Privacy 2010

Introduction

Ten years ago, I did a Probe radio program called "Privacy 2000."{1} At the time, American citizens were concerned about some of the new technological advances and government programs that seemed to be threats to their privacy.

So much has happened in the last ten years. Technological developments have provided individuals, companies, and governments with new tools which could be used to violate our privacy. A war on terror has changed our perception of what is or is not appropriate for government to know about its citizens. In fact, I developed a week of radio programs on "Homeland Security and Privacy."{2}

One thing I have noticed is that most Americans seem less concerned about intrusions into their lives. Part of it may be due to a resigned assumption that we have to give up some of our privacy to fight the terrorists. But another significant reason, I believe, is a younger generation that seems completely unconcerned with threats to their privacy. After all, many of them are sharing intimate details of the lives on Facebook and MySpace. Why be concerned if companies, the government, or the general public knows details of their lives when they voluntarily share those details on social networks?

This is not to say that all citizens are unconcerned about privacy violations. Recent debates about a national ID card and the collecting and centralization of medical information for government health care programs illustrate that many people are concerned about privacy. But the percentage of citizens concerned about privacy seems to be decreasing.

Privacy is something that most of us take for granted until we lose it. And often we lose our privacy in incremental steps so we are less aware of our increased exposure. Some events can shock us back to reality. Identity theft or the posting of embarrassing information on the Internet can quickly remind us how much privacy we have lost.

We should also make a distinction between privacy and secrecy. Whenever someone expresses concern over a violation of their privacy, another is sure to ask, “What do you have to hide?” The question confuses privacy with secrecy. You may not have anything to hide, but that doesn’t mean that you are willing to have companies collect lots of information about you and then sell it to other companies for a profit. You may not want your future boss to know about a medical procedure that was done twenty years ago. You may not want a telemarketer to have your purchasing history so he can call your mobile phone.

In this article we look at various ways we have lost our privacy. These range from intrusion to deception to profiling to identity theft.

Seven Sins against Privacy: Intrusion

Privacy is a common word but often misunderstood because of it various meanings. We know when we feel that someone have violated our privacy, but we can’t always give a definition to it, especially in this age in which new technology allows perpetrators to cross boundaries more easily than in the past.

David Holzman describes three basic meanings for privacy.{3} They are easy to remember because they all begin with the letter s. The first is seclusion. That is the right to be hidden from the perceptions of others. The second meaning is solitude. This is the right to be left alone. The third meaning is self-determination, which is the right to control information about oneself.

He suggests that privacy violations can be viewed as seven sins ranging from intrusion to deception to profiling to identity theft. Let’s look at each one of these sins against privacy.

Sin of Intrusion – The classical form of privacy abuse is intrusion. This “is the uninvited encroachment on a person’s physical or virtual space.”{4} In previous ages, it took the form of voyeurism or peeping. Technology today allows for a much great intrusion into our lives and is often much more difficult to detect.

In recent years, we have read about how actors, models, and sportscasters have had their privacy violated by people who placed cameras or listening devices in their rooms or on their person and recorded them. But it isn’t just the famous that are being recorded. Every day pictures are being taken of us as we walk into banks, into grocery stores, or past ATM machines. We are being recorded on the streets and at traffic lights. It has been estimated that the average person is caught on surveillance cameras three hundred times a day in London.{5}

And it is not just big brother that is watching and listening to you. Voyeurism technology is available to anyone who wants to purchase it. Stores and Web sites “sell remote listening devices, digital optics, scanners for picking up cell-phone conversations, and even infrared scanners.”{6}

Radio Frequency Identification Devices (RFID) act like a wireless bar code and is being used more often in stores and other establishments (such as libraries) for inventory control. Geographic Positioning System (GPS) receivers are satellite locating devices that are found in cars, cell phones, and many other devices.

Intrusion violations have been made easier by technology. In the past, someone had to get near to you in order to spy on you. And that increased the possibility that you would find out that someone is watching you. Now we live in a world where your privacy is being violated, and you are probably not even aware that it is happening.

Seven Sins against Privacy: Latency and Deception

Sin of Latency – Most of the damage to your privacy comes from stored information. The harm is minimized if personal information is not retained. The sin of latency comes from the excessive hoarding of information beyond an agreed-upon time. Most companies do not have a data-aging policy.

