Cyberspace Wars : Microprocessing vs. Big Brother

Daniel Brandt
July 1993

Just ten years ago the issues were so simple, the arguments so clean. The concept of hackers was cute and quaint, best understood through Hollywood thrillers like *WarGames*. The major media had yet to use the word "cyberspace", a term just then created by William Gibson in *Neuromancer*, his first masterpiece in a strange new genre of "cyberpunk" fiction.

It was ten years ago that establishment liberal David Burnham wrote *The Rise of the Computer State* with Ford, Rockefeller, and Aspen Institute money. This book ignored microprocessing and limited its nightmarish vision to the dangers posed by Big Brother's mainframes. One chapter covered the threat posed by the National Security Agency (NSA), the largest U.S. intelligence agency with the world's best computers, an agency that is not subjected to any oversight. In the mid-1970s the Senate Intelligence Committee headed by Frank Church warned that "if not properly controlled", the NSA's technology "could be turned against the American people at a great cost to liberty". For thirty years the NSA obtained copies of most telex messages entering and leaving the U.S., and the CIA illegally intercepted thousands of first-class letters as they left the country. If the high-tech NSA were ever turned against us, Church said, "no American would have any privacy left... There would be no place to hide" [1].

One word -- privacy -- summed up the debate nicely then, because Big Brother had a monopoly on computing power. But some cracks were already appearing in this pre-cyberspace version of the problem. In 1978 the Carter administration admitted that the Soviets were tapping into microwave links in New York, Washington, and San Francisco; microwave was like a sieve compared to the old underground intercity telephone cables. That was only a minor irritant compared to January 15, 1990, when half of the entire AT&T network crashed due to a single software bug. The technicians in the hardware lab where I worked used to kid the software engineers, saying that if civilization had developed the way programmers write programs, one woodpecker could come along and bring it all down.

Also in 1978 the NSA began harassing certain mathematicians in the private sector, claiming "sole authority to fund research in cryptography" [2]. Then came the microprocessor. Within a few years every mass-market magazine for microcomputer hobbyists was running an occasional article on new encryption techniques, and the NSA couldn't keep the lid on. Hackers were experimenting on their crude machines with a technique called "public key cryptography" [3]. A recent estimate has it that "a buildingful of NSA's specially hot-rodded supercomputers might take a day to crack a 140-digit code", but from NSA's point of view that's not good enough. Today's micros are roughly 100 times faster with 100 times the capacity of the machine I bought ten years ago; the price is lower and it fits on your lap. They can easily encrypt and decrypt with keys this size. While the world's most powerful supercomputer grinds all day to crack one key, "what is it going to do when 100 million people each use 100 different keys per day ?" [4]. Big Brother has suddenly lost his monopoly on encryption technology, and hackers everywhere could not be more delighted.

Yes, the rules of the game have changed, due primarily to the rapid evolution of microprocessing power. The simple concept of "privacy" no longer works as well as it did for Frank Church and David Burnham. The little guy on his microcomputer bulletin board system (BBS) -- by one estimate there are now 60,000 of these in the U.S. [5] -- wants privacy from Big Brother, but corporations will also be screaming for privacy as they adopt the

new encryption technology. And then what about transnational corporations seeking to avoid government intrusion ? Or organized crime and international drug cartels ? One, two, many Big Brothers ? Privacy for whom ?

William Gibson's vision in *Neuromancer* may read like heaven for hackers, but for the rest of us the term "cyberpunk" seems about right. We shudder at Gibson's future, where transnational corporations hold all the wealth and all the information, and outcast data pirates must jack into their cyberspace decks, maneuver around the "black ice" of corporate data security systems, and forage for their livelihoods. It's rather like children stealing food from garbage cans, but it all seems like ice cream to the hackers who find this inspiring.

