

An Electronic Bill of Rights
In Cyberspace, You Are Guilty Until Proven Innocent

You know, I tend to feel violated when I receive endless masses of junk mail that overflow from my undersized mailbox.

We can all travel back to our school days when we studied the Constitution and amendments added to it over the last two hundred years. Most Americans are acutely familiar with at least a few of those amendments, but perhaps the most familiar of all are the first ten amendments, also known as the Bill of Rights.

Today they are the envy of populations world-wide. They were meant to be a strong vehicle to protect our individual freedoms and liberty as our nascent country evolved into a great nation. Many of us forget, however, that as tourists in foreign countries, we are no longer protected by the rights that we take for granted here. In Mexico, there are no civil rights as we know them. In England, the press can be summarily banished from publishing information deemed harmful to that country - without the need for a trial or other due process. And those are our friendly neighbors!

While we sit idly by in our idealic national setting, however, there are great changes occurring around us, and indeed, many of those changes are having a distinct impact upon those original rights upon which this nation was founded.

We find that as technology improves our daily existence in ways unimaginable only a decade ago, that same technology has permitted a creeping loss of personal freedoms, liberties and privacy to invade our national essence.

Two hundred years ago, for example, the concept of public records was consistent with the goals of an inchoate democratic society. It meant that I, as an American, could mount my horse, ride down the elm-tree covered dirt lane, get saddle sore from the ten mile ride and freely enter the wooden courthouse. Once there, I could look through the public records and find out who bought the farm next door.

Today, though, with a single request of a professional data banker, (or if I have the wherewithal myself) I can dredge up the most private information on most any American, compile it, analyze and come to conclusions about that person without his consent or knowledge. Our identities have been

reduced to a virtual agglomeration of streams of data which is ripe for the picking with the simplest equipment and a minimum of keystrokes.

In many ways, our greatest national asset, our technology, is also the greatest weakness and vulnerability to our personal privacy. I find a comfortable solution to the complex dilemma in which we find ourselves is the creation of an Electronic Bill of Rights; a new set of guidelines which firmly and clearly establish the rights of the individual in an intangible and invisible world.

You Own You

This simple concept must be the premise of an Electronic Bill of Rights. You have legal authority over your body (I hope my female readers will excuse my not including Roe/Wade issues in this short essay). If you are physically struck, you have both legal and physically defensive recourse. You even have legal authority over your possessions. If someone steals your TV, they can go to jail.

I suggest that we must establish a parallel set of concepts over the digital 'You,' that electronic projection which defines who you are and how people perceive you in Cyberspace.

Do you own or have any real control over your electronic identity? Not much today. Consider that the average American's name is housed within 50,000 or more computer data bases along with different facts (or mere opinions) about you. Your name and that information is bought, sold and traded between five and ten times a day. Is that what we really want? Should a commercial concern with whom you have dealt be permitted to use that data for additional marketing purposes, or sell that information to other private organization?

I suggest a simple set of guidelines by which we can restore a great deal of our electronic privacy.

1. You own your name, and all of the information that resides along with it. People with whom you deal in commerce may not, without your explicit permission, be able to sell or use your name or its associated data for any purpose. (It is reasonable to exclude legitimate law enforcement needs.) We should perhaps consider the concept of royalty payments to individuals who do not object that they are added to an infinite supply of marketing lists.

2. Organizations who hold digital information on you will be required to protect that

information according to yet to be determined security criteria. This includes employers and records about their employees, banks who hold critical financial information about you, brokerage firms, doctors, insurance companies and so on. We have to reestablish confidence on the part of our citizenry.

3. Organizations who have your name in a data base, must, at least once a year, advise you that you are in their files. At your option, you may request a copy of all files and information they store on you, (perhaps at a reasonable fee of a couple of dollars.) This is critical because the untamed growth of the 'Digital You' is where the crux of the loss of privacy problem begins.

