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.