Privacy 2000

Introduction

Privacy is something I believe we all take for granted until we lose it. Then we begin to think about how someone invaded our privacy, often by incremental steps. In this article we are going to discuss ways in which we have lost our privacy. Most of the intrusions into our lives come from government, but not all. Businesses also buy and sell information about us every day. Most of us would be shocked to find out how much personal information is in databases around the country.

As we cover this important issue of privacy and focus on a specific threats to our privacy I want to begin by highlighting how quickly our privacy is being lost and how often it takes place without any debate.

Let's look at the last few years of congressional debate. It's amazing to me that there never was an extended debate on the issue of privacy. Granted there wasn't a lot of debate on a number of issues, but the lack of debate on this fundamental issue shows how far down the road we have gone. Let's look at a few of these issues.

For example, we saw absolutely no debate on issues such as the national ID card, the medical ID number, the administration's encryption policy, and the expansion of the FBI's wiretap capability.

Some of the proposals were defeated, at least for now. The national ID card was defeated, for example, not because Congress debated the issue, but because thousands of Americans wrote letters and made phone calls. Most other issues, however, are moving ahead. Congress gave the FBI permission to use "roving wiretap surveillance." That means that the next time you use a pay phone at your local grocery store, it may be tapped merely because there’s a criminal suspect within the area. One wiretap order in California authorized surveillance on 350 phones for over two years. In another case, five pay phones were tapped, intercepting 131,000 conversations.

Those are just a few of the examples we will discuss on the subject of privacy. Unfortunately whenever someone cries for privacy, another is sure to ask, “What do you have to hide?” The question confuses privacy and secrecy. I don’t really have anything I want to keep secret, but I’m not too excited about the government listening to every one of my phone conversations. You may not want your future boss to know that you have a genetic predisposition to breast cancer. You may not want a telemarketer to know what you just recently purchased so that he can call your home number and try to sell you more. The point is that each day we are losing a bit of our privacy. And we will continue to do so unless we work to establish some limits to this invasion of our privacy.

National ID Card

Issuing internal passports has been one of the methods used by communist leaders to control their people. Citizens had to carry these passports at all times and had to present them to authorities if they wanted to travel within the country, live in another part of the country, or apply for a job.

A few years ago, the Department of Transportation called for the establishment of a national ID system by October, 2000. Although presented as merely a move toward standardization, this seemed to many as a move toward a national passport to allow the government to “check up” on its citizens.

A little history is in order. Back in 1996, Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act. This charged the federal Department of Transportation with establishing national requirements for birth certificates and driver’s licenses. Add to this the 1996 Kennedy-Kassebaum health-care law that implies that Americans may be required in the future to produce a state- issued ID that conforms to federal specifications.

If all of this sounds to you like Big Brother or even the mark of the beast, then you have company. Congressman Ron Paul believes that the Department of Transportation regulations would adversely affect Americans and fought to end these regulations.

The law ordered the Attorney General to conduct pilot programs where the state driver's license includes a "machine-readable" social security number. It also ordered the development of a social security card that uses magnetic strips, holograms, and integrated circuits.

The good news is that the work by Congressmen Ron Paul and Bob Barr paid off and the attempt to create a national ID card was stopped, for now. But it is likely to surface again. After all there has been a push to establish a federal database for Americans and having each person carry an ID card would allow that information to be linked to a federal database. And while it would help the government catch illegal aliens, it could also be used to track law-abiding American citizens.

Tracking down illegal aliens and standardizing licenses are worthy goals. But the ends do not justify the means. That is why so many people wrote Congress to stop this push for a national ID card. Sometimes in the midst of this political debate, citizens must ask themselves how much they value their freedom and privacy.

Congressman Bob Barr says, "Novelists Aldous Huxley and George Orwell have given us countless reasons why we shouldn't trade our privacy for any benefit, no matter how worthwhile it sounds." In the end, we must ask, At what cost? Is it worth trading our privacy for the benefits government promises? The answer is no, and that's why we need to pay attention to governmental attempts to invade our privacy.

Carnivore

We’ve talked about attempts to establish a national ID card and attempts to expand wiretaps. Another threat to privacy is Carnivore, the FBI’s newest electronic snooping device that can read your e-mail right off your mail server.