4. You must have recourse. Today, albeit with great difficulty, the credit reporting bureaus are obligated to release your personal files to you upon request. They are further required to investigate and correct any errors or omissions if you ask. We must extend this concept much further. Insurance companies have access to your medical files but you do not. A single keystroke, an error, can transform a healthy person into a doomed HIV victim, and that person has no simple route for detection or correction. That is just downright wrong. People and organizations make decisions about you, the individual, based upon opinions, data and human error over which he has absolutely no control.

5. One large grocery chain in Chicago sent letters to its customers who used the store's debit card. "We want to tell you that for the last couple of years we have been secretly collecting information on your purchases. Once we decide, we will let you know what we are going to do with this information." Wrong. They should be able to do nothing more than fill their shelves because I bought all of the Ring Dings. I do not want Twinky and Hostess Cup Cake solicitations just because I bought a competing product. An organization should only be able to collect that information about you or me that is essential to complete the transaction, and once that transaction is completed, all unnecessary information should be deleted unless I give you explicit permission otherwise.

These simple concepts are core component of the Electronic Bill of Rights. But we face a number of related issues that must be sorted out before we can say there is equality and privacy in Cyberspace.

Government Privacy

The Government keeps a lot of secrets. Military secrets, legislative secrets and they have developed a means to classify those secrets. In general, there are five levels:

- Unclassified. Anything goes, anyone can have it to look at it. We call this open source information.

- Sensitive by Unclassified. Information which should receive some degree of protection, but not a whole lot.

- Classified, Secret and Top Secret. These are different levels of real secrets, and individuals with access to this information must undergo some degree of scrutiny to be permitted access to it.

The issue I care about is that the information the government holds on you and me; our tax records, medical records, social security files and so on, are not considered classified. The general press has covered stories about the abuse of this information when accessed by individual both inside of and outside of the government, and then used for profit, harassment, or even murder.

I would like to see an additional security sensitivity added. Perhaps we call it "Personal," which is assigned to all private and personal information about Americans that most of us want to be kept confidential between us and the government.

We would want to assign technical security criteria to that classification which would cover such issues as who can access it, what may be done with it once accessed, how easily it may be moved from one computer to another, and specifically, if it is ever permitted to leave the government's control without explicit permission. In addition, more stringent punitive steps must be available to prosecute those who violate these rules.

This step alone would do a great deal to restore confidence in the privacy rights that Americans want to formally establish.

The First Amendment

The rest of the world envies us for this most precious right - freedom of speech. As Americans we may hate an extremist or opposing or offensive viewpoint, yet we also defend to the death their right to say it. The denizens of Cyberspace - fifty million of us - want to insure that the first amendment is not a footnote in history, relegated as a local ordinance reserved for paper and TV and voice.

We have to ask, do we still have the right of free speech as we were taught in school?

It depends on the circumstances. If we threaten the President, we can't use the First

Amendment as a “get out of jail free” card. Bomb jokes at airports and yelling FIRE in a movie theater are notable exceptions to the first amendment's protections. Barring physical threats, we can voice just about any opinion we want: just listen to any politician voice his in a heated race.

But there are differences we find in Cyberspace that do not provide clear cut answers. So I return to the concept that we have to decide what we want, and how we want our country to be in the future; and not to sit by and idly let a chaotic electronic future descend upon us.

Active and Passive Publishing

With the emergence of Cyberspace as a global means of communication, we find there are two very distinct types of publishing. Passive and active. All of us with inexpensive hardware can publish our thoughts on the Information Highway. The active publisher transmits data/information from their electronic address to yours. He sends it to you.

Physically we are subjected to ever increasing amounts of junk mail and the same thing is occurring in Cyberspace with list servers, spamming and over-marketing. No matter what we do , we can't escape it! However, we must be good stewards of our technology and stay vigilant that electronic junk mail doesn't eat up our valuable computer resources - especially for those who have to pay by the kilobyte. Active publishing may also mean that you have requested materials such as electronic newsletters which are then actively sent to you.

We meet such issues here as electronic stalking, electronic harassment and propagandizing entire populations. What recourse do we have when we are subject to endless and perhaps annoying electronic transmissions? Again, we have to decide what behavior is acceptable, which is not, and come to grips with as much as we can within our own national borders.