The hacker ethic is a laissez-faire vision of total freedom to microcompute and telecommute, a world of unbreakable encryption, anonymous E-Money transfers, and lately talk of a fiber-optic data superhighway, leading to a place in cyberspace where everyone can connect with anyone. They even have their own Washington lobby. Electronic Frontier Foundation (EFF) started out with funding from Mitch Kapor and a few other computer millionaires, but is now underwritten by IBM, Apple, Microsoft, AT&T, MCI, Bell Atlantic, Adobe, the Newspaper Association of America, and the National Cable Television Association [6]. And the word "cyberspace" is trumpeted in *Scientific American*, *Time*, *Washington Post*, and *The New Republic*. We can expect to see it soon in Webster's. This is bigger than a handful of hackers, and it's time to become conversant with the issues.

There IS a new reality, and we needed a new word. But more than a mere reality, it's a massive moving target careening blindly into the future. No one has a handle on it. Cyberpunk novelist Bruce Sterling worries about hacker ethics, one narrow slice of the big picture, but he doesn't pretend to have many answers [7]. The Washington office of Computer Professionals for Social Responsibility (CPSR) is in the same building as EFF, and both work against the NSA's efforts to mandate encryption hardware that the government can break -- the so-called "Clipper Chip" that was announced by the White House on April 16, 1993 [8]. But on other issues CPSR is suspicious of EFF's pro-corporate leanings. One imagines CPSR arguing that our government, at least, can be petitioned and our representatives are elected. Comparatively, how much input are we allowed by major corporations ? Given their priorities, how responsive will they be to the information needs of the poor and underprivileged ? What will happen, for example, if public libraries and public schools get left behind in the dust of the data superhighway ?

In Washington DC, the information capital of the world, the newest game in town is Cyberspace Wars. Unfortunately, it's also the latest buzzword. Pack journalists in this town are seemingly required to log in on these, which invariably generates more heat than light.

I don't have a graduate degree, but I spent three years in grad school studying something they called "social ethics", which included much philosophy. My undergraduate degree is in sociology. In high school I had a ham radio license, and spent many evenings building equipment and working traffic networks, a Morse Code version of "cyberspace" (these days my transmitter is hooked to my computer). After grad school I retrained in electronics, and during the 1980s I held a variety of hardware and software jobs in high-tech industries. The hardware ranged from telephone interface circuits to digital switches at the senior tech or junior engineer level. The software was generally written using Assembly, dBase or BASIC to develop hardware control systems or database programs.

In other words, my career is so checkered that no one will ever refer to me as an "expert", which is also why you are reading this in an obscure little publication. But I am familiar with the territory. And could it be that too many of the experts are too narrow ? Furthermore, I can recognize high-tech hype when I see it and I can recognize sloppy ethics; there's too much of both in cyberspace. I can forgive EFF guru and co-founder John Barlow, a former Grateful Dead songwriter, for being an "acid-head ex-Republican county chairman" (Mitch

Kapor's description). But when he invokes Pierre Teilhard de Chardin's "noosphere" as a model for cyberspace, a "global brain that would seal humanity's spiritual destiny" [9], I have to draw the line. I studied enough of Teilhard to know that his theology lacks any conception of evil. Where cyberspace and New Age meet out in California's Silicon Valley somewhere, everything becomes alarmingly mushy.

Another example of sloppy ethics is found in the way the word "privacy" is babbled about without qualification. I have yet to see any suggestion that the right to privacy ought to be inversely proportional to social power, and should be balanced against the right to know. Joe Sixpack deserves more privacy than David Rockefeller, because Joe's simple livelihood may be affected by Rocky's wheeling and dealing. Joe has more of a right to know what Rocky is up to than vice-versa. It does not require a philosophy degree to grasp this; libel law in the U.S., for example, makes a similar distinction between a public figure and a private figure. Every journalist knows this, but when writing about privacy issues the same concept never makes it into print. Then again, my definition of privacy does not justify hacker ethics (microcomputer vs. mainframe, little guy vs. Big Brother), because hackers are motivated more by malicious amusement than by genuine self-defense.

