June 12, 1991

Gerard Van der Leun
Director of Communications
Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141

Dear Mr. Van der Leun:

Thank you for your kind letter regarding the Community Memory Project.

Of course, we appreciate the Electronic Frontier Foundation's efforts in direct advocacy. However, we also believe that support for projects which demonstrate the potential of these networks -- particulary to constituencies who are cut out of the debate -- is crucial to the development of a regulatory and legal framework that doesn't merely benefit those who already have access to mass communications.

As allies with a shared mission, we look forward to working with the Electronic Frontier Foundation to shape a future in which communications tools allow individuals and communities to forge new ways of living and being which serve the common good.

Of course, we'll be delighted to keep you updated on the Community Memory Project's progress.

Best wishes,

Evelyn Pine
Executive Director

Bernard DeKoven (MC)
Institute for Better Meetings
2972 Clara Drive
Palo Alto, CA 94303
(415) 857-1757

comm

dial-in interest

EFFECTOR

Effector – The Newsletter of the Electronic Frontier Foundation

March 1991
Volume 1 Number 1

Goals of the EFF

1. To engage in and support educational activities that increase the popular understanding of the opportunities and challenges posed by computing and telecommunications.

2. To develop among policy-makers a clearer comprehension of the issues underlying free and open telecommunications.

3. To support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.

4. To raise public awareness about civil-liberties issues arising from rapid advances in computer-based communications media.

5. To support litigation in the public interest to preserve, protect, and extend Constitutional rights to the realm of computing and telecommunications technology.

6. To encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

A Man From the FBI:

The Origins of the Electronic Frontier Foundation

By John Perry Barlow

The Electronic Frontier Foundation was started by a visit from the FBI.

In late April of 1990, I got a call from Special Agent Richard Baxter of the Federal Bureau of Investigation. He asked if he could come by the next day and discuss a certain investigation with me. His unwillingness to discuss its nature over the phone left me with a sense of global guilt, but I figured turning him down would probably send the wrong signal.

On Mayday, he drove to Pinedale, Wyoming, a cow town 100 miles north of his Rock Springs office (where he ordinarily investigates livestock theft and other regional crimes). He brought with him a thick stack of documents from the San Francisco office and a profound confusion about their contents.

He had been sent to find out if I might be a member of the NuPrometheus League, a dread band of info-terrorists (or maybe just a disaffected former Apple employee) who had stolen and wantonly distributed source code normally used in the Macintosh ROMs. Agent Baxter's errand was complicated by a fairly complete unfamiliarity with computer technology. I realized right away that before I could demonstrate my innocence, I would first have to explain to him what guilt might be.

The three hours I passed doing this were surreal for both of us. Whatever this source code stuff was, and whatever it was that happened to it, had none of the cozy familiarity of a few yearling steers headed across the Wyoming border in the wrong stock truck.

What little he did know, thanks to the San Francisco office, was also pretty well out of kilter. He had been told, for example, that Autodesk, the publisher of AutoCAD, was a major Star Wars defense contractor and that its CEO was none other than John Draper, the infamous phone phreak also known as Cap'n Crunch. As soon as I quit laughing, I started to worry.

I realized in the course of this interview that I was seeing, in microcosm, the entire law enforcement structure of the United States. Agent Baxter was hardly alone in his puzzlement about the legal, technical, and metaphorical nature of datacrime.

I also found in his struggles a framework for understanding a series of recent Secret Service raids on some young hackers I'd met in a Harper's magazine forum on computers and freedom. And it occurred to me that this might be the beginning of a great paroxysm of governmental confusion during which everyone's liberties would become at risk.

When Agent Baxter had gone, I wrote an account of his visit and placed it on the WELL, a computer BBS in Sausalito which is digital home to a large collection of technically hip folks, including Mitch Kapor, the father of Lotus 1-2-3.

Turns out Mitch had also been visited by the FBI, owing to his having unaccountably received of one of the source code disks which NuPrometheus scattered around. Mitch's experience had been as dreamlike as mine. He had, in fact, filed the whole thing under General Inexplicability until he read my tale on the WELL. Now he had enough corroboration for his own strange sense of alarm to begin acting on it.

Several days later, he found his bizjet about to fly over Wyoming on its way to San Francisco. He called me from somewhere over South Dakota and asked if he might literally drop in for a chat about Agent Baxter and related matters.