Packed in a slim laptop computer, this program looks downright docile, but privacy advocates believe that it is quite dangerous. This automated system to wiretap the Internet is called Carnivore because it rapidly finds the “meat” in vast amounts of data. The programmers devised a “packet sniffer” system that can analyze packets of data flowing through computer networks to determine whether it is part of an e-mail message or some other piece of Web traffic.

The FBI has been quietly monitoring e-mail for about a year. Finally the bureau went public with their operation to what the *Wall Street Journal* called “a roomful of astonished industry specialists.” Although the device has been used in less than 100 cases, there is every reason to believe that it will be expanded. A judge can issue a court order to tap your e-mail just as they tap your phones.

In this electronic age, new devices threaten our privacy. And in this current political climate, administration officials seem to have little concern about threats to our Fourth Amendment rights. Critics argue that Carnivore, like some ravenous beast, will be too hungry to be trusted. But the FBI says that this new device can be tailored to distinguish between packets of information and only grab e-mails from the suspect. Carnivore appears to be more discriminating than a standard telephone wire tap. The FBI says that messages belonging to those not being probed (even if criminal) would not be admissible in court. Perhaps that is true, but privacy advocates wonder how this new device will be used in the future.

Carnivore is nothing more than a standard computer with special software. The computer is kept in a locked cage for about a month and a half. Every day an agent comes by and retrieves the previous day’s e-mail sent to or by someone suspected of a crime. But it can also capture file downloads and chat room conversations. And once it is installed, the FBI can dial into Carnivore to make changes and monitor data that have been collected.

Critics are concerned that Carnivore will soon become a hungry beast, ready to devour personal and confidential information in people’s e-mail messages. The FBI says that won’t happen, but such assurances do nothing to mollify the critics. Maybe Carnivore will never tap into your e-mails, but its existence is just one more good reason why we should be careful about what we put in our e- mails.

Encryption

The privacy threats surrounding today’s technology are numerous, and I want to turn to computers and talk about another important issue: encryption. Now I know that’s probably an unfamiliar word. But stay with me. Encryption is big word for a big issue that I think you need to know about.

Encryption is a relatively new technology that enables you to have private phone conversations and send e-mail messages that are secure. Encryption codes your words so that they cannot be deciphered by people listening in on your conversation or reading your mail.

As you may know, nosy people already can listen in on your wireless phone calls (cellular or cordless phones). And they can intercept and read your e-mail. Sending e-mail without encryption is like mailing a postcard—everyone can read it along the way. And we all know that people will do exactly that. If you have ever had a phone on a party line, you know that people listen in.

What you may not know is that various branches of the government are demanding the authority to read encrypted messages. Now remember that the Fourth Amendment guarantees citizens be free of unreasonable searches and seizures. Nevertheless, these and other law enforcement officers believe they have the right to open your mail.

What they are asking for is the key to the code. When you send a message in code, you need a key to enable you to send the code and the recipients need the same key to read the code. The Clinton administration is demanding access to all encryption keys. This is like giving the government the power to steam open all the letters we send in the mail. Frankly you only see this level of surveillance in totalitarian countries. If government has the key, then it could call up information on you, your family, your medical records, your bank records, your credit card purchases, and your e- mail messages to all of your friends and relatives.

What is even more disturbing is the current attempt by government to limit American citizen's access to strong and power encryption software. A new study from the Cato Institute says that "People living outside the United States find it amusing and perplexing that U.S. law regulates the distribution of strong encryption."

Everyone wants encryption in the computer age. Citizens want private communication. Businesses want to prevent billing records and personnel records from falling in the wrong hands. Consumers don't want their credit card numbers widely distributed. That is why we need strong encryption software, and that is why government should not be given a key to the messages we send. Most Americans would not like to turn over so much of their privacy to the government, but unfortunately most Americans don't realize that they already have.

Privacy and Your Life

We have been talking about the threats to our privacy through wiretaps of our phones and e-mail correspondence, as well as through the issuing of a national ID number. Common citizens are having their privacy violated in new and unexpected ways.

Such is life in the cyberage. As more and more people are seeing their privacy violated, they wonder what to do in a time of financial and personal indecent exposure. What used to be called public records weren't all that public. Now they are all too public. And what used to be considered private records are being made public at an alarming rate. What should we do?

First, don't give out personal information. You should assume that any information that you do give out will end up on a database somewhere. Phone solicitors, application forms, warranty cards all ask for information you may not want to give out. Be careful how much information you disclose.