More hype comes from a bizarre intersection of cyberspace with conspiracy theory : the incredible PROMIS software by Inslaw, Inc. For months I was reading accounts of how this software was revolutionary, and could track everything about everyone. This is crazy, I thought, because as a programmer I knew that software is painfully developmental, never revolutionary. After ten years of inputting for NameBase I also knew that until you key in good data, a mere database program is nothing at all. Then it came out that there was a "back door" installed in PROMIS. This made more sense, as a "back door" to get around password protection is easy for any programmer, and it explained why the intelligence community might be interested in peddling it to foreign governments.

Please note, however, that you still need physical access to the computer, either through a direct-connect terminal or a remote terminal through the phone lines, in order to utilize a back door. Ari Ben-Menashe wants us to believe that foreigners (Britain, Australia, Iraq, South Korea, Canada, and "many others") allow technicians from another country to install new computer systems in the heart of their intelligence establishments, and don't even think to secure physical access to the system before they start entering their precious data.

Then he claims that PROMIS, "a sinister, Big Brother-like computer program", can suck in every other database on earth, such as those used by utility companies, and correlate everything automatically. The rest of his book is frequently believable, but this example of hype is grating because publisher Bill Schaap, who is not computer illiterate, should have done Ben-Menashe a favor by deleting the chapter on PROMIS [10]. I generally believe that "conspiracy is the normal continuation of normal politics by normal means" [11], so I don't like to see whistleblowers like Ben-Menashe needlessly discredited by their own high-tech gullibility.

The last example of hype is from a 1988 article, which suggests that the right also suffers from an overactive technical imagination :

> Retired Maj. Gen. John K. Singlaub, a member of the board, says Western Goals wanted to build a computer data base containing the leadership structure and membership of every left-wing group in the country. The right, he says, needed to match the left's ability to mobilize on short notice and track the activities of conservative Americans. "The radical left", he claims, "in this country has an incredible, computer-connected network that has enormous files connected with them" [12].

Singlaub swallowed someone's line the same as Ben-Menashe did, and just as journalists are inclined to do when it comes to high-tech issues. It is no longer excusable for major players to remain ignorant of important high-tech developments. The remainder of this article will follow the battles and trends of the last few years --

the Cyberspace Wars that unfolded as microprocessors robbed Big Brother of its monopoly on data access and manipulation. Then I'll propose a somewhat expanded, more useful definition of "cyberspace" to include all digitized information, and consider the issues involved in the potential data networks that worried Singlaub. His notion of the left was fantastic and his plans for Western Goals never materialized. But the Anti-Defamation League of B'nai B'rith, which is beginning to use computers, was caught this year in a massive spying scandal. Their defense of spying is my ultimate example of sloppy ethics. In another ten years there might not be scandals, because the files will have been sucked into cyberspace, complete with unbreakable encryption and access by anonymous players. It may not be the NSA, or the ADL, or any current entity. But we will all be at risk, and Ben-Menashe, Singlaub, and the cyberpunk novelists will finally seem prophetic.

Privacy and domestic security are a zero-sum game. Society consists of discrete individuals; if these individuals each have total privacy, then society has zero security. Conversely, for the body politic to have total security as an organism, the individuals within must have zero privacy. Idealists may quibble with this scenario, but today we're required to coexist with massive national security establishments, and they tend to see things this way. Realistically, then, it's a useful handle for understanding Cyberspace Wars.

A 1992 Harris poll showed that 78 percent of Americans now express concern about their personal privacy, and 68 percent perceive a threat from computers. These figures have roughly doubled over the last twenty years [13]. One area of concern is in the workplace, where U.S. privacy laws lag behind those in Europe and Japan. Although the 1986 Electronic Communications Privacy Act (ECPA) prohibits phone and data-line tapping, law enforcement and employers are exempted, so an E-Mail system that is paid for or run by the employer might not be secure. Macworld asked 301 companies about snooping, and "about 22 percent of our sample have engaged in searches of employee computer files, voice mail, E-Mail, or other networking communications" [14]. Job applicants sometimes find that the company has a contract with a research service to scan credit reports, workers' compensation claims, medical records, and criminal histories. Access to some of this data for such a purpose has recently become illegal, but employers say they need this data because of the rash of "negligent hiring" lawsuits.

