the words do not apply to a given conflict in

life, that same child will begin to twist those words to make them say whatever he wants them to.

This may be the state of which the Constitution is in. American morality cannot adapt to the information age because the principles of the Constitution have been forgotten. As a result, the mere words of the Constitution have no stand against something so life-changing as the computer. This is exactly why the information age has stripped the American society of privacy and other liberties. It is because words cannot deter the raw power of the computer. The only combat that the document has is the principles that make up its foundation. Nevertheless, the United States is forgetting the principles and morality that it once stood on and is now twisting the Constitution to say whatever they want to.

This goes back to what Mencius, the ancient Chinese philosopher, said about the multitudes of people. They are following a way in which they do not know where they are going. Unfortunately, the consequence of their not knowing where they are going is resulting in the government and private institutions leading them in a way that they want them to go. Thus, the individual loses not only his or her privacy and identity, but the American society becomes an image of 1984, which is total control of the people by the

government and organizations. The only difference from Orwell's "Big Brother" is that the American people are deceived and actually think they are in power because that is what the "words" of the Constitution tells them.

The Future

The future does not hold much hope for the restoration of America's personal privacy and individual autonomy. Newer and more powerful forms of technology have yet to be introduced. While these inventions and advances may claim to enhance the quality of life, the truth is that privacy and personal identity will be even more endangered. "Americans seem to have opted against privacy even in trivial matters: coinless telephones in the U.S., for example, rely on credit cards and a centralized database (Wallich 27)." Thus, information about who Americans are talking to, and how long, is now becoming available to organizations.

Electronic highway toll booths are now being tested in several cities to take the same approach as the coinless telephone system. These systems would record the identity of all cars passing through them and then just send the individual a monthly bill. Therefore, these same organizations will know where an individual travels and how often. Farther into the future, some experts say America may become a cashless society. It is immeasurable how much personal information the government and private institutions will know about Americans then. Whether Americans want to believe it or not, they will have

to pay the price for any conveniences they attain by new inventions of the information age.

"To achieve the proper balance between societal and individual rights will become increasingly challenging (Stephens 25)". Because there is such a disagreement among society about where Americans should "expect" privacy, it is clear that these values will continue to be lost. Plus, once privacy is gone, it is very difficult to restore. Already there are inventions or discoveries that will challenge and stretch American society's value of privacy and freedom.

Genetic Discrimination

One of these advances in technology could totally devastate a person's life even before they are born. Genetic engineers are becoming more successful in reading the blueprints of life that contain the specific heredity of every human being. Currently, researchers have only identified about 3,000 of the estimated 100,000 genes that compose human DNA (Gruson B6).

However, these genes alert researchers of those patients that may be more susceptible to cancer, arthritis or approximately 4,000 other heredity illnesses simply because of their genetic makeup. Considering that there is no current protection of medical or insurance records, a person's life may be completely

altered before they can even talk.

Since records travel so quickly, he or she may never be granted their presumed rights as an American. Prospective employers, insurance companies, the military or even possible spouses may have access to this information. This means that this individual may have great difficulty finding a job or spouse, will not be eligible for the military and will be paying an excessively high insurance rate for his entire life, if he can find an insurance company that will give coverage. Consequently, a person's destiny can live and die with medical technology. This certainly does not sound like the fundamental ideals of fairness, equality and privacy that every United States citizen is supposed to be born with. That is because these kind of ideals have become lost in the information age.

Experts who follow the issue say that these techniques are becoming more common and less expensive all the time. Already, five percent of the Fortune 500 companies use genetic profiling for screening employees, while 55 more companies say they might start using these tests by 1994. Plus, in a recent two year span, an informal study in San Francisco found 50 cases in which people were denied jobs, insurance claims or other benefits simply because of their genes (Gruson B6).

To confront this privacy loss, only four states have passed laws to prohibit employers from discriminating on the basis of genetic information. However, three of the four states only include the disease of sickle-cell anemia, while all of them only prevent prospective employers and not insurance companies or other agencies from using this information. This not only proves that law follows technology by a long way, but it asks the central question of the entire analysis of the information age. Is technological and computerized advancements worth the loss of human liberty? A look farther into the future asks this question even more boldly.