It is understandable why companies and the government collect excessive information. First, they need to have enough information so they know they have the right person. There are lots of John Smiths in a particular locality. They need to know you are the particular John Smith they want. In the past, a telephone number was sufficient identification. Now we have more than one phone and change numbers regularly. So our Social Security number and other identifiers are necessary.

A second reason for companies to collect information is so they can more effectively sell their products and services to you. They collect that information from the forms you fill out and even place cookies on your computer in order to catalogue your visits to their Web site.

We might assume that a company would delete your information when you close your account. Most companies merely mark your file as inactive. And many of them sell your information to others. "A consumer record with up-to-date information is worth around $200 for cell phone information. Social Security information sells for $60 and a student's university class schedule goes for $80."{7}

One of the largest collectors of personal data is Google. When you search for items on the Internet, Google collects that information, and that reservoir of information can begin to paint a picture of your interests, opinions, and worldview. And because Google saves that information for a long time, it can do extensive database matching.

Google was involved in a legal battle with the U.S. Department of Justice that subpoenaed their log files. They wanted to use them to make the case that pornography constitutes a substantial part of Internet searching. A judge ruled that Google needed to only turn over a limited set of information with identifying notations stripped off.{8}

Sin of Deception – With so much electronic information available in databases, it is tempting for individuals, companies, and even bureaucrats to use personal information in a way that was not authorized by the person.

Here are some principles that arise from our discussion so far. When a company or governmental agency asks for personal information we should have the right to know three things: what they are going to do with it, how long they will keep it, and whether they will make it available to others. When we fill out a form for a credit card or enter into a contract for a car or house, we reveal lots of information. We may naively assume that they will be the only ones who will see that information. That is not so. Regularly we see stories in the news about companies selling consumer data to third parties. Most of us would be shocked at how much information about us in the hands of people who have never met or done business with.

Seven Sins against Privacy: Profiling and Identity Theft

Sin of Profiling – Past behavior is not always a perfect predictor of future behavior, but it can be a surprisingly accurate one. That is where profiling comes in. Collecting information about what goods and services someone purchases can enable companies to predict a consumer's future purchases.

Profiling is often used to predict more than that. David Holzman says that he worked with one credit card company that said "it was able to pinpoint when its consumers were having life crises such a mid-life depression by psychographically analyzing their buying patterns."{9}

One of the best known examples of profiling is credit scoring. Equifax, Experian, and TransUnion rely on FICO scores. A high score will help you get a home loan. A low score may result in being denied a home loan and even having to pay higher interest on other forms of credit. Most Americans don't know their credit score (only about two percent), and most do not understand the algorithm used to calculate it.

Profiling is also used to fight terrorism, but have also caught innocent people in their profiling net. For some time my name was on a watch list, and people like columnist Cal Thomas and Senator Ted Kennedy were on a no-fly list.

These mistakes prove an important point: profiling is a guessing game. And sometimes a wrong guess can have a detrimental impact on citizens and consumers.

Sin of Identity Theft – Most of us know what identify theft is because it has happened to someone we know or else we have heard commercials about how to protect ourselves from identity theft. Although this crime did exist in the past, it has exploded on the scene now because of technology and the changing nature of transactions. Personal information is readily accessible on the Internet. And in the electronic marketplace of today, purchases are not made face-to-face. It is easy for someone to assume your identity and leave you with the consequences.

How easy is it? A New York busboy was caught stealing the identities of people on the Forbes 400 list. He used the

Internet to do the research and had been successful in stealing the identities of famous people like Steven Spielberg, Oprah Winfrey, and Ted Turner.{10}

Sometimes all a hacker or thief needs is your Social Security number and your mother's maiden name. Unfortunately it is relatively easy to obtain this information. Universities, banks, and all sorts of institutions use your Social Security number as your identification number. Genealogy files online most likely have your mother's maiden name. Once a theft has that information, he or she is ready to access your financial accounts.

Sometimes we inadvertently give out that information. A phone call from someone pretending to be a bank executive can often elicit confidential information. "Phishing" is a mass e-mail with a message pretending to be a bank or brokerage. People who believe that it is genuine will enter information that the theft can use to drain their bank accounts.