So, while a late spring snow storm swirled outside my office, we spent several hours hatching what became the Electronic Frontier Foundation. I told him about the sweep of Secret Service raids that had taken place months before and their apparent disregard for the Bill of Rights.

Alarmed, he gave me the phone number of Harvey Silverglate, whose willingness to champion unpopular causes was demonstrated by his current defense of Leona Helmsley. He said that Harvey would probably know if this were as bad as it was starting to sound. He also said that he would be willing to pay the bills that generally start to appear whenever you call a lawyer.

I finally found Harvey in the New York offices of Rabinowitz, Boudin, Standard, Krinsky and Lieberman, a firm whose long list of successfully defended civil-liberties cases includes the Pentagon Papers case. I told him and Eric Lieberman what I knew about recent government flailings against cybercrime. They were even less sanguine than I had been.

The next day a trio code-named Acid Phreak, Phiber Optik, and Scorpion entered the walnut-panelled chambers of Rabinowitz, Boudin and told their tales to a lawyer there named Terry Gross. While EFF as a formal organization would not exist for two months, its legal arm was already flexing its muscle.

A few days later I received a phone call from the technology writer for the Washington Post. He was interested in following up on the Harper's forum, and knew nothing of Mitch's and my joint endeavors. I filled him in, hoping to expose the Secret Service. Several days later, the Post published the first of many newspaper stories, all of which could have shared the headline: "Lotus Founder Defends Hackers."

continued page 2

Why Defend Hackers?

By Mitchell Kapor

An all-too-common perception of the EFF that prevails in the computer industry and those who report on it—from John Sculley to the Wall Street Journal—is that the EFF is an organization that has "something to do with hackers." (They use "hackers" as a term not of approbation but of rebuke). Most of these sometime colleagues and associates of mine are puzzled as to why I would be doing such a thing. (A few think I've just become a loony.) Anyway, they've heard about the terrible problems caused by hackers who break into computer systems, they worry that I'm out to defend such practices, and they disapprove.

But their disapproval is based on the pure misconception that the EFF's purpose is to defend people's right to break into computer systems. Let me clear up that misconception now.

I regard unauthorized entry into computer systems as wrong and deserving of punishment. People who break into computer systems and cause harm should be held accountable for their actions. We need to make appropriate distinctions in the legal code among various forms of computer crime, based on such factors as intent and the degree of actual damage. In fact, the EFF has drafted a bill that has the backing

continued page 3

Washington Watch

by Marc Rotenberg

• *Computer Crime Legislation*

Several proposals to expand computer crime law were introduced in the past Congress. In the end, a modest proposal, introduced by Senator Leahy, passed the Senate but did not make it through the House. Senator Leahy's bill would have penalized reckless computer acts that place computer systems at risk and would have required that the Justice Department report annually to Congress on computer crime prosecutions

• *National ID Card*

A proposal to begin a national ID card pilot project, tucked into amendments to the Immigration Control and Reform Act, was knocked out when civil libertarians objected.

• *Electronic Dissemination Policy*

A proposal to establish principles for the dissemination of electronic information by the federal agencies narrowly failed to pass the Congress as last minute negotiations on a related measure collapsed. The proposal grows out of a report from the Office of Technology Assessment "Informing the Nation" that stressed the need to develop new information policy to promote the development of CD-ROMs and on-line information services.

• *Caller ID*

A bill to allow the offering of Caller ID by regional phone companies if a per-call blocking feature is also provided failed to gather support this past Congress. Several states have already adopted similar measures.

• *Computer Security Policy*

The Presidential directive on computer security policy was revised finally to comply with the Computer Security Act of 1987. The Act reestablished control for computer security at a civilian agency — the National Institute for Standards and Technology — after the previous administration attempted to place computer security authority at the National Security Agency.

• *Upcoming Policy*

CPSR hosted the first Computing and Civil Liberties policy roundtable on February 21 and 22, 1991 at the American Association for the Advancement of Science in Washington, DC. The purpose of the roundtable was to bring together leading experts to explore two issues: free speech and computer networks, and searches of computer bulletin boards. What speech restrictions currently exist? Should federal agencies or private companies be allowed to restrict the content of a computer message and, if so, in what circumstances? The second issue was the investigation of computer bulletin boards by law enforcement agents. Are there any restrictions on the ways that police may monitor computer communications and computer bulletin boards? If not, should such restrictions be developed? The conference was the first in a series of policy roundtables that will be held in Washington, DC and that are made possible with funding from the Electronic Frontier Foundation.