Now, think of passive publishing in Cyberspace as resembling a large library. The Web perhaps. The librarian compiles information and places it on the server for you to retrieve. If you want it, you have to go after it. You actively solicit and search out the material and then choose to bring it into your domain. In Cyberspace the information may be free to you or you may need to enter a security code, a password, or a credit card if the information is for sale.

The technical differences between the two publishing methods demand that we find appropriate rules for both methods that tie in with the idea of freedom of speech.

· **Censorship**

I don't favor electronic censorship guidelines chosen by the government. I am a great fan of self censorship (not by intimidation) and personal responsibility. I do not object to the proposed V-Chip because it places the responsibility upon the parents or viewer to determine what is acceptable to them. I do not want the government telling me that Baywatch is too racy if I choose to enjoy watching lycra bathing suits in motion.

Censorship is the antithesis of what this country was founded upon and we should aggressively counter the small minded special interest groups who know best what information is right for you and me. Because, if at first they censor what you don't like, and then they censor what someone else doesn't like, then one day, it might be my turn, and I will censor you. It's a vicious downhill slalom certain to end in disaster, and we must make sure we don't leave the starting gate. Never.

In 1994, a Tennessee postal inspector electronically ordered adult oriented materials from a couple (man and wife) in California where they were breaking no laws whatsoever. Upon receipt, he indicted them in Memphis, Tennessee, where they stood trial for violation of local obscenity laws - and lost!

Is this what we want? In such a fashion, any local yokel ordinance takes legal precedence over that of a distant location, and permits selective remote control enforcement. Is this really what we want, or is it time to lock our personal rights to our physical location?

As a parent of a young girl and boy, I can clearly understand how parents become distraught when their children have complete access to inappropriate materials as they explore the Information Superhighway. In Cyberspace, there is so much "R", NC-17 and XXX material available to children that it would make a drunken sailor blush. And much of that material is clearly illegal throughout the entire United States. Do we arrest the country of Denmark because its culture and laws are different? Of course not. Better technical solutions are being developed. We have to learn personal responsibility, engage in better parenting and quit trying to blame the other guy.

Bad law is not a solution for poor engineering.

· **The Fourth Amendment**

Think about the Fourth Amendment. Its concepts includes “secure in house, papers, and effects” from unreasonable search and seizure. Does that amendment cover information that may be housed on a disk or information you can pick up on the Internet? That amendment has become a prime example of decaying legislation which is no longer relevant. Information is not in the same place where it was for our forefathers. Life was simpler then! So what is the litmus test for the need to confiscate information? The American Civil Liberties Union, a watchdog of our personal freedoms, represented by Ira Glasser, stated “Because of the Supreme Court rulings, the Fourth Amendment has become a relic of formalism: it protects the places where private information use to be, but not the places where it is today.”

We must specifically migrate the concept of the fourth amendment into Cyberspace so we all know exactly where we stand.

Providers Versus Publishers

Should an Internet provider be sued or penalized because the content of its computers were in violation of the law? Prodigy was sued because one of its customers placed allegedly libelous statements in a public forum about a financial company. Was that Prodigy's fault? The court says yes, because it was a moderated forum. The implication here is that a forum moderator, say on the subject of Mayan Sun Tanning Lotions must also be a legal expert on what is a libelous statement or not. I don't think so.

No more than the telephone company is held liable for obscene telephone calls should an electronic provider be responsible for the contents of its computers. Lawrence Livermore Lab computers were found to contain 30,000+ pornographic images which made it a popular destination for lots of Net surfers. Should they be responsible?

The Electronic Bill of Rights must spell it out.

CyberCops

Should we allow police to monitor and eavesdrop data networks, search Cyberspace and come up with incriminating evidence? We have no choice but to draw a line in the sand dictating what is acceptable and unacceptable modus operandi for law enforcement officers. If an E-Mail transmission on America On Line contained a plan to rob Fort Knox who would we hold

responsible? How much monitoring of Cyberspace do we as a society want? My local police department entrapped and caught an electronic pedophile while masquerading as a young teen on the Net. We naturally think that is good, but we must choose how far we are willing to go, what rights we are willing to give up in order to maintain a lawful society.