Seven Sins against Privacy: Outing, Lost Dignity

Sin of Outing – Some privacy violations are deliberate and can take place when someone reveals information that another person would like to remain hidden. The term "outing" is usually used to describe a public revelation of a closet homosexual, but we can use the term to describe any information that is published about a person they do not want to be public.

Citizens, politicians, and even corporations have been the targets of Internet messages that have been used to damage their reputation. A number of court cases have attempted to force Web site managers to reveal the identities of those who are spreading false and libelous information.

Sometimes outing is a good thing. Think of all the potential pedophiles that have been caught because they thought they were chatting online with a potential underage victim. Sting operations by the police have successfully revealed the motives of some who intend to proposition their young victims.

Sin of Lost Dignity – This last concern is more difficult to quantify, but we all realize that when private information is made public, we can lose a part of our dignity. What if all of your medical records were made public? What if every essay you ever wrote in school was available online?

Even public figures (like politicians) believe they should have a zone of privacy. Past and current presidents have refused to publish all of their medical records, school records, and other private information. While we may debate whether public figures should reveal all of this information, we would probably all agree that private citizens should not lose a zone of privacy in their lives.

In this article we have talked about how technology allows us to peer into other people’s lives. That is why we need to revisit the subject of ethics as it relates to technology that can violate our privacy. We shouldn’t use technology to spy on others or to hurt their reputation. Christians should express their concerns about intrusions into their privacy.

This subject also reminds us that we must live our lives 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. Live a life of integrity and you won’t have to be so concerned about what may be made public in age where we are losing our privacy.

Notes

1. Kerby Anderson, "Privacy 2000," Probe Web site, 2000, www.probe.org/privacy-2000/.
2. Kerby Anderson, "Homeland Security and Privacy," Probe Web site, 2003, www.probe.org/homeland-security-and-privacy/.
3. David Holzman, *Privacy Lost: How Technology is Endangering Your Privacy* (San Francisco: Josey-Bass, 2006), 4.
4. Ibid., 5.
5. Ibid., 6.
6. Ibid.
7. Ibid., 10.
8. Ibid., 13.
9. Ibid., 19.
10. Ibid., 23.

Homeland Security and Privacy

A Supersnoop's Dream

Every day we seem to wake up to news about another terrorist threat, so it's not surprising that Americans are placing more of their faith in the government to protect them. But there are also important questions being raised about our loss of privacy and constitutional protections. So in this article we are going to take a look at some of these issues as we focus on the subject of homeland security.

The Department of Homeland Security was created by combining twenty-two existing agencies and 170,000 federal employees with an annual budget of approximately $35 billion. While the implications of this megamerger of governmental agencies will be debated for some time, some columnists have already begun to question the impact it will have on our private lives.

The Washington Times called it “A Supersnoop’s Dream.” Columnist William Safire of the *New York Times* wrote a column entitled “You Are a Suspect” in which he warned of a dangerous intrusion into our lives. He predicted in November 2002 that if the Homeland Security Act were not amended before passage, the following would happen to you:

> - *Every purchase you make with a credit card, every magazine subscription you buy and medical prescription you fill, every Web site you visit and e-mail you send or receive, every academic grade you receive, every bank deposit you make, every trip you book and every event you attend—all these transactions and communications will go into what the Defense Department describes as a virtual centralized grand database.*
> - *To this computerized dossier on your private life from commercial sources, add every piece of information that government has about you—passport application, driver’s license and bridge toll records, judicial and divorce records, complaints from nosy neighbors to the F.B.I., your lifetime paper trail plus the latest hidden camera surveillance—and you have the supersnoop’s dream: a Total Information Awareness about every U.S. citizen.*

It is important to point out that these concerns about a potential invasion of privacy did not start with the passage of the Homeland Security Act. Over a year ago, critics pointed to the hastily passed U.S.A. Patriot Act which widened the scope of the Foreign Intelligence Surveillance Act and weakened 15 privacy laws.