EFFECTOR

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

The Board of the Electronic Frontier Foundation:
Mitchell Kapor, John Barlow, John Gilmore, Stewart Brand, Steve Wozniak
Staff Counsel: Mike Godwin
Staff Volunteer: Leila Gallagher

EFFECTOR was edited and produced by Gerard Van der Leun

Art Direction and design by Lisa DeFrancis, DeFrancis Studio, 80 Trowbridge Street, Cambridge, MA 02138

FBI ***continued***

While this was an irritating misrepresentation, we were more interested in defending the Constitution than digital miscreants, the publicity produced a couple of major supporters: Steve Wozniak, who called and offered an unlimited match to Mitch's contributions, and John Gilmore (Sun Microsystems employee #5) who e-mailed me a six figure offer of support.

Operation Sundevil

Meanwhile, the list of apparent outrages lengthened. We learned about an Austin role-playing games publisher named Steve Jackson whose office equipment had been confiscated by the Secret Service in an apparent effort to restrain his publication of a game called Cyberpunk which they thought, with ludicrous inaccuracy, to be "a handbook for computer crime."

All over the country computer bulletin boards were being confiscated, undelivered e-mail and all. A Secret Service dragnet called Operation Sundevil seized more than 40 computers and 23,000 data disks from teenagers in 14 American cities, using levels of force and terror which would have been more appropriate to the apprehension of urban guerrillas than barely postpubescent computer nerds.

And there was the Craig Neidorf case. Neidorf, also known by the nom de crack Knight Lightning, had published an internal BellSouth document in his electronic magazine Phrack. For this constitutionally protected act, Neidorf was being charged with interstate transport of stolen property with a possible sentence of 60 years in jail and a $122,000 in fines.

I wrote a piece about these events called "Crime & Puzzlement." I did so at the request of the Whole Earth Review—it made its first print appearance in the Fall 1990 issue of WER—but I "published" it on the Net in June and was astonished by the response. It was like planting a fence-post and discovering that the ground into which you've driven it is actually the back of a giant animal that quivers and heaves at the irritation.

By July, I was receiving up to 100 e-mail messages a day. They came from all over the planet and expressed nearly universal indignation. I began to experience datashock, but I also realized that Mitch and I were not alone in our concerns. We had struck a chord.

The Law in Cyberspace

In Cambridge, Mitch was having something like the same experience. Since the Washington Post story, he found himself bathed in media glare. However, the more he learned about ambiguous nature of law in Cyberspace, the more of his considerable intellectual and financial resources he became willing to devote to the subject.

In late June, Mitch and I threw several dinners in San Francisco, to which we invited major figures from the computer industry. We weren't surprised to learn than many of them had exploits in their past which, undertaken today, would arouse plenty of Secret Service interest. It appeared possible that one side-effect of current government practices might be the elimination of the next generation of computer entrepreneurs and digital designers.

It also became clear that we were dealing with a set of problems which was a great deal more complex and far-reaching than a few cases of governmental confusion. The actions of the FBI and Secret Service were symptoms of a growing social crisis: Future Shock. America was entering the Information Age with neither laws nor metaphors for the appropriate protection and conveyance of information itself.

We realized that our legal actions on behalf of a few teen-age crackers would go on indefinitely without much result unless something were done to ease social tensions along the electronic frontier. The real task at hand was the civilization of Cyberspace. Such an undertaking would require more juice and stamina than two men could muster, even amplified by the Net and a solid financial supply. We would need some kind of organizational identity.

With this in mind, we hired a press coordinator, Cathy Cook (who had formerly done PR for Steve Jobs), set a squad of lawyers to work on investigating the proper organizational tax status, and, over a San Francisco dinner with Stewart Brand, Nat Goldhaber, Jaron Lanier, and Chuck Blanchard, we selected a name and defined a mission.

Founding the Foundation

We announced the formation of the Electronic Frontier Foundation at the National Press Club on July 10. Mitch and I were joined for the announcement by Harvey Silverglate, Terry Gross, and Steve Jackson.