Personal privacy is a problem outside the workplace as well. Surveys of the data available from the big three credit bureaus -- TRW, Equifax, and Trans Union -- find error rates of up to 43 percent. Federal laws have addressed this issue for years, and more may be on the way. Lately the credit bureaus have seen their monopoly on personal information eroded from a variety of commercial information brokers (over 1,253 are listed in the Burwell Directory). Most of these collect information on companies, but some specialize in records such as address, marital, salary, driving, and employment history, as well as corporate affiliations, who your neighbors are, vehicle and real estate holdings, and civil and criminal court records. Lotus Development Corporation (where Mitch Kapor made his millions) and Equifax recently proposed to compile some of this data for 120 million consumers on CD-ROM, and market it for $700 as "Marketplace : Households". But 30,000 angry letters killed their proposal [15].

If it's only name, address, and telephone number that interests you, then check out ProPhone. This is a set of seven CD-ROM disks consisting of 70 million residential and 7 million business listings. The software can access the listings through either the name, address, or phone number, and the business listings are indexed by SIC code as well. The listings tend to be at least several years old or otherwise incomplete, but this will improve over the next few years. We bought it because most NameBase users are investigative journalists. Zeroing in on a neighborhood where you lived as a child in a little town in North Dakota, and getting a printout of today's residents, feels something like what hackers must feel when they break through password protection. It also feels like an excellent reason to keep one's own number unlisted.

While cyberspace trends give privacy advocates plenty to worry about, the situation is equally alarming from the perspective of the government. If you live in an apartment building and have a scanner, your neighbors'

cordless telephone conversations are easily monitored. Cellular phone monitoring became illegal in 1986 but not cordless, which is reasonable because no one HAS to use a cordless phone. The law against cellular monitoring was opposed by hams and shortwave listeners, who generally feel that if the signal makes it into their living rooms, they have a right to tune it in. Last year President Bush signed a second law, prohibiting the manufacture or import of scanners that are capable of cellular monitoring. But in a demonstration for a congressional subcommittee last April, a technician took three minutes to reprogram a cellular phone's codes so that it could be used for eavesdropping. It turns out that you don't have to use a scanner at all : "Every cellular phone is a scanner, and they are completely insecure", John Gage of Sun Microsystems told the subcommittee [16]. Congress keeps slipping off the back end of the cyberspace curve, simply because the curve is moving so fast.

Congress is caught in the middle, pulled in one direction by privacy advocates and the other by our national security establishment. In March 1992 the FBI proposed legislation that would require private industry to provide access ports in digital equipment for the purpose of tapping specific conversations. Telephone carrier signals are increasingly digitized and multiplexed, with specific channels interleaved among many others in a continuous stream of ones and zeros. For decades, the FBI needed only a pair of alligator clips to tap phones, and now they're getting panicky. This particular proposal died, but the FBI is going to try again. Several years ago I worked for a little company that made analog long-distance equipment for export to Soviet bloc countries. Frequently the specifications called for an access port for each channel, which we dubbed the "KGB output". Now it turns out that the FBI wants the same thing.

Not to be outdone, the NSA played the major role in the development of the "Clipper Chip" recently approved by President Clinton, and soon the government will start requiring industry to provide phones and computers equipped with it. This chip contains encryption algorithms that can be broken by two halves of a secret master key. The idea is that someone with a warrant will then go to each of two agencies to get the portion of the key in their custody, like two pieces of a treasure map torn in half. This chip will be used to scramble phone lines used for voice, modems, and fax machines. Presumably the NSA already has both halves of the key, and their record for self-restraint is not reassuring. Private industry is not enthusiastic. For one thing, U.S. products containing NSA-breakable encryption will not compete well on the international market. One person asked, "Do you think I'm dumb enough to buy something endorsed by the NSA ?" [17].