On the other hand, there are many who argue that these new powers are necessary to catch terrorists. Cal Thomas, for example, writes that “Most Americans would probably favor a more aggressive and empowered federal government if it lessens the likelihood of further terrorism. The niceties of civil liberties appear to have been lost on the 9/11 hijackers and countries from which they came. Wartime rules must be different from those in peacetime."{1}

The Patriot Act

Let's look more closely at the U.S.A. Patriot Act. When Senator Russ Feingold voted against the Act, he made these comments from the Senate floor on October 11, 2001:

> *"There is no doubt that if we lived in a police state, it would be easier to catch terrorists. If we lived in a country where police were allowed to search your home at any time for any reason; if we lived in a country where the government is entitled to open your mail, eavesdrop on your phone conversations, or intercept your e-mail communications; if we lived in a country where people could be held indefinitely based on what they write or think, or based on mere suspicion that they are up to no good, the government would probably discover more terrorists or would-be terrorists, just as it would find more lawbreakers generally. But that wouldn't be a country in which we would want to live."*

Most would agree that the Patriot Act weakens grand jury secrecy. Already there is criticism that grand juries have become mere tools of the prosecution and have lost their independence. By destroying its secrecy, any federal official or bureaucrat can "share" grand jury testimony or wiretap information.

The Patriot Act also weakens Fourth Amendment protection against unreasonable searches and seizures. Under the Act, law-enforcement agencies can in "rare instances" search a person's home without informing that homeowner for up to ninety days. This so-called "sneak and peek" provision can be used to sneak into your home, and even implant a hidden "key logger" device on a suspect's computer (allowing federal officials to capture passwords and monitor every keystroke).

And, the Patriot Act weakens financial privacy. The bill added additional amendments and improvements to the Bank Secrecy Act which already encourages FDIC member banks to profile account holders and report to the government (FBI, IRS, DEA) when you deviate from your usual spending or deposit habits. The Act exempts bank employees from liability for false reporting of a money laundering violation.

Michael Scardaville of the Heritage Foundation, however, isn't concerned about conferring this new power on bureaucrats. "Even if they wanted to, the program's employees simply won't have time to monitor who plays football pools, who has asthma, who surfs what Web site or even who deals cocaine or steals cars. They'll begin with intelligence reports about people already suspected of terrorism."{2}

Immigration Threats

Lincoln Caplan, writing in the November-December issue of *Legal Affairs* (a magazine of the Yale Law School), said that the U.S.A. Patriot Act "authorized law enforcement agencies to inspect the most personal kinds of information – medical records, bank statements, college transcripts, even church memberships. But what is more startling than the scope of these new powers is that the government can use them on people who aren't suspected of committing a crime."

Although there has been some concern expressed about the intrusion of government into our lives, an even greater concern is how the Homeland Security Act fails to address the real threat to our country through lax enforcement of immigration laws. Michelle Malkin, author of *Invasion*, cites example after example of problems at the Immigration and Naturalization Service (INS).

Foreign students getting visas to enter the U.S. constitute a major problem that is out of control. Malkin says that the bill establishing this new department doesn’t do anything about it. There is also a problem with foreigners getting tourist visas to enter the U.S. and then overstaying their visas. The bill doesn’t do anything about this problem either.

More than 115,000 people from Iraq and other Middle Eastern countries are here illegally. Some 6,000 Middle Eastern men who have defied deportation orders remain on the loose. Add these numbers to those who are here legally, but still intend harm to the United States, and you can begin to grasp the extent of the problem.

Consider the case of Hesham Mohamed Hedayet, who shot and killed people at the Los Angeles International Airport. He managed to stay in this country by obtaining a work permit after his wife won residency in a visa lottery program (given to 50,000 foreigners on a random basis).

Michelle Malkin broke the story about the Washington, D.C. area sniper suspect John Malvo. The INS had him in custody but released him. The U.S. State Department failed to obtain a warrant for the arrest of the other sniper suspect, John Muhammad, after he was suspected of using a forged birth certificate to obtain a U.S. passport.

Congress needs to take another look at both the Patriot Act and the Homeland Security Act. In its rush to deal with the imminent terrorist threat, it has conferred broad powers to bureaucrats that should be refined and failed to address some crucial concerns in immigration that continue to threaten our safety. It is time for Congress to pass some common sense amendments to these two pieces of legislation.