We were also joined by Marc Rotenberg of the Washington office of Computer Professionals for Social Responsibility. One of our first official acts had been to grant that organization $275,000 for a project on computing and civil liberties. CPSR would keep a wary eye on developments "inside the Beltway" and work in conjunction with congressional staffers to see that any legislation dealing with access to information was sensibly drafted.

While in Washington, we also took inventory of the terrain, meeting with congressional staffers, the Washington civil liberties establishment, and officials from the Library of Congress and the White House. The area to be covered, from intellectual property to telecommunications policy to law enforcement technique, was daunting, as were the ambient levels of confusion and indifference.

We also generated an enormous amount of press. And it became apparent that not everyone was persuaded of our cause. Business Week called Mitch naive for his willingness to believe that computer crackers were somehow less dangerous that drug kingpins. Various burghers of the computer establishment, ranging from the executive director of the Software Publishers Association to a columnist for ComputerWorld, called us fools at best and, more likely, dangerous fools.

The Wall Street Journal printed a particularly hysterical piece which alleged that the document Craig Neidorf (into whose case we had entered a supporting amicus brief) had published was a computer virus capable of bringing down the emergency phone system for the entire country. In fact, the text file which Neidorf distributed dealt with the bureaucratic procedures of 911 administration in the BellSouth region and contained nothing which could be used to crack a system. Indeed, it contained nothing which could not be easily obtained through by legal means.

Neidorf's first major break came in late July. Thanks in part to the independent work of John Nagel, who was prepared to testify that the prosecutors had seriously overstated the value of the E911 document, the government was forced to abandon its case against Neidorf after 4 days in Chicago's Federal Court.

Although our briefs supporting Neidorf's activities under the First Amendment were not admitted, it became apparent, before such loftier matters could even be broached, that the government had indicted him with no clear understanding of the purpose or availability of the document he had distributed. Like Agent Baxter, they knew too little to critically examine the misinformation they had been given by the corporate masters, in this case, officials at Bellcore.

Following the resolution of the Neidorf case, and, to some extent because of it, skepticism of EFF has moderated considerably. If anything, the most recent press accounts of our activities have been almost fulsome in their praise. Recent favorable coverage has appeared in the New York Times, The Economist, Infoworld, Information Week, PCweek, and Boston Magazine.

Since July, we have been absurdly busy on numerous fronts: We've worked on raising public awareness of the issues at stake. We are organizing legal responses to the original and continuing intemperance of law enforcement. We have worked on the political front, developing and lobbying for rational computer security legislation. We have started to create a network of interested experts on computer security, intellectual property, telecommunications policy, and international information rights. And lately we've been attending to the organizational demands of the non-profit equivalent of a hyper-successful computer startup.

The Expanding Mission

When we first defined the mission of the Electronic Frontier Foundation, we saw our task as assuring the application of the U.S. Constitution to digital media. And this remains much of what we are about.

However, information has little natural regard for national borders or local ordinances. Cyberspace is transnational. During the tsunami of e-mail which Crime & Puzzlement elicited, there were many items from foreign countries. Their authors wanted to know how they could protect or establish their rights of free expression. And I had no idea what to tell them.

The question arose again at Esther Dyson's recent East-West Technology Conference in Budapest which Mitch and I attended. EFF was well-known among the Soviets at this meeting, some of whom were already involved in drafting what they called an Information Bill of Rights. (One young Moscow programmer had managed to hack together an Internet connection through Finland in order to contact me.)

Like intellectual property and telecom policy, the development of international principles of free digital speech is a large angel to wrestle with. We will have to be careful not to allow this immense task to divert EFF from its specific legal agenda. But neither can we ignore the fact that Cyberspace is hardly an American territory.

The Electronic Frontier Foundation grew from an effort to fight a specific legal brushfire into a full-fledged Cause much faster than we could have imagined. And, like any explosive start-up, it spends a lot of time playing catch-up.

Reaching Out

Electronically amplified, Mitch and I were able to personally conduct much of EFF's business in the first few months of operations. But gradually we had to confront the fact that while the Net is very broad, it is also quite shallow. Without even a sense of their physical location, we have been unable to marshal the hundreds of people who have e-mailed us with their volunteered services. Also, we found ourselves administering a significant cash-flow in both donations and expenditures. (By year's end, EFF will have spent around $220,000. Our tentative 1991 budget predicts expenses of almost half a million.)