Second, live your life above reproach. Philippians 2:14-15 says "Do all things without grumbling or disputing, that you may prove yourselves to be blameless and innocent, children of God above reproach in the midst of a crooked and perverse generation, among whom you appear as lights in the world." 1 Timothy 3:2 says that an elder must be "above reproach" which is an attribute that should describe all of us. If you live a life of integrity, you don't have to be so concerned about what may be made public.

Third, exercise discretion, especially when you use e-mail. Too many people assume they have a one-on-one relationship with someone through the Internet. The message you send might be forwarded on to other people, and the message may even be read by other nosy people. One Web site provider says, "A good rule of thumb: Don't send any e-mail that you wouldn't want your mother to read."

Finally, get involved. When you feel your privacy has been violated, take the time to complain. Let the person or organization know your concerns. Many people fail to apply the same rules of privacy and confidentiality on a computer that they do in real life. Your complaint might change a behavior and have a positive effect.

Track congressional legislation and write letters. Many of the threats to privacy I've covered started in Congress. Citizens need to understand that many governmental policies pose a threat to our privacy. Bureaucrats and legislators are in the business of collecting information and will continue to do so unless we set appropriate limits.

Sadly most Americans are unaware of the growing threats to their privacy posed by government and private industry. Eternal vigilance is the price of freedom. We must continue to monitor the threats to our privacy both in the public and private sector.

Privacy Issues

The Need to Discuss Privacy Issues

Privacy is something I believe we all take for granted until we lose it. Then we begin to think about how someone invaded our privacy, often by incremental steps. In this article we are going to talk about ways in which we have lost our privacy. Most of the intrusion into our lives comes from government, but not all. Businesses also buy and sell information about us every day. Most of us would be shocked to find out how much personal information is in databases around the country.

As I address this important issue, I will focus on several specific threats to our privacy. I want to begin, though, by discussing how quickly our privacy is being lost and how often it takes place without any debate.

Let’s look at the last session in Congress. It’s amazing to me that there never was an extended debate on the issue of privacy. Granted there wasn’t much debate on a number of issues, but the lack of debate on this fundamental issue shows how far down the road we have gone.

For example, we saw absolutely no debate on issues such as the national ID card, the medical ID number, the Clinton administration encryption policy, the expansion of the FBI’s wiretap capability, along with the Clinton administration’s Executive Order authority and federal databases.

Some of the proposals were defeated, at least for now. The national ID card was defeated, for example, not because Congress debated the issue, but because thousands of Americans wrote letters and made phone calls. Meanwhile, plans by the Clinton administration to develop a medical ID number are on hold, but could surface at any time.

Most other issues, however, are moving ahead. Congress gave the FBI permission to use “roving wiretap surveillance.” That means that the next time you use a pay phone at your local grocery store, it may be tapped merely because there’s a criminal suspect within the area. And if you think I am overreacting, look at what has already happened in California. One wiretap order there authorized surveillance on 350 phones for over two years. In another case, five pay phones were tapped, intercepting 131,000 conversations.

Recently, the Federal Communications Commission mandated that cell phones and other wireless telephone companies track the location of the customers from the time the call was initiated until the time it was terminated. By locating the cell site the person was using, the government can pinpoint the location of every citizen who uses a cell phone since the telephone companies must track and log the locations.

Those are just a few of the examples we will discuss on the subject of privacy. Unfortunately, whenever someone cries for privacy, another is sure to ask, “What do you have to hide?” The question confuses privacy and secrecy. I don’t really have anything I want to keep secret, but I’m not terribly excited about the government listening to every one of my phone conversations. You may not want your future boss to know that you have a genetic predisposition to breast cancer. You may not want a telemarketer to know what you just recently purchased so that he can call your home number and try to sell you more.

The point is that each day we are losing a bit of our privacy. And we will continue to do so unless we work to establish some limits to these invasions of our privacy.

National ID Card

Issuing internal passports has been one of the methods used by communist leaders to control their people. Citizens had to carry these passports at all times and had to present them to authorities if they wanted to travel within the country, live in another part of the country, or apply for a job.

The Department of Transportation has recently called for the establishment of a national ID system by the first of October, in the year 2000. Although presented as merely a move toward standardization, this seemed to many as a move toward a national passport to allow the government to “check up” on its citizens.