History of Governmental Power

I think all of us would strongly support the President and

Attorney General in their attempts to track down terrorists and bring them to justice. But some wonder if Congress has put too much power in the hands of the executive branch, power that could easily be abused by this administration or future administrations.

Let’s consider our history. President John Adams used the Alien and Sedition Act to imprison his political enemies and curb newspaper editors critical of him. President Woodrow Wilson permitted his attorney general (Mitchell Palmer) to stop political dissent during the Palmer Raids. And President Franklin Delano Roosevelt interned thousands of Japanese-American citizens during World War II.

It is interesting that some of the greatest expansions of powers have come under Republican presidents. The first Republican president, Abraham Lincoln, suspended the writ of habeas corpus. (This is a judge’s demand to bring a prisoner before him, with the intent to release people from unlawful detention.) This led to the imprisonment of physicians, lawyers, journalists, soldiers, farmers, and draft resisters. Sixteen members of the Maryland legislature were arrested in order to prevent them from voting for their state to secede from the Union. By the time the Civil War was over, 13,535 arrests had been made.

Although Democrats have often been credited with expanding the size and scope of the federal government, Republican administrations are actually the ones who have expanded various police powers. RICO and nearly all the seizure laws (where police can confiscate cars, boats, even homes without due process) were passed by Republican administrations.

Dana Milbank wrote in the *Washington Post* (Nov. 20, 2001) that “The Sept. 11 terrorist attacks and the war in Afghanistan have dramatically accelerated a push by the Bush administration to strengthen presidential powers, giving President Bush a dominance over American government exceeding that of other post-Watergate presidents and rivaling even Franklin D. Roosevelt’s command.”

Perhaps it is time for Congress to revisit this important topic of anti-terrorism and modify some of the provisions of the Patriot Act. Some have suggested that Congress pass legislation that would sunset all aspects of the Patriot Act. The bill currently has sunset provisions that apply to selected portions of the legislation. But sunset provisions do not apply to the expanded powers given to the federal government which weaken the Fourth Amendment protections we are guaranteed under the Bill of Rights. The bill was touted as an emergency wartime measure, but some of the most dangerous aspects of the bill would continue on even after America wins the war on terrorism. It is time to revisit this bill and make some necessary changes.

Christian Perspective on Government and Privacy

Let’s focus in on the matter of government and privacy.

To begin with, Christians must acknowledge that Romans 13:1-7 teaches that civil government is divinely ordained by God. Government bears the sword, and that means it is responsible to protect citizens from foreign invaders and from terrorists. So on the one hand, we should support efforts by our government to make our society safer.

On the other hand, we should also work to prevent unwarranted intrusions into our privacy and any violation of our constitutional liberties. In the past, drawing lines was easier because an unconstitutional search was conducted by a person who came to your door. Today we live in a cyber age where our privacy can be violated by a computer keystroke.

In the past, 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, 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.

Second, get involved. When you feel your privacy has been violated or when you believe there has been an unwarranted governmental intrusion into your life, take the time to complain. Let the person, organization, or governmental agency 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.

Third, call for your member of Congress to take another look at both the Patriot Act and the Homeland Security Act. In their rush to deal with the imminent terrorist threat, Congress may have expanded federal powers too much. Track congressional legislation and write letters. 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 law enforcement. Eternal vigilance is the price of freedom. We need to strike a balance between fighting terrorism and protecting constitutional rights.

Notes

1. Cal Thomas, “More Power to the Government,” Nov. 21, 2002.
2. Michael Scardaville, “TIA Targets Terrorists, Not Privacy,” Nov. 22, 2002.

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.

Computers and the Information Revolution

The Impact of the Information Revolution

What has been the impact of the information revolution, and how should Christians respond? Those are the questions we will consider in this essay. Let's begin by considering how fast our world shifted to a computer-based society. At the end of World War 2, the first electronic digital computer ENIAC weighed thirty tons, had 18,000 vacuum tubes, and occupied a space as large as a boxcar. Less than forty years later, many hand-held calculators had comparable computing power for a few dollars. Today most people have a computer on their desk with more computing power than engineers could imagine just a few years ago.