So, despite a mutual terror of bureaucracy and organizational sclerosis, we have started to adopt some institutional trappings.

First, in order to satisfy the requirements for a 501c3 tax status (which we should have in about six months), we found that we needed something more substantial than two guys with modems. Thus, on October 9, we held our first official board meeting and formally elected Stewart Brand, Steve Wozniak, and John Gilmore to join us as board members.

And we have started to take on staff. We recently hired Mike Godwin, a freshly minted Texas lawyer and USENET adept, to sort through the factual and legal details of the many cases we are being asked to intervene in. In his short time with us, he has investigated several cases to determine their fit with EFF's constitutional mission, their winnability, and their likelihood of producing clear legal precedent.

We are determined that EFF will remain an agile, swift-moving sort of outfit. We will adopt any new bureaucratic manifestations with the greatest skepticism. But we are being bombarded with many legitimate requests for assistance, advice, and information. In order to respond rapidly and appropriately, the Electronic Frontier Foundation has had to become an institution. One method by which we hope to maintain organizational lightness involves keeping a clear distinction between strategy and tactics.

On the strategic level, EFF has a very broad mission involving such amorphous endeavors as defining intellectual property, helping establish a transnational culture of information, designing telecommunications policy, sponsoring humane software design... civilizing Cyberspace. With an appropriate sense of their limitations, the board members will remain responsible for these matters.

This will prevent the staff's losing tactical focus on more tangible action items like litigation, political action, communicating through the press and across the Net, and organizational care and feeding.

The problem with history is that it keeps happening. Today, as I was working on this EFF mini-biography, I learned that Mitch has just had his fingerprints subpoenaed by the FBI. Turns out they are now examining the NuPrometheus distribution disks for fingerprints and want to be able to sort his out. Or, perhaps, search for their appearance on other disks...

So the Wheels of Justice grind blindly on. And we will go on trying to prevent anyone's being ground up in them.

Postcard from the Edge

"I went on to test the program in every way I could devise. I strained it to expose its weaknesses. I ran it for high-mass stars and low-mass stars, for stars born exceedingly hot and those born relatively cold. I ran it assuming the superfluid currents beneath the crust to be absent — not because I wanted to know the answer, but because I had developed an intuitive feel for the answer in this particular case. Finally I got a run in which the computer showed the pulsar's temperature to be less than absolute zero. I had found an error. I chased down the error and fixed it. Now I had improved the program to the point where it would not run at all."

George Greenstein,
"Frozen Star: Of Pulsars, Black Holes and the Fate of Stars"

How Prosecutors Misrepresented the Atlanta Hackers

Reading Between the Lines of the BellSouth Sentences

By Mike Godwin

Although the Electronic Frontier Foundation is opposed to unauthorized computer entry, we are deeply disturbed by the recent sentencing of Bell South hackers/crackers Riggs, Darden, and Grant. Not only are the sentences disproportionate to the nature of the offenses these young men committed, but, to the extent the judge's sentence was based on the prosecution's sentencing memorandum, it relied on a document filled with misrepresentations.

Robert J. Riggs, Franklin E. Darden, Jr., and Adam E. Grant were sentenced Friday, November 16, in federal court in Atlanta. Darden and Riggs had each pled guilty to a conspiracy to commit computer fraud, wire fraud, access-code fraud, and interstate transportation of stolen property. Grant had pled guilty to a separate count of possession of access codes with intent to defraud.

All received prison terms; Grant and Darden, according to a Department of Justice news release, "each received a sentence of 14 months incarceration (7 in a halfway house) with restitution payments of $233,000." Riggs, said the release, "received a sentence of 21 months incarceration and $233,000 in restitution." In addition, each is forbidden to use a computer, except insofar as such use may be related to employment, during his post-incarceration supervision.

The facts of the case, as related by the prosecution in its sentencing memorandum, indicate that the defendants gained free telephone service and unauthorized access to BellSouth computers, primarily in order to gain knowledge about the phone system. Damage to the systems was either minimal or nonexistent. Although it is well-documented that the typical motivation of phone-system hackers is curiosity and the desire to master complex systems, the prosecution attempts to characterize the crackers as major criminals, and misrepresents facts in doing so.