A little history is in order. Back in 1996, Congress passed the Illegal Immigration Reform and Immigrant Responsibility Act. This charged the federal Department of Transportation with establishing national requirements for birth certificates and drivers' licenses. Add to this the 1996 Kennedy-Kassebaum health care law that implies that Americans may be required in the future to produce a state-issued ID that conforms to federal specifications.

If all of this sounds to you like Big Brother or even the mark of the beast, then you have company. Congressman Ron Paul believes that the Department of Transportation regulations would adversely affect Americans. He says, "Under the current state of the law, the citizens of states which have drivers' licenses that do not conform to the federal standards by October 1, 2000, will find themselves essentially stripped of their ability to participate in life as we know it."

Congressman Paul adds that, "On that date, Americans will not be able to get a job, open a bank account, apply for Social Security or Medicare, exercise their Second Amendment rights, or even take an airplane flight, unless they can produce a state-issued ID that conforms to the federal specifications."

The law orders the Attorney General to conduct pilot programs where the state driver's license includes a "machine-readable" Social Security number. It also orders the development of a Social Security card that uses magnetic strips, holograms, and integrated circuits. The law also requires that states collect Social Security numbers from all applicants for various licenses. It requires states to transmit the name, address, and Social Security number of every new worker to a Directory of New Hires.

The good news is that the work by Congressmen Ron Paul and Bob Barr paid off and the attempt to create a national ID card was stopped, for now. But it is likely to surface again.

After all, there has been a push to establish a federal database for Americans and having each person carry an ID card would allow that information to be linked to a federal database. And while it would help the government catch illegal aliens, it could also be used to track law-abiding American citizens.

Tracking down illegal aliens and standardizing licenses are worthy goals. But the ends do not justify the means. That is why so many people wrote Congress to stop this push for a national ID card. Sometimes in the midst of this political debate, citizens must determine how much they value their freedom and privacy.

Congressman Bob Barr says, “Novelists Aldous Huxley and George Orwell have given us countless reasons why we shouldn’t trade our privacy for any benefit, no matter how worthwhile it sounds.” In the end, we must ask, At what cost? Is it worth trading our privacy for the benefits government promises?

Medical ID Number

While the Department of Transportation is moving ahead with plans for a national ID card, the Department of Health and Human Services is working to assign everyone a lifetime medical ID number.

The purpose of the ID number is to make it easier to keep accurate records of patients as they change doctors and health plans. The identification was required in a 1996 law that guarantees workers continued access to health coverage even if they change jobs.

One solution proposed is to merely use Social Security numbers. But doing that could give credit card companies and other organizations access to medical records. This would raise a greater concern over privacy of medical records. And that’s the point. Even a secure number still could pose a privacy nightmare by potentially giving everyone from insurance companies to computer hackers access to medical histories.

One doctor expressed his concern that a “unique patient identifier could lead to a central database.” He fears that “someone without permission could break into those records.” But even if the record is secure, doctors fear that patients will withhold embarrassing information if there is a chance someone else might get access to the records.

Robert Gellman, an information policy consultant said at a recent hearing, “Once everyone’s required to use a government-issued health identification card, it may become impossible for any American citizen to walk down the street without being forced to produce that card on demand by a policeman.”

Why are so many people concerned? Perhaps past history is an indication. One of the features of Hillary Clinton’s national health care plan was a federal database of every American’s medical records. During one of his State of the Union addresses, President Clinton waved a card with a “unique identifier number” that would give government bureaucrats and health care providers easy computer access to everyone’s medical history.

Although the American people rejected that plan back in 1993 and 1994, the government is still moving ahead with a plan to give every American an “unique identifier number” and to compile medical records into a federal database. Five years ago the argument for a medical card and number linked to a federal database was to aid in health care planning and to eliminate fraud by health care providers. The American people, however, feared it would end medical privacy and increase federal control over health care.

The fear is justified. Just listen to what has already happened in a system without a medical ID number. For example, there is the banker on a county health care board who called due the mortgages of people suffering with cancer. There was a congresswoman whose medical records, revealing a bout of depression, were leaked before primary day. And there are a number of drug store chains that sell the name, address, and ailments of their customers to marketing firms.

