# 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.

© 2000 Probe Ministries International

# **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.

©1999 Probe Ministries.

# Financial Security for the Future

Kerby Anderson looks at our financial future, especially of baby boomers, discussing savings, corporate pensions, Social Security and retirement.

What kind of financial security can you expect in the future? The answer to that question may depend on when you were born. The generation currently entering retirement will do much better as a group than the baby boom generation following it.

A major reason is demographics. The baby boom was preceded, and more importantly, succeeded by consecutive years of fewer births. Thirty-five percent more Americans were born during the baby boom than during the previous nineteen years. And 12 percent more were born than during the subsequent nineteen years. This nineteen-year blip in fertility has created more than just an oddity in social statistics. It has clouded the financial future of baby boomers. The elderly are supported, especially during the waning years of their old age, by members of the younger generation. The baby boom was immediately followed by a baby bust, or what many commentators have labeled a "birth dearth." This disproportionate ratio between baby boomers and baby busters raises questions about the boom generation's future and suggests it will face an

impending crisis of financial security.

Concern arises from both economic and demographic realities. The harsh economic reality in the 1990s is the federal deficit which mushroomed during the 1980s. Aggravating this economic situation are also such issues as trade deficits, increased taxes, higher oil prices, and an inevitable downturn in the economy.

A survey released by the International Association of Financial Planning found that "the long term psyche of the American public is depressed," with significant majorities fearing a resurgence of high inflation and worrying about the chances for a deep recession. But the more important issue is not economics but how demographics affect economics. The sheer size of the boom generation has had a negative impact on its members. Paul Hewitt of the Retirement Policy Institute put it this way:

The baby boom as a generation has been its own worst enemy. Whenever we wanted anything the price went up, and when we sold the price went down. So we got less for our labor and paid more for our houses. When we want to sell those houses the price will go down, and when we want medical care in old age, prices will go up.

Boomers in general, and leading-edge boomers in particular, find themselves part of what has become called "the triple-squeeze generation." The more than 25 percent of Americans between the ages of 35 and 44 are finding their own retirement being squeezed out by the college costs of their children and the long-term health care costs of their aging parents. Sixty-six percent of baby boomers surveyed by the International Association of Financial Planning said "providing long-term care fora parent would affect their ability to save for their children's education" and would no doubt also affect their ability to save for their own retirement.

Commentators have also referred to these people as the "sandwich generation" because they are sandwiched between an older generation dependent upon them for elder care and a younger generation dependent upon them for housing and education. Surely this is one generation that needs to take a hard look at its financial future. The economic and demographic realities may seem dismal, but they will be much worse if we fail to apply biblical principles to our finances. The key to financial security for most Americans has been the three-legged stool of savings, pensions, and Social Security. Unfortunately, economic termites threaten the strength of that stool.

### Savings

The first leg on the retirement stool is savings. The boomers are justly concerned about the savings (or more to the point, the lack of savings) they have put away so far for their retirement. A survey of leading-edge boomers found that six out of ten expressed great concern about being able to meet all of their financial responsibilities, and 62 percent fear that they will outlive their retirement savings.

But they aren't the only ones concerned. A survey by the American Academy of Actuaries echoed boomers' fears. Seventy-two percent of pension-fund actuaries polled predict that half the baby boom won't have the wherewithal to retire at age 65.

How much have baby boomers saved so far? Well, not very much if a recent survey is any indication. When a group of 35- to 49-year- olds were asked if they could come up with three thousand dollars in a few days without borrowing or using a credit card, 49 percent said they could and 49 percent said they couldn't. Not surprisingly a smaller percentage (only 29 percent) of the 18- to 24-year-olds had the three thousand dollars.

The inability of so many boomers to come up with the sum of

three thousand dollars illustrates two things. First, it shows how little (if anything) they have in savings or investments. Second, it demonstrates how much many of them are in debt. The first leg of the three-legged stool is in awful shape because, for many in the boom generation, savings are decreasing while debt is increasing. The reasons for boomer debt are fairly simple. First, the boomers had great expectations for themselves and were often willing to go deeply in debt in order to finance the lifestyle they had chosen for themselves. Second, they had the misfortune of entering the consumer world at the time when wages were stagnant and when most of the goods and services they craved were hit by inflation. This further fueled consumer borrowing, which became both a cause and a consequence of their downward mobility.