Some worry that the administration may try to ban encryption altogether if this chip doesn't catch on. Ham radio operators, for example, have for decades been prohibited from using encryption on the air, and export of encryption software has been restricted for years under COCOM regulations. Others are amused that the government is even bothering along these lines, since encryption that is practically unbreakable is already easily purchased, or even available as shareware by downloading it from a BBS.

The most dramatic conflict between privacy and security occurred in 1990. Big Brother was already edgy, as BellSouth in Florida had discovered in mid-1989 that microcomputer intruders had been harmlessly reprogramming their digital switches. It seems that callers to the Palm Beach County Probation Department were reaching "Tina", a phone-sex worker in another state. BellSouth was not amused, and worried that their 911 system was vulnerable. Then when the AT&T system half-crashed the following January -- even though this was NOT hacker-related -- the Secret Service, which had nothing if not an active imagination, began working closely with telco cops. The federal effort started years earlier after Congress passed the 1986 Computer Fraud and Abuse Act, but in May 1990 it culminated in Operation Sundevil, by far the largest series of high-profile raids ever conducted against hackers. About 42 computer systems were seized around the country, along with 23,000 floppy disks.

Federal anti-hacker strategy involves a dramatic search and seizure. Agents crash simultaneously through the front and back doors, everyone is questioned, and then they carry off the evidence : computers, monitors, keyboards, printers, modems, manuals, disks, notebooks, telephones, answering machines, and even Sony

Walkmans. There are no arrests and even much later charges are rarely filed. In the meantime, however, the feds study their "evidence" for months or even years. It's enough to bring many hackers to their knees.

EFF began defending these hackers, and by 1991 the steam had gone out of the crackdown. One document, a description of 911 system administration called "E911", was found on a BBS and came to the attention of AT&T security. They considered it hot property worth exactly $79,449. E911 later formed the basis of one of the hacker prosecutions, but the government's case fell apart when the defense showed that more detailed information about the 911 system was publicly available from AT&T for the mere price of $13 :

> The right hand of Bellcore knew not what the left hand was doing. The right hand was battering hackers without mercy, while the left hand was distributing Bellcore's intellectual property to anybody who was interested in telephone technical trivia... The digital underground was so amateurish and poorly organized that it had never discovered this heap of unguarded riches [18].

Another hacker legal victory resulted from a raid against Steve Jackson Games of Austin, Texas. SJG published games that were played on paper, with pencils, dice, and books. Jackson and his fifteen employees used computers to run the business, not for hacking. One of the games he developed was published as a book titled *GURPS Cyberpunk*. Upon seeing the word "cyberpunk", our fearless G-men assumed that the E911 document was lurking on SJG's computers. The warrant was sealed, however, so for months the SS led everyone to believe that they carted off SJG's computers because SJG presumed to publish a science fiction book. This naturally resulted in much sympathy for the defense. Without its computers the company was crippled, and had to lay off half of its employees.

In 1991 the company sued the government, and on 12 March 1993 a federal judge in Austin awarded the company $42,000 for lost profits in 1990, plus expenses. He also ruled that the Secret Service violated the 1986 ECPA because it had seized stored messages from many users of the BBS who were not suspected of anything. Several hackers in other cases have actually gone to prison over the last few years. But considering how sociopolitically stunted many hackers were until EFF finally sent in some lawyers, it's amazing how little the government has to show for all of its dramatic efforts.

The term "cyberspace" is normally meant to convey that fuzzy area between two digital devices, like the term "airwaves" that refers to a thin slice of the spectrum most often used for communications. But only a small portion of this accepted notion of cyberspace is in the form of microwave links; the rest is plain old traces or wires, from inside the microprocessor chip all the way to the telco office and beyond. Before "cyberspace" finds its way into the dictionary, I propose an expanded definition which will place the emphasis on the unique nature of digitized information. Any digitized information is already in cyberspace, whether it's in a file on a floppy, a CD-ROM at your local library, or a minicomputer on an Internet node. Once digitized, information takes on an entirely new quality; it is this quality that begs for a new word to describe it.