Examples of such misrepresentation include:

1. Misrepresenting the E911 file.

The E911 file, an administrative document, was copied by Robert Riggs and eventually published by Craig Neidorf in the electronic magazine PHRACK. Says the prosecution: "This file, which is the subject of the Chicago [Craig Neidorf] indictment, is noteworthy because it contains the program for the emergency 911 dialing system. As the Court knows, any damage to that very sensitive system could result in a dangerous breakdown in police, fire, and ambulance services. The evidence indicates that Riggs stole the E911 program from BellSouth's centralized automation system (i.e., free run of the system). Bob Kibler of BellSouth Security estimates the value of the E911 file, based on R&D costs, is $24,639.05."

This statement by prosecutors is clearly false. Defense witnesses in the Neidorf case were prepared to testify that the E911 document was not a program, that it could not be used to disrupt 911 service, and that the same information could be ordered from Bell South at a cost of less than $20. Under cross-examination, the prosecution's own witnesses admitted that the information in the E911 file was available in public documents, that the notice placed on the document stating that it was proprietary was placed on all Bell South documents (without any prior review to determine whether the notice was proper), and that the document did not pose a danger to the functioning of the 911 system.

2. Guilt by association.

The prosecution begins its memorandum by detailing two crimes: 1) a plot to plant "logic bombs" that would disrupt phone service in several states, and 2) a prank involving the rerouting of calls from a probation office in Florida to "a New York Dial-A-Porn number."

Only after going to some length describing these two allegations does the prosecution state, in passing, that *the defendants were not implicated in these crimes.*

Elsewhere in the memorandum, the prosecution attempts to suggest the defendants' responsibility in a third offense—another person's crime. Because the defendants "freely and recklessly disseminated access information they had stolen," says the memorandum, a 15-year-old hacker committed $10,000 in electronic theft. Even though the prosecution does not say the defendants intended to facilitate that 15-year-old's alleged theft, the memorandum seeks to implicate the defendants in that theft.

3. Guilt by knowing too much.

The prosecution goes to great lengths describing the crimes the defendants *could* have committed with the kind of knowledge they had gathered: "During the course of the conspiracy, the defendants and other LOD [Legion of Doom] members illegally amassed enough knowledge about the telecommunications computer systems to jeopardize the entire telephone industry!"

The prosecution does not mention, however, that the mere possession of dangerous knowledge is not a crime, nor does it state, explicitly, that the defendants never conspired to cause such damage to the phone system.

4. Misrepresentation of motives.

As noted above, it has been documented that young phone-system hackers are typically motivated by the desire to understand and master large systems, not to inflict harm or to enrich themselves materially. Although the prosecution concedes that "[d]efendants claimed that they never personally profited from their hacking activities, with the exception of getting unauthorized long distance and data network service," the prosecutors nevertheless characterize the hackers' motives as similar to those of extortionists: "Their main motivation [was to] obtain power through information and intimidation."

5. Failure to acknowledge the outcome of the Craig Neidorf case.

In evaluating defendants' cooperation in the prosecution of Craig Neidorf, the government singles out Riggs as being less helpful than the other two defendants, and recommends less leniency because of this. Says the memorandum: "The testimony was somewhat helpful, though the prosecutors felt defendant Riggs was holding back and not being as open as he had been in the earlier meeting." The memorandum fails to mention, however, that Riggs's testimony tended to support Neidorf's defense that he had never conspired with Riggs to engage in the interstate transportation of stolen property or that the case against Neidorf was dropped.

Perhaps the most egregious aspect of the governments's memorandum is the argument that Riggs, Grant, and Darden should be imprisoned, not for what *they* have done, but to send the right "message to the hacking community." The government focuses on the case of Robert J. Morris Jr., the computer-science graduate student who was sentenced to a term of probation in May of this year for his release of the worm program that disrupted many computers connected to the Internet. Urging the court to imprison the three defendants, the government remarked that "hackers and computer experts recall general hacker jubilation when the judge imposed a probated sentence. Clearly, the sentence had little effect on defendants Grant, Riggs, and Darden."

The government's criticism is particularly unfair in light of the fact that the Morris sentencing took place almost a year *after* the activities leading to the defendants' convictions!