- **Viruses and the First Amendment**

Many of us who have had those dastardly virus' crash our systems and have thought about the need to outlaw that type of software. Cyberspace needs to take a hard stand on the issue of malevolent software. The arguments can go on forever. They have the right to "write" the virus....or do they? Suppose serious damages occur from malicious software? How about poor Joe Blow Programmer who inadvertently screws up and his error causes damage? Do we throw him in the slammer?

We have to keep in mind that the only difference between malicious software and a deadly programming error is intent. Let's not make criminals out of experimenters.

- **National Security**

There is a fuzzy line between national security and the rights of our citizens. Our national security defenders want to get their voices heard about freedom of speech and shout when it comes to encryption. The export of excellent cryptography is restricted by the NSA, but I think we will need a definition of "export" and propose means to enforce it in light that the Department of Justice chose not to indict Phil Zimmermann.

The government has been remarkably slow to develop workable solutions that meet both the legitimate needs of the individual and Americans and American interests, and the real needs of law enforcement. Despite years of public debate, only a handful of technical approaches are on the table.

Anonymity and Identity Replication

Kevin Mitnick assumed my electronic identity on the Net to wage a war of words against one of his adversaries. I had a lot of explaining to do to the press: "No, it wasn't me."

Tantalizing entertainment to some, malicious to others, spoofing identities on the Net occurs with increasing regularity. While most of us probably say spoofing is a bad idea, should it be made illegal? Or do we just ignore it as foolish shenanigans.

And what about electronic anonymity? Through such sites as penet.fi in Finland, any of us can acquire an anonymous identity and surf the net wildly, with the prospect of suffering no personal indignities or repercussions. After all, no one knows who we are.

Guilty Until Proven Innocent

An Electronic Bill of Rights is critical if we are to maintain some semblance of order as we move into the twenty-first century. There are many questions and we have only begun to explore the possibilities and endless issues that will be created as we make our great electronic leaps forward.

Have you ever had the experience of a mistake on your credit report? Argue with your bank about an incorrect transaction? Take on the IRS because they miscalculated your 1040? We are judged by others and they base their judgements upon the contents of computers over which we have little or no control, access or recourse.

We are presumed guilty until we go to the walls supplying our burden of proof of innocence. That is the opposite of the premise of our legal system. If the data entry is incorrect, too bad. We assume the computer is right even when the person who entered the data is wrong.

Taking on the credit bureaucracy means give yourselves plenty of expendable time because you will be placed on hold, maneuvered through voice mail hell, or sent to the wrong extension by some human operator who really doesn't give a damn about you. In our busy lives, some of us don't take time to review our statements, bank accounts, credit report. The creeping control of computers over our lives grows daily and must be placed under arrest until we can design a legal and ethical construct that echoes our beliefs and desires.

The Media

Alvin Toffler once said that if we control the media, we destroy democracy. If we don't control it, then they will.

Cyberspace provides an infinite variety of information sources - true news anarchy. The

tantalizing migration of big companies into Cyberspace will spawn a shakeout that has occurred within virtually every growth industry since the industrial revolution.

With the media, though, we have to be careful. The FCC regulates how many news outlets a company can have: TV stations, radio stations, newspapers. But what about in Cyberspace? How do avoid the historical tendency for a few huge companies to dominate a field and in this case control the distribution of information?

We are crying our for answers

Conclusion

As the original Bill of Rights was meant to protect America's citizenry in a physical world, an Electronic Bill of Rights is meant to provide similar protections in the intangible nether world of Cyberspace

What is required is vision. Vision to take a look at the future, accept the risks and opportunities to our personal freedoms, and construct and legislate a guide for our future. We must design the future we choose, not accept one that we helplessly slide into/

Our lives truly are “open books” and the Electronic Bill of Rights I propose closes the book on that abuse.

As an old Chinese proverb says: "If we don't change directions, we are go to end up where we are going." I know that's not what most of us want.