First and foremost, digitized information can be copied locally or remotely an infinite number of times without any degradation. Secondly, the physical space required for storage is minuscule by previous standards. And finally, the software required to translate digitized information between two devices with different functions is usually trivial. However, if the data is converted to analog form, as when a file is sent to a printer, then its "cyberspace" quality is lost. Converting from the printed page back into ones and zeros is not trivial, and generally causes information to be lost or degraded.

NameBase resides in cyberspace, then, even though we send disks through the mail. It's trivial to dump the results of searches into a new file, and zap them by modem to another computer. Daisy-chain that file between every computer in the world, and if the transfer software uses error-correction protocol, at the end of the process

you have exactly the same file you started with. If it didn't infringe on our copyright, every set of NameBase disks we've distributed could each generate an infinite number of additional sets. Incidentally, another advantage to disk distribution as opposed to on-line systems is its decentralized quality. One of AT&T's computers in Dallas had so much extra capacity that they generously allowed it to used as a BBS host. But as their paranoia increased in 1990, AT&T considered it too risky and pulled the plug without warning, leaving 1,500 little modems out there, searching and chirping for their disconnected mother [19].

Any public or private intelligence agency that uses computers is potentially more ominous than one that doesn't, and the public has a right to expect certain standards for collection and dissemination. An example of an intelligence agency that fails this test is the Anti-Defamation League, whose San Francisco and Los Angeles offices were caught in a scandal earlier this year. The tax-exempt ADL has 30 regional offices in the U.S. (and offices in Canada, Paris, Rome, and Jerusalem), a staff of 400, and an annual budget of $32 million. For many decades they have been gathering information on U.S. citizens, using public sources as well as paid infiltrators, informants, investigators, and liaison with local law enforcement and the FBI. There is also evidence of connections with Mossad and South African intelligence.

As a private agency the ADL enjoys no oversight, no requirements for probable cause prior to political spying, and no Privacy Act or Freedom of Information Act responsibilities to the public. By contrast, the FBI, CIA, and some major police departments in the U.S. are held accountable by various hard-won legal restrictions. Some observers feel that the ADL's relationship with many local police, the FBI, and intelligence agencies suggests that they are playing the role of a cutout. Government agencies might be getting the information they want without incurring any legal risk, simply by using the ADL. In exchange, the ADL apparently enjoys privileged access to police and FBI files.

This is what happened in San Francisco, where a police intelligence officer (and former CIA agent in El Salvador) named Tom Gerard has been indicted for passing confidential police intelligence files to the local ADL office. Another principal in this case is Roy Bullock, who was a secret employee of the ADL for 40 years, a close associate of Gerard, and also an FBI informant. After learning that Gerard was meeting with South African intelligence, the FBI investigated. This encouraged the involvement of San Francisco prosecutors. They served two ADL offices with search warrants, and Bullock's computer was seized from his home. Interviews with Bullock revealed that he had tapped into one group's phone message system, and his computer contained data on 9,876 individuals and 1,359 political groups, distributed about evenly on both the left and right [20]. While it's evident that ADL spying is centrally coordinated from New York by ADL spymaster Irwin Suall, at this writing it's unclear whether San Francisco authorities will try to prosecute anyone from this powerful organization.

The ADL does not hail from any particular portion of the left-right political spectrum. Such a classification is irrelevant once a group becomes a private intelligence agency, as then they generally inbreed with their adversaries and mutate into a peculiar political animal. John Singlaub's Western Goals, and Political Research Associates (PRA) of Cambridge, Massachusetts, both extremely tiny compared to the ADL, are two additional examples of this phenomenon. All three groups identify with certain constituencies as a flag of convenience : the ADL with the Jewish community, Western Goals with the right, and PRA with the left. But by using the same methods of collecting information -- garbage surveillance, infiltration of target groups, and the use of guilt-by-association in their propaganda -- each of these three groups has perverted itself with clandestinism and denunciation for its own sake.

