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.