Information Age May Even Threaten Thoughts

Possibly the ultimate threat to privacy and identity may yet to be seen. Researchers are considering the possibility of transferring RNA memory molecules from one individual to another or from the stored memory molecules of the deceased. This could be used against a murderer if the victim was killed during a crime (Stephens 24). However, what incredible threat does this entail? Will the information age actually diminish the American society's "expectation of privacy" to the point where they cannot even think without the fear of someone finding out about it? Even Big Brother could not read the public's

thoughts. This idea may seem preposterous now, but think of how much privacy expectations have dwindled in the last forty years. Society in the 1950s would have thought it was ridiculous to think that the government and private organizations would know such intimate details about them that they would be able to exploit them in numerous ways.

As a result, who knows what privacy will actually encompass in the 21st century? If society continues to indulge in the temporal values of the information age, the United States may become an intensified vision of 1984. Ironically, society may still be blinded and praising technology by claiming that it enhances the value of life, when the fact is that they will have no clue of what true freedom really is.

Conclusion

"In itself the computer poses no threat to our liberties or our privacy: but, like a gun or a motor-car, it can be the very devil of a threat in the wrong hands. The challenge of the computer is, therefore, an old one revived in a technological guise - how to safeguard human rights and fundamental freedoms when a new invention arises which is full of promise for mankind but can, if abused, do great harm (Sieghart vii)."

The information age has redefined terms that have been part of American heritage since its founding. Terms like freedom, independence, autonomy and free-will have been so watered down that Americans may not even know what these words originally meant. In return, the information age has supplied generic terms for what these definitions of freedom are. It is selling Americans new "freedoms" that actually take away the truth of what freedom is. In fact, it is to the point where "America is so 'free' that they are in bondage."

Perhaps the loss of power to the individual and increase in power of the government and institutions is a inevitable last step in any civilization. Maybe the Roman and Egyptian empires actually fell because they lost contact with the

fact that a nation is built on the principles and morality created and maintained by its people. Surely, the Soviet empire forgot the precious collection of its people and it collapsed too. Now they are probably wondering why the United States, who fought for years against governmental and institutional control, are pointing the finger at other nations while the information age creates this type of society in the U.S. Perhaps Orwell's novel was not just a prophecy of America's future but rather a prophecy for any nation who promotes the nation as a whole while neglecting the individuals who make up that country.

The key problem is that many Americans people do not see this deterioration of freedom. They are so engulfed in the temporal conveniences of the information age, that they do not see the cost of it. One of America's forefathers voiced the danger of this even back in 1788:

"There are more instances of the abridgement of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations (Linowes 169)."

-James Madison

Sadly, the devastation of this subtle loss of humanity that Madison is referring to here is the same effect that a nuclear war might have. "The alarm is raised here that while we are only too aware now of the danger of losing everything in a nuclear holocaust, there is also the danger of losing it all in the green glow

from a little phosphor screen (Burnham viii)."

Another scary thought of this information age is that there may be no turning back on the path that Americans have already chosen. "Any attempt by the government to restrain this electronic revolution... is to ensure that other nations will take the lead in shaping the future (Hamilton 958)." The future may not look too bright anyway simply because the walls of privacy and humanity that America's forefathers built for years is now being quickly destroyed by the almighty computer.

Orwell may have said it best himself. "I do not believe that the kind of society I describe necessarily will arrive, but I believe... that something resembling it could arrive (Burnham 226)." Unfortunately, Mr. Orwell, the day of resemblance has arrived, and the possibilities for the future could take America far beyond the horror of 1984.

Bibliography

All Rapped Up. Videocassette. Reel to Reel Ministries: 1991.

Branwyn, Gareth. "Computers, Crime and the Law." The Futurist, September- October, 1990 v24 n5, page 48.

Burnham, David. The Rise of the Computer State. New York: Random House, 1983.

Dejoie, Roy. Ethical Issues in Information Systems. Boston: Boyd and Fraser Publishing Company, 1991.

Department of Communications/Department of Justice. Privacy and Computers. Ottawa, Canada: Crown Copyrights, 1970.

Fost, Dan. "Privacy Concerns Threaten Database Marketing." American Demographics, May, 1990 v12 n5, pages 18-20.

Gruson, Lindsey. "Gains In Deciphering Genes Set Off Effort to Guard Data Against Abuses." New York Times, April 22, 1992 v141, page B6(N).

Hamilton, David P. "Information Decontrol Urged." Science, May 25, 1990 v248 n4958, pages 957-958.

Hoffman, Lance J. Computers and Privacy in the Next Decade. New York: Academic Press, 1980.

Huber, Peter. "Good Tidings From Lotus Development." Forbes, December 24, 1990 v146 n14, page 136.