The Hippocratic Oath says, “That whatsoever I shall see or hear of the lives of men, which is not fitting to be spoken . . . I shall keep inviolably secret.” Current attempts by the federal bureaucracy to standardize and centralize medical information are presented as a way to make health care delivery more effective and efficient, but they also have the potential to invade our privacy and threaten doctor-patient confidentiality. Frankly, I think the administration needs to rethink their current proposal. Or, to put it in medical terms, I think they need a second opinion.

Encryption

As we have been looking at the issue of privacy, we’ve considered attempts to establish a national ID card and a medical ID number. I want to turn to computers and talk about another important issue: encryption. Now I know that’s probably an unfamiliar word. But stay with me. Encryption is big word for a big issue that I think you need to know about.

Encryption is a relatively new technology that enables you to have private phone conversations and send e-mail messages that are secure. Encryption codes your words so that they cannot be deciphered by people listening in on your conversation or reading your mail.

As you may know, nosy people already can listen in on your wireless phone calls (cellular or cordless phones). And they can intercept and read your e-mail. Sending e-mail without encryption is like mailing a postcard — everyone can read it along the way. And we all know that people will do exactly that. If you have ever had a phone on a party line, you know that people listen in.

What you may not know is that various members of the Clinton administration (like Attorney General Janet Reno and FBI Director Louis Freeh) are demanding the authority to read encrypted messages. Now remember that the Fourth Amendment guarantees citizens be free of unreasonable searches and seizures. Nevertheless, these and other law enforcement officers believe they have the right to open your mail.

What they are asking for is the key to the code. When you send a message in code, you need a key to enable you to send the code and the recipients need the same key to read the code. The Clinton administration is demanding access to all encryption keys. This is like giving the government the power to steam open all the letters we send in the mail. Frankly, you only see this level of surveillance in totalitarian countries. If the government has the key, then it could call up information on you, your family, your medical records, your bank records, your credit card purchases, and your e-mail messages to all of your friends and relatives.

What is even more disturbing is the current attempt by the government to limit an American citizen's access to strong and powerful encryption software. A new study from the Cato Institute says that "People living outside the United States find it amusing and perplexing that U.S. law regulates the distribution of strong encryption." Critics of the administration's policy point out that true criminals (terrorists, drug dealers, the mafia) are unlikely to use anything less than the strongest encryption for their communication and data storage. The government will unlikely have a key to that level of encryption. Meanwhile, the average citizen must use weak encryption to protect private data and run the risk that the government will have a key to access it.

Everyone wants encryption in the computer age. Citizens want private communication. Businesses want to prevent billing records and personnel records from falling into the wrong hands. Consumers don’t want their credit card numbers widely distributed. That is why we need strong encryption software, and that is why government should not be given a key to the messages we send. Most Americans would not like to turn over so much of their privacy to the government, but unfortunately most Americans don’t realize that they already have.

Privacy and Your Life

Dave Ballert thought he was being a savvy consumer when he attempted to download a copy of his credit report from a web site. He hadn’t checked it recently and thought it was worth paying the eight bucks. But when the report arrived a few minutes later, it wasn’t his. It was a report for someone in California. The next thing he knew he received a call from the *Washington Post*, who said they received his report. The web site halted access later, but the damage was already done. How would you like a major newspaper to have a copy of your credit report?

Consider the case of the Social Security Administration. They provided earnings information to individuals via the Internet. After more than a month of virtually unfettered access for disgruntled employees, ex-spouses, and their attorneys, the Social Security Administration pulled the plug.

Such is life in the cyberage. More and more people are seeing their privacy violated and wonder what to do in a time of financial and personal indecent exposure. What used to be called public records weren’t all that public. Now they are all too public. And what used to be considered private records are being made public at an alarming rate. What should we do?

First, don’t give out personal information. You should assume that any information that you do give out will end up on a database somewhere. Phone solicitors, application forms, warranty cards all ask for information you may not want to give out. Be careful how much information you disclose.

Second, live your life above reproach. As it is written in Philippians 2:14-15, “Do all things without grumbling or disputing, that you may prove yourselves to be blameless and innocent, children of God above reproach in the midst of a crooked and perverse generation, among whom you appear as lights in the world.” 1 Timothy 3:2 says that an elder must be “above reproach,” which is an attribute that should describe all believers. If you live a life of integrity, you don’t have to be so concerned about what may be made public.