The impact of computers on our society was probably best seen when in 1982 *Time* magazine picked the computer as its “Man of the Year,” actually listing it as “Machine of the Year.” It is hard to imagine a picture of the Spirit of St. Louis or an Apollo lander on the magazine cover under a banner “Machine of the Year.” This perhaps shows how influential the computer has become in our society.

The computer has become helpful in managing knowledge at a time when the amount of information is expanding exponentially. The information stored in the world’s libraries and computers doubles every eight years. In a sense the computer age and the information age seem to go hand in hand.

The rapid development and deployment of computing power however has also raised some significant social and moral questions. People in this society need to think clearly about these issues, but often ignore them or become confused.

One key issue is computer crime. In a sense, computer fraud is merely a new field with old problems. Computer crimes are often nothing more than fraud, larceny, and embezzlement carried out by more sophisticated means. The crimes usually involve changing address, records, or files. In short, they are old-fashioned crimes using high technology.

Another concern arises from the centralization of information. Governmental agencies, banks, and businesses use computers to collect information on its citizens and customers. For example, it is estimated that the federal government has on average about fifteen files on each American. Nothing is inherently wrong with collecting information if the information can be kept confidential and is not used for immoral actions. Unfortunately this is often difficult to guarantee.

In an information-based society, the centralization of information can be as dangerous as the centralization of power. Given sinful man in a fallen world, we should be concerned about the collection and manipulation of vast amounts of personal information.

In the past, centralized information processing was used for persecution. When Adolf Hitler’s Gestapo began rounding up millions of Jews, information about their religious affiliation was stored in shoe boxes. U.S. Census Bureau punch cards were used to round up Japanese Americans living on the West Coast at the beginning of World War II. Modern technology makes this task much easier.

Moreover, the problem it not limited to governmental agencies. Many banking systems, for example, utilize electronic funds-transfer systems. Plans to link these systems together into a national system could also provide a means of tracking the actions of citizens. A centralized banking network could fulfill nearly every information need a malevolent dictator might have. This is not to say that such a thing will happen, but it shows the challenges facing each of us due to the information revolution.

The Social Challenges of Computers

One of the biggest challenges raised by the widespread use of computers is privacy and the confidentiality of computer records. Computer records can be abused like any other system. Reputations built up over a lifetime can be ruined by computer errors and often there is little recourse for the victim. Congress passed the 1974 Privacy Act which allows citizens to find out what records federal bureaucracies have on them and to correct any errors. But more legislation is needed than this particular act and Congress needs to consider legislation that applies to the information revolution.

The proliferation of computers has presented another set of social and moral concerns. In the recent past most of that information was centralized and required the expertise of the “high priests of FORTRAN” to utilize it. Now most people have access to information because of increasing numbers of personal computers and increased access to information through the Internet. This access to information will have many interesting sociological ramifications, and it is also creating a set of troubling ethical questions. The proliferation of computers that can tie into other computers provides more opportunities for computerized crime.

The news media frequently carry reports about computer “hackers” who have been able to gain access to confidential computer systems and obtain or interfere with the data banks. Although these were supposed to be secure systems, enterprising computer hackers broke in anyway. In many cases this merely involved curious teenagers. Nevertheless, computer hacking has become a developing area of crime. Criminals might use computer access to forge documents, change records, and draft checks. They can even use computers for blackmail by holding files for ransom and threatening to destroy them if their demands are not met. Unless better methods of security are found, professional criminals will begin to crack computer security codes and gain quick access into sensitive files.

As with most technological breakthroughs, engineers have outrun lawmakers. Computer deployment has created a number of legal questions. First, there is the problem of establishing penalties of computer crime. Typically, intellectual property has a different status in our criminal justice system. Legal scholars should evaluate the notion that ideas and information need not be protected in the same way as property. Legislators need to enact computer information protection laws that will deter criminals, or even curious computer hackers, from breaking into confidential records.

A second legal problem arises from the question of jurisdiction. Telecommunications allows information to be shared across state and even national borders. Few federal statutes govern this area and less than half the states have laws dealing with information abuse.