This opinion of mine is based on statements from John Rees (formerly of Western Goals and a person with extensive computer files on the left), Chip Berlet of PRA (formerly a BBS operator, with extensive files on the right), and testimony from Mira Boland of the ADL (extensive files on everyone). All admit to attending one or more secret meetings in 1983-1984 with U.S. intelligence operatives such as Roy Godson, representatives from

intelligence-linked funding sources, and journalists such as Patricia Lynch from NBC. Besides Berlet, other leftists attending included Dennis King and Russ Bellant. The purpose of these meetings was to plan a campaign against Lyndon LaRouche. The LaRouche organization was another private intelligence agency, but they had too many curious foreign contacts and were getting too close to certain individuals at the National Security Council. More importantly, LaRouche opposed U.S. intervention in Nicaragua just as the NSC was planning an expanded role there [21]. In another ten years, scenarios like this might be played out in cyberspace. Instead of a fifteen-year prison sentence, a future incarnation of LaRouche might jack into his cyberspace deck one day, and to his horror, discover that his collection of hard-won access codes no longer works.

ADL national director Abraham Foxman defends his organization by claiming that the ADL's sources "function in a manner directly analogous to investigative journalists" and "the information ADL obtains is placed in the public domain" [22]. He adds that "the very people making these charges [of ADL spying] themselves maintain and use such files whether they be journalists, lawyers or academics" [23]. But as we begin to enter the cyberspace age, his excuses seem particularly inadequate.

We have only Foxman's dubious word that ADL's information is placed in the public domain. Various investigative journalists, even those whose interests parallel the ADL's, have told me that it's difficult to get access to the ADL's main library in New York; you have to be connected to their old-boy network before you can see their files. Secondly, journalists seldom use the methods preferred by ADL's spies : going through a target's garbage and using deception to infiltrate target groups. On the rare occasions that a journalist does these things, it is implicitly balanced against the public interest, and done only to develop a specific story. Once published, the journalist's targets know what happened and have recourse to civil litigation. Normally journalists are expected by the standards of common decency to contact all parties criticized in a story, and double source any dubious items. Journalists identify themselves before soliciting any information, in order to provide the choice of cooperating on the record, not for attribution, on background, off the record, or refusing comment altogether. Finally, the public reasonably expects that journalists are not secretly working with law enforcement and intelligence agencies.

Foxman is simply blowing smoke on this issue. At Public Information Research we resent any hint of a comparison between his activities and ours. NameBase is basically a value-added public library; it has a citation from the public record for every bit of information, and is available to every member of the public. The extra value comes from the enhanced access to the public record. We don't consort with law enforcement or intelligence agencies, and we don't use deception to collect information.

On one occasion in ten years, a person whose name we had indexed complained to me that the source we cited misrepresented the facts. I asked him for a copies of published material about him that he considered more accurate, and cited these under his name along with the original citation (if he didn't have such sources, but could convince me that a source we cited was mistaken, then I would I have deleted the citation). On another occasion a person with whom I had worked for two years was upset to find her name in NameBase after I entered a book about the left that was published by the right. Her name is still in NameBase because I knew that the information about her in this book was true. I don't claim to be objective; my subjectivity is seen in the annotations I write for the sources, and in the selection of materials for inputting. This level of subjectivity comes with the territory -- sometimes it's unavoidable, and other times I like it, feeling that it's my only reason for continuing. But at the same time I do try to use common sense.

It would be comforting to have a Cyberspace Bill of Rights and Responsibilities, if the target wasn't moving so rapidly. Even an issue as self-evident as "privacy" is tricky, as the transnational corporations join the chorus in an effort to preclude government regulation. The international elites who control these corporations are well on their way toward installing the New World Order, and are no friends of the little guy who really needs privacy. Then again, our national security apparatus has an equally poor record. Everyone is waiting to see where the

chips fall before they declare themselves. In the meantime we find ourselves peering over the edge into cyberspace, surrounded by high-tech hype and journalistic buzzwords. We need a better-informed public with a keener sense of their own interests, but there's no time to wait. For those of us who work in this new cyberspace, our ethical thinking -- the ability to consider interests beyond our own -- must be honed to a new level.