Between 1970 and 1983, the percentage of boomer families paying off consumer debt increased from two-thirds to three-fourths. Of families in debt in 1983, the average amount of debt was nearly five thousand dollars.

Families in debt usually are not saving. If they had any financial resources to save and invest, they would be wise to first retire their high interest consumer debt. In 1984, more than a third of all households headed by a person under thirty-five had no savings whatsoever on deposit with banks and other financial institutions, aside from non-interest-paying checking accounts.

The solution to this problem is simple: Get out of debt and put money into savings and retirement. Now while this may be easy to say, it is difficult for the current generation to do. Baby boomers' expectations frequently exceed their income, and the changing economic and demographic realities place them in a precarious position. But if this generation wants to have a more secure financial future, it must take appropriate financial measures now.

#### **Corporate Pensions**

In the past, there used to be an unwritten agreement between a company and an individual. If you faithfully worked for the company, the company would take care of you in your retirement. But this tacit agreement has broken down for two reasons.

First, many of these companies lack the financial resources to take care of the baby boom generation. Consolidation of some companies and the bankruptcies of many others put pensions in jeopardy. Other companies heavily invested in speculative schemes by thrifts and junk bonds, and their portfolios rest on shaky ground. In other cases, the current financial resources seem adequate but have yet to be tested when the millions of baby boomers begin to retire. Second, many baby boomers have not spent enough time with any one company to earn a significant pension. It was not uncommon for the parents of baby boomers to have worked for a single company for more than twenty years. Baby boomers, on the other hand, change jobs if not career paths with unprecedented frequency.

This apparent restlessness is born from both choice and necessity. Boomers are much less likely to stay in a job that does not enhance personal development and self-expression. Unlike their fathers, who would often remain with a company "for the sake of the family," the boom generation is much more likely to move on.

Boomers also change jobs out of necessity. They find themselves competing with each other for fewer uppermanagement positions for a number of reasons. First, companies have thinned their management ranks. Most of this restructuring was done in the 1980s to make companies more efficient. The rest was a natural result of buyouts, takeovers, and consolidation leaving fewer structural layers in upper management and fewer jobs.

Second, boomers crowded into middle-management ranks at the same time restructuring was taking place. The leading-edge boomers in their prime career years are finding themselves on career plateaus and becoming dissatisfied. Many wonder if they will ever make it to the corner office or the executive suite.

Third, there was a boom of business school graduates. The first boomers who graduated with MBAs were often ridiculed by classmates in other academic disciplines. But this initial condemnation gave way to active pursuit, and the number of business graduates quickly proliferated. As supply has outstripped demand, this ambitious group with heightened expectations finds itself frustrated and constantly looking for a job change.

All of these factors have put this generation in a precarious position. By and large, they are not saving and have inadequate pensions to give them a secure financial future. So many are trusting that Social Security will be there for them when they retire. But will it?

## Social Security

The impending Social Security debacle is complex and the subject of whole books. But the basic issue can be illustrated by once again looking at the demographic impact of the boom generation.

When Social Security began in the mid 1930s, the ratio of workers to recipients was ten to one and life expectancy was two years below retirement age. The pay-as-you-go system could work with those kinds of numbers.

But two fundamental demographic changes threaten to send Social Security off a cliff. First is the "senior boom." Advances in modern medicine have raised life expectancy by 28 years in just this century. Today the median age is already 32 and still climbing. Some demographers see the median age

reaching as high as 50 years old. One has to wonder about the stability of Social Security in a country where half of the people qualify for membership in the American Association of Retired Persons.

The second demographic change is the ratio between the baby boom generation and the baby bust generation. The smaller generation following the boom generation will be called upon to support Social Security when boomers retire. The system will face incredible strains through the next few decades as the ratio of workers to Social Security beneficiaries continues to decline.