Enforcement will also be a problem for several reasons. One reason is the previously stated problem of jurisdiction. Another is that police departments rarely train their personnel in computer abuse and fraud. A third reason is lack of personnel. Computers are nearly as ubiquitous as telephones or photocopiers.

Computer fraud also raises questions about the role of insurance companies. How do companies insure an electronic asset? What value does computer information have? These questions also need to be addressed in the future.

Computers are a wonderful tool, but like any technology poses new challenges in the social and political arenas. I believe that Christians should be the forefront of these new technologies providing wise direction and moral guidelines. We need Christians in the fields of computer technology and electrical engineering who can wisely guide us into the 21st century.

Principles for Computer Ethics

I would like to propose some principles for computer ethics. The first principle is that **one should never do with computers what he or she would consider immoral without them.** An act does not gain morality because a computer has made it easier to achieve. If it is unethical for someone to rummage through your desk, then it is equally unethical for that person to search your computer files. If it is illegal to violate copyright law and photocopy a book, then it is equally wrong to copy a disk of computer software.

A second principle is to **treat information as something that has value.** People who use computers to obtain unauthorized information often do not realize they are doing something wrong. Since information is not a tangible object and can be shared, it does not seem to them like stealing since it does not deprive someone of something. Yet in an information-based society, information is a valuable asset. Stealing information should carry similar legal penalties as stealing tangible objects.

A third principle is to remember that **computers are merely tools to be used, not technology to be worshiped**. God's mandate is to use technology wisely within His creation. Many commentators express concern that within an information society, people may be tempted to replace ethics with statistics.

Massive banks of computer data already exert a powerful influence on public policy. Christians must resist society's tendency to undermine the moral basis of right and wrong with facts and figures. Unfortunately, growing evidence indicates that the computer revolution has been a contributing factor in the change from a moral foundation to a statistical one. The adoption of consensus ethics ("51 percent make it right") and the overuse of cost-benefit analysis (a modernized form of utilitarianism) give evidence of this shift.

Fourth, **computers should not replace human intelligence.** In *The Society of Mind* Marvin Minsky, professor at the Massachusetts Institute of Technology, says that "the mind, the soul, the self, are not a singly ghostly entity but a society of agents, deeply integrated, yet each one rather mindless on its own." He dreams of being able ultimately to reduce mind (and therefore human nature) to natural mechanism. Obviously this is not an empirical statement, but a metaphysical one that attempts to reduce everything (including mind) to matter.

The implications, however, are profound. Besides lowering humans to the material process, it begins to elevate machines to the human level. One article asked the question, Would an

Intelligent Computer Have a “Right to Life?” Granting computer rights might be something society might consider since many are already willing to grant certain rights to animals.

In a sense the question is whether an intelligent computer would have a soul and therefore access to fundamental human rights. As bizarre as the question may sound, it was no doubt inevitable. When seventeenth-century philosopher Gottfried Wilhelm von Leibniz first described a thinking machine, he was careful to point out that this machine would not have a soul, fearful perhaps of reaction from the church. But this will be our challenge in the future: how to manage new computing power that will most likely outstrip human intelligence.

The Bible teaches that humans are more than bits and bytes, more than blood and bones. Created in the image of God, human beings have spiritual dimensions. They are more than complex computers. Computers should be used for what they do best: analyze discrete data with objective criteria. Computers are a wonderful tool, but they should not replace human intelligence and intuition.

Biblical Principles Concerning Technology

I would like to present a set of biblical principles concerning technology in general and computer technology in particular.

In essence, technology is the systematic modification of the environment for human ends. Often it is a process or activity that extends or enhances a human function. A microscope, for example, extends man’s visual perception. A tractor extends one’s physical ability. A computer extends a person’s ability to calculate. Technology also includes devices that make physical processes more efficient. The many chemical processes we use to make products fit this description of technology.

The biblical mandate for developing and using technology is stated in Genesis 1:28. God gave mankind dominion over the land, and we are obliged to use and manage these resources wisely in serving the Lord. God's ideal was not to have a world composed exclusively of primitive areas. Before the Fall (Gen. 2:15) Adam was to cultivate and keep the Garden of Eden. After the Fall the same command pertains to the application of technology to this fallen world, a world that "groans" in travail (Rom. 8:22). Technology can benefit mankind in exercising proper dominion, and thus remove some of the effects of the Fall (such as curing disease, breeding livestock, or growing better crops).