References

1. David Burnham, *The Rise of the Computer State*, forward by Walter Cronkite (New York : Random House, 1983), pp. 124, 130, 206.

2. Ibid., p. 139.

3. John Smith, "Public Key Cryptography", Byte Magazine, January 1983, pp. 198-218.

4. Kevin Kelly, "Cypherpunks, E-Money, and the Technologies of Disconnection", Whole Earth Review, Summer 1993, pp. 46-47.

5. Washington Times, 10 May 1993, p. A3, citing a recent issue of Boardwatch, "a leading BBS magazine".

6. Robert Wright, "The New Democrat from Cyberspace", The New Republic, 24 May 1993, p. 20.

7. Bruce Sterling, "A Statement of Principle", Science Fiction Eye, June 1992, pp. 14-18.

8. John Mintz and John Schwartz, "Chipping Away at Privacy? Encryption Device Widens Debate Over Rights of U.S. to Eavesdrop", Washington Post, 30 May 1993, pp. H1, H4.

9. Wright, p. 26.

10. Ari Ben-Menashe, Profits of War : Inside the Secret U.S.-Israeli Arms Network (New York : Sheridan Square Press, 1992), pp. 127-141.

11. Carl Oglesby, *The Yankee and Cowboy War* (Berkley Publishing, 1977), p. 25.

12. Doug Birch, "Master of the Politics of Paranoia", Baltimore Sun Magazine, 5 June 1988, p. 26.

13. Charles Piller, "Privacy in Peril", Macworld, July 1993, p. 124.

14. Charles Piller, "Bosses With X-Ray Eyes", Macworld, July 1993, p. 120.

15. Piller, "Privacy in Peril", p. 126-127.

16. Cindy Skrzycki, "Dark Side of the Data Age", Washington Post, Business Section, 3 May 1993, pp. 19, 28.

17. Mintz and Schwartz, p. H4.

18. Bruce Sterling, *The Hacker Crackdown: Law and Disorder on the Electronic Frontier* (New York : Bantam books, 1992), p. 278.

19. Ibid., pp. 125-126, 141-142.

20. I obtained the 700 pages of documents which San Francisco prosecutors released on 8 April 1993. For a summary of this case see Robert I. Friedman, "The Enemy Within", Village Voice, 11 May 1993, pp. 27-32; and Richard C. Paddock, "New Details of Extensive ADL Spy Operation Emerge", Los Angeles Times, 13 April 1993, pp. A1, A16.

21. For an outline of the conspiracy against LaRouche by the ADL and U.S. intelligence operatives, see U.S. District Court for the Eastern District of Virginia, Alexandria Division, Petitioners' Rebuttal to the Government's Response and Memorandum. In United States v. Lyndon H. LaRouche, Jr., William F. Wertz, Jr. and Edward W. Spannaus, Case No. 88-243-A. Submitted by Odin Anderson, Ramsey Clark, and Scott T. Harper, attorneys for the defense, 1 May 1992, pp. 1-16. For a description of the secret meetings at the residence of John Train, see Herbert Quinde, Affidavit, Commonwealth of Virginia, County of Loudoun, 20 January 1992, pp. 1-28. Quinde describes interviews with Rees, Berlet, and several others. For confirmation of Chip Berlet's role, see Doug Birch, "Master of the Politics of Paranoia", Baltimore Sun Magazine, 5 June 1988, p. 27. Birch's description of John Rees' career includes a quotation from Chip Berlet, a longtime Rees watcher, that inadvertently confirms Berlet's collusion with Rees at an anti-LaRouche meeting. Berlet's spying is confirmed by his quotations in David Miller, "Letter from Boston", Forward, 22 January 1993, pp. 1, 14. This article also quotes ADL's Leonard Zakim : "The information that Political Research Associates has shared with us has been very useful".

22. Abraham H. Foxman, "Letter to the Editor", Village Voice, 18 May 1993, p. 5.

23. Abraham H. Foxman, "It's a Big Lie, Hailed by Anti-Semites", New York Times, 28 May 1993, p. A29.