Third, exercise discretion, especially when you use e-mail. Too many people assume they have a one-on-one relationship with someone through the Internet. The message you send might be forwarded on to other people, and the message may even be read by other nosy people. One web site provider advises, “A good rule of thumb: Don’t send any e-mail that you wouldn’t want your mother to read.”

Finally, get involved. When you feel your privacy has been violated, take the time to complain. Let the person or organization know your concerns. Many people fail to apply the same rules of privacy and confidentiality on a computer that they do in real life. Your complaint might have a positive effect.

Track congressional legislation and write letters. Many of the threats to privacy I’ve talked about started in Congress. Citizens need to understand that many governmental policies pose a threat to our privacy. Bureaucrats and legislators are in the business of collecting information and will continue to do so unless we set appropriate limits.

Sadly, most Americans are unaware of the growing threats to their privacy posed by government and private industry. Eternal vigilance is the price of freedom. We must continue to monitor the threats to our privacy both in the public and private sector.

National Health Care

One of the hottest areas of debate in our society today is in the area of health care. Congress, the President, state legislatures, doctors, insurance companies, and private citizens are talking about rising health costs and proposing ways to deal with this issue.

Consider the following scenario: Suppose the federal government decided to do something about hunger in America and instituted food reform. Imagine that the proposed solution was to herd everyone into food alliances. Then it required that everyone buy food from those food alliances or else required them to eat their meals in huge cafeterias, all offering the same government-approved menu at government approved prices.

What would be the impact? If everyone had to go to food alliances to buy food, the price of food would go up. Imagine if every month money were deducted from your paycheck to pay for food insurance. Then when you went to the food alliance, you gave the cash register receipt to the government for reimbursement. Since you aren’t paying for it, you would rarely comparison shop. You wouldn’t be looking for bargains and eventually the cost of food would sky-rocket.

The only way the federal government could keep the price down would be to institute price control. It would have to tell manufacturers what they could charge for food. But this would lead to scarcity, because some farmers and manufacturers would conclude that the price was too low for them to make a profit. And some supermarkets would find the profit margin too small so they would go out of business.

Finally what would be the impact on you—the consumer? Well, you would see less diversity and less food at the food alliance. And there would be much more governmental regulation than is really necessary.

This, essentially, is what is being proposed in the area of health care. Government will establish health alliances, set prices, and implement employer mandates. These are just a few of the elements of what is called managed competition.

But is there a better way? Of course there is, and we can return to our food analogy to find it. Currently what does the federal government do to help people who do not have enough to eat? Does it assign people to food alliances or herd them into huge cafeterias? No. It gives them food stamps which they can use in local grocery stores. They comparison sop and find the food and prices they think is best.

Many are saying that this is the model we should use for health care. Don’t socialize health care and turn over the decision-making to a few federal bureaucrats and national health boards. Put the power and responsibility into the hands of 100 million individuals who would effectively organize and regulate the health care market.

This of course is just one proposal, but it illustrates rather dramatically what could happen if we made people responsible to their own actions rather than enlarge the role of government in health care.

How Many Americans Are Uninsured?

During the 1992 campaign, Bill Clinton said that there were 37 million Americans who are uninsured. We were told we need to reform health care in the U.S. in order to provide for the millions of Americans who do not have health insurance.

How many Americans are truly uninsured? During the campaign Bill Clinton stated that 37 million Americans are uninsured. But during his 1994 State of the Union speech President Clinton began using the higher figure of 58 million. Did that mean that 21 million Americans lost health insurance during the first year of the Clinton Administration? Obviously not. So what is the correct figure?

Well, it turns out that these figures only work if you include the Clinton disclaimer “some time each year.” This would include anyone who changed jobs, changed health plans, moved, etc. Using that criterion, it would be true to say that I have been homeless in the past since I have been “between homes during some time during a year.” But that did not mean that I slept under an overpass. Perhaps a better way to look at this issue would be to figure out how many people do not have insurance over a longer period of time—this would be the people who are chronically uninsured.

So how many Americans are chronically uninsured? It turns out that half the uninsured used in President Clinton’s statistic have insurance again within six months. Only 15 percent stay that way for more than 2 years. This produces a figure of about 5.5 million chronically uninsured.

But 37 percent of those people are under the age of 25. For them, insurance plans are often a bad buy or even unnecessary because they may still be covered by their parents’ plans. So if we eliminate the 37 percent, this brings the number down to approximately 3 million Americans who are chronically uninsured.