Technology is neither good or evil. The worldview behind the particular technology determines its value. In the Old Testament, technology was used both for good (e.g., the building of the ark, Gen. 6) and for evil (e.g., the building of the Tower of Babel, Gen. 11). Therefore the focus should not be so much on the technology itself as on the philosophical motivation behind its use. There are a number of important principles that should be considered.

First, **technology should be seen as a tool, not as an end in itself.** There is nothing sacred about technology. Unfortunately Western culture tends to rely on it more than is appropriate. If a computer, for example, proves a particular point, people have a greater tendency to believe it than if the answer was a well-reasoned conclusion given by a person. If a machine can do the job, employers are prone to mechanize, even if human labor does a better or more creative job. Often our society unconsciously places machines over man. Humans become servants to machines rather than the other way around.

There is a tendency to look to science and engineering to solve problems that really may be due to human sinfulness (wars, prejudice, greed), the fallenness of the world (death, disease), or God's curse on Adam (finite resources). In Western culture especially, we tend to believe that technology will save us from our problems and thus we use technology as a substitute for God. Christians must not fall into this trap, but instead must exhibit their ultimate dependence on God. Christians must also differentiate between problems that demand a technological solution and ones that can be remedied by a social or spiritual one.

As Christians we should see the value of technology but not be seduced into believing that more and better technology will solve social and moral problems. Computers and the Internet will tell us more about *how* people live, but they won't tell us how *to* live. Televisions, VCRs, and computers may enrich our lives, but they won't provide the direction we need in our lives. The answer is not more computers and more technology. The ultimate answer to our problems is a personal relationship with Jesus Christ.

A second principle is that **technology should be applied in different ways, according to specific instructions.** For example, there are distinctions between man and animal that, because we are created in God's image (Gen. 1:26-27), call for different applications of medical science. Using artificial insemination to improve the genetic fitness of livestock does not justify using it on human beings. Christians should resist the idea that just because we can do something we should do it. Technological ability does not grant moral permission.

Many commentators, most notably E. F. Schulmacher, have focused on the notion of appropriate technology. In Third World countries, for example, sophisticated energy-intensive and capital-intensive forms of agriculture may be inappropriate for the culture as it presently exists. Industrial advance often brings social disruption and increasing havoc to a society. Developing countries must use caution in choosing the appropriate steps to industrialize, lest they be greatly harmed in the process.

I believe we should resist the temptation to solve every problem with computers. Our society today seems bent to putting computers in every classroom and in every place of work. As helpful as computers may be, I believe we need to question this seemingly mindless attempt to fill our world with computers. They are a wonderful tool, but that is all they are. We must be careful not to substitute computers for basics like phonics, mathematics, logic, and wise business practices.

Third, **ethics rather than technology must determine the direction of our society.** Jacques Ellul has expressed the concern that technology moves society instead of vice versa. Our society today seems all too motivated by a technological imperative in our culture. The technological ability to do something is not the same as a moral imperative to do it. Technology should not determine ethics.

Though scientists may possess the technological ability to be gods, they nevertheless lack the capacity to act like gods. Too often, man has tried to use technology to become God. He uses it to work out his own physical salvation, to enhance his own evolution, or even to attempt to create life. Christians who take seriously human fallenness will humbly admit that we often do not know enough about God’s creation to use technology wisely. The reality of human sinfulness means that society should be careful to prevent the use of technology for greed and exploitation.

Technology’s fruits can be both sweet and bitter. C.S. Lewis writes in *The Abolition of Man*, “From this point of view, what we call Man’s power over Nature turns out to be power exercised by some men over men with Nature as its instrument. . . . There neither is nor can be any simple increase of power on Man’s side. Each new power won by man is a power over man as well. Each advance leaves him weaker as well as stronger. In every victory, besides being the general who triumphs, he is also the prisoner who follows the triumphal car.”

Christians must bring strong biblical critique to each technological advance and analyze its impact. Computers are a wonderful tool, but Christians should constantly evaluate their impact as we live through the information revolution.