Both demographic changes are relevant. Americans are living longer, and ratios between generations are skewed. These two changes are certain to transform the current pay-as-you-go system into nothing more than an elaborate Ponzi scheme by the twenty-first century. The solutions to the Social Security crisis are few and all politically difficult to achieve. Either you have to change the supply of contributions or the demand of the recipients. Increasing the supply of contributors could be achieved by increasing the birth rate (unlikely, and probably too little too late) or allowing more immigration of workers who could contribute to Social Security. The only other way to increase the supply of contributions is to increase FICA payments. But there will have to be an upper limit on how much Americans can be taxed. If benefits stay at their current levels, workers in the year 2040 could find Social Security taking as much as 40 percent of their paychecks.

Decreasing demand would require trimming benefits. Current recipients benefit most from Social Security. A retiree on Social Security today recovers everything he paid into the system in about four years. On the other hand, few boomers will ever get the amount of money they paid into the system. Some politicians have suggested trimming benefits to current recipients. Others suggest applying a means test to wealthy

recipients or those who receive other pension income. Neither proposal has much likelihood of passage.

More likely, Congress will be forced to trim future benefits. Congress has already increased the age of retirement and may induce workers to stay on the job until age 70. Another solution would be to provide the biggest tax breaks for workers to fund their own retirement through IRAs or Keoghs.

Obviously the solutions are not popular, but the alternative is a collapse of the Social Security system in the next decade. If something isn't done, the demographic realities will destroy the system.

#### Retirement

Although this generation grew up assuming retirement would be the norm, the changing social and economic conditions we have discussed may force a rethinking of that basic assumption. After all, the idea of retirement historically is of recent origin.

When Social Security was first adopted in 1935, life expectancy was below 63, a full two years under the retirement age. Retirement was for the privileged few who lived long enough to enjoy the meager financial benefits from the system.

Even as late as the 1950s, the contemporary image we have today of retirement communities and the elderly sightseeing in recreational vehicles did not exist. Retirement still did not exist as an institution. Nearly half the men over age 65 were still in the workforce.

Polls taken during the 1950s and early 1960s showed that most Americans desired to work for as long as they could and saw retirement merely for the disabled. Today, however, most Americans look forward to their retirement as a time to travel, pursue personal interests, and generally indulge themselves. Yet the demographic landscape suggests we might

have to revise our current images of retirement.

As baby boomers slowly jog towards Golden Pond, they will likely be the largest generation of senior citizens in history, both in absolute size and in relative proportion to the younger generation. By the year 2000, the oldest boomers could be taking early retirement. The number of workers and dependents retired by 2025 could swell to as many as 58 million workers and dependents, more than double the current number of retirees.

These large numbers are certain to precipitate a "retirement crisis" for two reasons. First, people are living longer. We have raised the life expectancy by 28 years. During most of human history, only one in ten lived to the age of 65. Today eight out of every ten Americans zoom past their 65th birthday.

Second, the burden of providing retirement benefits will fall upon the younger, (and more to the point) smaller generation born after the baby boom. Never will so few be required to fund the retirement of so many. When Social Security was adopted in 1935, there were ten workers for every person over age 65. That ratio shrank to six to one in the 1970s.

Today there are about 3.4 working Americans to support each retiree. But by the time the last boomer hits retirement age in 2029, the ratio of workers to retirees will drop to less than two to one. Obviously, baby boomers face much greater uncertainty than their parents did when they entered into the years now seen as the time of retirement.

This next generation may even decide to reject the idea of retirement, choosing instead to enrich themselves with meaningful work all of their lives. Yet such an idyllic vision could quickly be crushed by the harsh reality of failing health. Working until you are 70 or beyond may not be physiologically possible for all people.

No wonder a chorus of Cassandras is predicting financial disaster in the next century. But significant changes can be made now to avert or at least lessen a potential crisis in the future. Wise investment according to biblical principles now is absolutely necessary to prepare for this uncertain future. The future really depends on what this generation does in the 1990s to get ready for the Retirement Century.

© 1993 Probe Ministries.