I might also add that some of these 3 million may not want to be insured. Some may be very wealthy and not want health insurance. Some of the other 3 million may want to be outside the system. The Amish may not want to be forced to buy insurance. Christians who are part of a group called “the Brotherhood” have opted out of traditional insurance and pay one another’s bills.

So we may have even less than 3 million people are chronically uninsured and want to be insured. That is no small number and it certainly isn’t insignificant if you are one of those people who are uninsured. But the 3 million figure does put the problem in a different light.

We could merely expand Medicaid to include these people. We could provide supplementary insurance for these people. We could even come up with free market alternatives. But we don’t need government to take over one-seventh of the American economy merely to deal with the problem of 3 million uninsured Americans.

And that’s the point, some of the numbers are being used to justify rash and draconian actions. We don’t need health alliances, employer mandates, national health boards, or mandated universal coverage if the real problem is that 3 million Americans are chronically uninsured. We can develop a simple program to meet their needs and avoid the problems of socialized medicine.

What About the Costs?

At this place in the discussion it’s appropriate to focus on the possible cost of health care reform. Most Americans want to know the price tag of health care reform. And when you hear people talking about the potential cost, recognize that you probably aren’t hearing the whole story. Proponents will talk about the direct cost of health care reform, but remember that are other hidden costs that may be more significant.

For example, what will be the impact of health care reform on business? Proponents argue that the impact will be minimal. Business owners are not so sure. They fear that employer mandates will hurt their business, affect their bottom line, and create substantial unemployment.

During a Presidential town meeting in April 1994, President Clinton got into a verbal sparring match with Herman Cain, president and CEO of Godfather’s Pizza. The President asked, “Why wouldn’t you be able to raise the price of pizza two percent? I’m a satisfied customer. I’d keep buying from you.” Then he asked to see Mr. Cain’s calculations. Mr. Cain replied in a letter to the President (later reprinted in the *Wall Street Journal*). The following is a brief summary of the letter.

Although there are over 10,000 employees with Godfather’s Pizza, two-thirds are owned and operated by franchisees. Mr. Cain focused his calculation only on the approximately one-third which were corporate-owned operations.

Mr. Cain concluded that the Clinton Health Care plan would cost nearly $2.2 million annually. This represents a $1.7 million increase. In other words this increase would be a 3 1/2 times their insurance premium for the previous year!

If these calculations by Mr. Cain are accurate (and no one has challenged them so far), then how did President Clinton arrive at his figures of a 2 percent increase in price of pizza? President Clinton stated that restaurants with approximately 30 percent labor need only increase prices by 2.5 percent. Apparently he multiplied 30 percent by the employer mandate of 7.9 percent.

But Mr. Cain’s detailed calculations show that it just isn’t that simple. He estimates that you would need a 16 to 20 percent increase in “top line” sales to produce the same “bottom line” due to variable costs such as labor, food costs, operating expenses, marketing, and taxes.

I would argue that even a 2 percent increase in pizza costs could be devastating. Most people buy pizza to save time and money. Even a small increase in the cost of pizza would affect business. Mr. Cain noted that half of all Godfather's Pizza customers use coupons to purchase pizzas. The impact of a 16 to 20 percent increase would be devastating to Godfather's Pizza. And what would be the impact on the economy? In essence the President was predicting that health care reform would require the inflation of prices.

Will a health care reform bill with employer mandates adversely affect business? Proponents say that health care reform will not be costly to the American taxpayer or to American business. But tell that to Herman Cain and Godfather's Pizza. Their detailed spreadsheets project that these health care bills will more than triple their insurance costs in just the first year.

Health care reform may cost much more than we think it will. The direct costs may not seem like much, but don't forget to count the indirect costs to you and to American business.

Other Issues

Other key issues being discussed along with health care reform need to be examined. The first is health care costs. Originally only about 5 percent of the Gross Domestic Product was spent on health care. And until the mid-1980s, it was less than 10 percent. But now it is approximately 14 percent of Gross Domestic Product and could be as high as 18 percent by the end of the decade. In actual numbers, health care costs were $74.4 billion in 1970 and will be approximate $1.7 trillion by the year 2000.