The memorandum raises other questions besides those of the prosecutors' biased presentation of the facts. The most significant of these is the government's uncritical acceptance of BellSouth's statement of the damage the defendants did to its computer system. The memorandum states that "In all, [the defendants] stole approximately $233,880 worth of logins/passwords and connect addresses (i.e., access information) from BellSouth. BellSouth spent approximately $1.5 million in identifying the intruders into their system and has since then spent roughly $3 million more to further secure their network."

It is unclear how these figures were derived. For one thing, the stated cost of the passwords is highly questionable: What is the dollar value of a password?

And it's similarly unclear that the defendants caused BellSouth to spend $4.5 million more than they normally would have spent in a similar period to identify intruders and secure their network. Although the government's memorandum states that "[t]he defendants ... have literally caused BellSouth millions of dollars in expenses by their actions," the actual facts as presented in the memorandum suggest that BellSouth had already embarked upon the expenditure of millions of dollars *before* it had heard anything about the crimes the defendants ultimately were alleged to have committed.

Not only are there questions about the justice of the restitution requirement in the sentencing of Riggs, Darden, and Grant, but there also are Constitutional issues raised by the prohibition of access to computers. The Court's sentencing suggests a belief that anything the defendants do with computers is likely to be illegal; it ignores the fact that computers are a communications medium, and that the prohibition goes beyond preventing future crimes by the defendants—it treads upon their rights to engage in lawful speech and association.

EFF does not support the proposition that computer intrusion and long-distance theft should go unpunished. But we find highly disturbing the misrepresentations of facts in the prosecutors' sentencing memorandum as they seek disproportionate sentences for Riggs, Darden, and Grant—stiff sentences that supposedly will "send a message" to the hackers and crackers.

The message this memorandum really sends is that the government's presentation of the facts of this case has been heavily biased by its eagerness to appear to be deterring future computer crime.

20 Things You Can Do to Advance Electronic Freedom

1. Spread the word about EFF as widely as possible, both on and off the Net.

2. Be alert for any local, state or national legislation that effect electronic freedom.

3. Put the immense processing horsepower of your mind to the task of finding new metaphors for the realities of the physical world which seem up for grabs in these less tangible regions.

4. Try to communicate to technically unsophisticated friends the extent to which their future freedoms depends on understanding digital communication.

5. If you are online, spread the word to local boards.

6. If you are at a school, inform interested people about the goals of the EFF.

7. Connect responsibly.

8. Work locally for an understanding of what the electronic frontier means in a global sense.

9. Learn and use the technology. Only by having an understanding of computers can one evaluate statements about computer crime.

10. Stop and think, about the many ways in which we rely on information in our lives, and what the effect might be if that information were distorted, corrupted, limited, or denied us.

11. Remember that words on a computer are SPEECH, protected by the Constitution.

12. Help your non-computerized friends see the potential of the net: search out a low airline fare for them, or send a fast cheap message to friends across the country.

13. Check to see if your local and state representatives understand the potential of electronic communication.

14. Reject techno-elitism and recognize that entry into the networking domain is a rite of passage and that someone else probably helped you with it.

15. Do your backups.

16. Educate your local librarians about electronic freedoms.

17. Welcome all interested participants.

18. Argue in a way that informs all the participants in the argument.

19. Develop better tools for linking people and networks.

20. Keep in touch with us. Pass on your thoughts, concerns, insights, contacts, and news.

Why Defend Hackers *continued*

of the Governor and Attorney General of Massachusetts and that embodies these principles.

But if the EFF isn't trying to advance the cause of computer hackers, you may ask, what is it doing and why? What is it that was sufficiently powerful to motivate me to help start a whole organization?

As I began to find out the real story behind government raids and indictments last summer, I became incensed at the fact that innocent individuals were getting caught up in the blundering machinations of certain law enforcement agencies and large corporations. These were kids really, young people with whom I identified, who faced the prospect of having their lives ruined.

Take Craig Neidorf for example. Neidorf, a defendant in one case and the publisher of an electronic newsletter, was indicted on felony charges of wire fraud and interstate transportation of stolen property. Neidorf had published a document about administrative procedures used in the 911 emergency response telephone system that someone else had removed from a BellSouth computer. On the fourth day of the trial, the prosecution dropped the case after it became clear that the information in the "highly confidential" BellSouth document at issue was publicly available for less than $20.

Justice was served by the government's decision to drop the case, but it was expensive justice. Neidorf and his family face $100,000 in legal bills, to say nothing of the disruption and suffering caused by the trial for an action that should never have been brought against him to begin with.