Katz, James E. "Public Opinion Trends: Privacy and Information Technology." Public Opinion Quarterly, Spring, 1990 v54 n1, pages 125-143.

- Lacayo, Richard. "Nowhere to Hide: Using Computers, High-Tech Gadgets and Mountains of Data, an Army of Snoops Is Assaulting Our Privacy." Time, November 11, 1991 v138 n19, pages 34-40.
- Linowes, David F. "Changing Customer Concerns in the 1990's: the Privacy Issue." Vital Speeches, January 15, 1992 v58 n7, pages 198-200.
- Linowes, David F. Privacy in America: Is Your Private Life in the Public Eye? Chicago: University of Illinois Press, 1989.
- Marshall, Patrick G. "Your Right to Privacy." Editorial Research Reports, January 20, 1989 v1 n3, pages 30-42.
- McMasters, Paul. "Rights In Conflict: Access Vs. Privacy." The Quill, June, 1989 v77 n6, page 19.
- Miller, Annetta. "Would New Laws Fix the Privacy Mess?" Newsweek, June 3, 1991 v177 n22, page 42.
- Newfeldt, Victoria. Webster's New World Dictionary, Third College Edition. New York: Webster's New World Dictionaries, 1988.
- Phillips, Stephen. "Never Mind Your Number - They've Got Your Name." Business Week, September 4, 1989 n3122, page 81.
- "Postal Service Criticized For Giving Companies Access to Addresses." New York Times, May 14, 1992 v141, page A17(L).
- "Provide Information Cautiously." USA Today (Magazine), April, 1992 v120 n2563, page 11.
- Rothfeder, Jeffrey. "Is Nothing Private?" Business Week, September 4, 1989 n3122, pages 74-82.
- Rule, James B. "Where Does It End? The Public Invasion of Privacy." Commonweal, February 14, 1992 v119 n3, pages 14-16.
- Russell, Cheryl. "Kiss and Tell." American Demographics, December, 1989

v11 n12, page 2.

Schwartz, John. "How Did They Get My Name: Consumers Are Growing More Uneasy About Threats to Privacy - and Are Fighting Back." Newsweek, June 3, 1991 v117 n22, pages 40-42.

Seymour, Jim. "PCs and Privacy Issues." PC Magazine, August, 1991 v10 n14, pages 89-90.

Sieghart, Paul. Privacy and Computers. London: Latimer New Dimensions Limited, 1976.

Stephens, Gene. "High-Tech Crime Fighting: the Threat to Civil Liberties." The Futurist, July-August, 1990 v24 n4, pages 20-25.

Thompson, Daniel. Big Brother in Britain. New York: Prentice Hall Publishing Company, 1981.

Tribe, Laurence. "The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier." The Humanist, September-October, 1991 v51 n5 pages 15-22.

Wallich, Paul. "Of Two Minds About Privacy." Scientific American, June, 1991 v264 n6, page 27.

APPENDIX

State Privacy Laws

This chart shows which states have laws to protect the confidentiality of personal information contained in various records and data bases. The scope and effectiveness of these statutes may vary widely from state to state.

State	Arrest records	Bank records	Computer crime	Credit reporting and investigation	Criminal justice information systems	Data banks in government	Employment records	Insurance	Mailing lists	Privacy statutes/ state constitutions	School records	Social security numbers	Tax records	Testing in employment	Wiretaps
Alabama	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Alaska	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Arizona	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Arkansas	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
California	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Colorado	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Connecticut	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Delaware	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
District of Columbia	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Florida	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Georgia	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Hawaii	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Idaho	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Illinois	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Indiana	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Iowa	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Kansas	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Kentucky	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Louisiana	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Maine	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Maryland	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Massachusetts	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Michigan	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Minnesota	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Mississippi	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Missouri	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Montana	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Nebraska	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Nevada	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
New Hampshire	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
New Jersey	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
New Mexico	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
New York	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
North Carolina	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
North Dakota	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Ohio	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Oklahoma	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Oregon	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Pennsylvania	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Rhode Island	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
South Carolina	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
South Dakota	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Tennessee	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Texas	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Utah	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Vermont	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Virginia	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Washington	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
West Virginia	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Wisconsin	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/
Wyoming	/	/	/	/	/	/	/	/	/	/	/	/	/	/	/

† Fair Information Practices Acts.

‡ Significant court decision affecting privacy.

SOURCE: Compilation of State and Federal Privacy Laws, 1988.