Part of the problem is that a third party pays for health insurance. If there were more personal accountability, people would comparison shop and bring market pressures to bear on some of the health care costs. For example, if I told you I was going to take you to dinner on the Probe credit card, you would probably spend a lot of time looking at the left side of the menu. However, if I said, “Let’s go out to eat, Dutch treat,” you would probably spend a lot more time looking at the right side of the menu. When someone else pays for our medical bills, we don’t pay as much attention to cost. When we have a personal responsibility, we pay more attention and thereby lower costs.

A second issue is tax fairness. Nearly 90% of all private health insurance is employer-provided and purchased with pre-tax dollars. But the self-employed and those who buy their own insurance must buy theirs with after-tax dollars. Presently the government “spends” about $60-billion a year subsidizing employer-based health insurance by permitting employers to deduct the cost.

Tax fairness would allow all people to buy health insurance with pre-tax dollars. One solution is to allow those who purchases their own health insurance to have a tax deduction or tax credit. This would eliminate the tax benefit for getting health insurance through an employer and employees could purchase their own insurance which leads to the next issue.

Portability is the third major issue. Americans usually cannot take their health insurance with them if they change jobs. A fair tax system would offer no tax subsidy to the employer unless the policy was personal and portable. If it belonged to the employee, then it would be able to go with the employee when he or she changed jobs.

In essence, health insurance is merely a substitute for wages. In a sense, it is an accident of history. Health insurance was provided as a benefit after World War II. Health insurance should be personal and portable. After all, employers don’t own their employees’ auto insurance or homeowner’s insurance. Health insurance should be no different.

Price fairness is another issue. Proponents of socialized medicine would force people with healthy lifestyles into a one tier system with people who smoke, drink too much, use drugs, drive irresponsibly, and are sexually promiscuous. A better system would be one that rewards responsibility and penalizes irresponsibility. Obviously we should provide for the very young, the very old, the chronically ill, etc., but we shouldn't be forced into a universal risk pool and effectively subsidize the destructive behavior of those who voluntarily choose sin over righteousness.

These are just a few of the key issues in the health care debate. Unfortunately many of them have been ignored. A truly ethical health care system must provide tax fairness, price fairness, and portability.

The Moral Costs

I would like to conclude by examining the social and moral implications of health care reform? Critics of health care reform warn that it will inevitably lead to rationing. Most of the government health care plans proposed will be forced to ration care and no doubt put a squeeze on the aged and on high tech medicine. This would be the only way to save money. For example, when Hillary Clinton testified before the Senate Finance Committee, she explained to the Senators their justification for health care services. She said their proposal creates "the kind of health security we are talking about, then people will know they are not being denied treatment for any reason other than it is not appropriate—will not enhance or save the quality of life." Medical services will be curtailed for those whose quality of life is not deemed necessary to treat. This has been the inevitable result in other industrialized countries that have socialized medicine. If you increase demand (by providing universal coverage), you will have to decrease supply (health care benefits provided to citizens). Those patients whose quality of life is not deemed satisfactory will be denied treatment.

Canada, for example, has a single-payer plan. They have found that their health care costs are going up as fast as U.S. while their research is lagging behind. Patients find themselves in waiting lines and have been coming in significant numbers to the U.S. for health care. Those remaining in Canada wait in line. There are currently 1.4 million waiting for care and 45 percent say they are in pain.

There would also be a squeeze on high tech medicine. The quickest way to save money is to limit the number of CAT scans, MRIs, or other sophisticated forms of technology. In Canada high tech equipment is relatively rare and used sparingly. In the U.S., the latest technology is available to nearly all Americans.

Health care expert Danny Mendelson writing in *Health Affairs* journal predicted that “a few years down the line, you first start to see what we call silent rationing, where the patient’s don’t even know that they’re not receiving the beneficial care that they need. Further down the line, I think it would become very clear that we were denying patients some of the latest technology in order to save money.”

Finally, critics wonder if government should be entrusted with running the health care system in America. Government has not proven to be an efficient deliverer of services. As one wag put it, if we have government take over health care, we might end up with a system that has the efficiency of the post office, the compassion of the IRS, at Pentagon prices. No slight is intended to the good people who work in those areas of government, but the joke does underscore the growing concern over government delivery of services, especially health care.

As Americans begin to evaluate the costs of various health care reform packages, they are beginning to find they are a bad buy. The solution is to reduce the scope of government in health care, not expand it.