In a second case, the EFF continues to assist Steve Jackson, a game manufacturer in Austin, Texas, who has suffered substantial business losses after a Secret Service raid in early March. The seizure of Jackson's computer equipment caused him to lay off nearly half of his staff and threatened the survival of the business. As subsequent revelations have showed, there was no good reason for this raid. It never should have been permitted to occur in the first place.

While helping defend the innocent is one role for the EFF to play, there is more at stake than trying to prevent individuals from being wronged. It is also a matter of rights for all of us.

The legal protections afforded Craig Neidorf's electronic newsletter and its publisher and the computer bulletin board system (BBS) seized in the Steve Jackson raid are neither clear nor well-established. I believe it is terribly important to extend to these new digital media the same strong First Amendment protections of freedom of speech and freedom of expression which we enjoy in our own lives and in the print media. The government should not be able to seize a BBS any more easily than they can seize a printing press. We must find ways for law enforcement to do its job in protecting the property of some of us without violating the freedom of speech of the rest of us. This is clearly a matter of protecting civil liberties and familiar to those who take an interest in upholding the Bill of Rights, but it is also more than that.

These embryonic media of electronic mail, BBSs, and conferencing systems, provide open forums of communication. They are an antidote to the corrosive effects of the power of large, centralized institutions, private and public, and to the numbness induced by one-way, least-common-denominator mass media.

In the global suburbs in which more and more of us live, one's horizon is limited to the immediate family. Even close neighbors are often anonymous.

In the realities that can be created within digital media there are opportunities for the formation of virtual communities—voluntary groups who come together not on the basis of geographical proximity but through a common interests. Computer and telecommunications systems represent an enabling technology for the formation of community, but only if we make it so. I believe it is urgent, as a matter of national policy, that we encourage and further stimulate the social experiments and developing infrastructure that are taking place on the Net every day. The ultimate mission of the EFF is to help articulate this vision and play a constructive role in the working out of the new legal and social norms which we are faced with developing.

As John Barlow and I meditated together last June on the broader implications of the initial events—a meditation that catalyzed the formation of the EFF—we could see that what was at stake was not merely seeing justice be served in the case of a few individuals, nor simply the preservation of the civil liberties of all of us, although these goals are vitally important.

The larger issue is how our society will come to terms with the onrush of transformative technology. If we take the right steps now—and EFF is working to take those steps—new and increasing access to information technology will enhance rather than inhibit the positive growth and development of individuals, of communities, and of society as a whole.

CPSR Announces the First Conference on Computers, Freedom & Privacy

Tutorials & Invitational Conference, Limited to 600 Participants

About Computers, Freedom & Privacy —
We are at a crossroads, as individuals and organizations conduct more and more of their activity using computers and computer networks. By the end of the 1990s, most information will be collected, distributed and utilized electronically.

Thus far, an uncoordinated jumble of policies and procedures is rapidly developing as each group develops ways of collecting, manipulating, extracting, sharing and protecting information in its computers and exchanged on its networks.

Information on individuals and groups is being computerized by numerous organizations, agencies and special interests, often without the knowledge or approval of those it concerns.

Computerization can greatly assist individuals, organizations and government in making sound decisions based on efficient access to adequate information.

Or, it can seriously threaten the fundamental freedoms, personal privacy, and democratic processes that are at the very foundation of this nation.

More and more people are concerned about how organizations handle personal, family and lifestyle information about individuals. Many feel powerless to prevent private organizations and government from building, marketing and distributing confidential dossiers on them. Valuable information about government is increasingly computerized in government systems, but freedom of access to it in useful, computerized form by interested citizens, researchers and the press remains difficult and often prohibited.

Governments' regulation of national and international information exchange is increasing, often restricting it in the name of protecting competitiveness or confidentiality. There are increasing protests from business leaders unable to conduct effective business in a global economy.

Businesses are losing millions of dollars and thousands of work-hours, annually, to computerized mischief, vandalism, fraud and theft. Perpetrators are usually individuals abusing their authorized access.

Instances of computer misuse by young people raise special questions about the values that adults are practicing and passing along to these children.

Each year, new laws are proposed responding to the latest type of abuse or misuse of computers. Penalties applied to uncharged suspects and convicted computer criminals vary wildly from case to case, with little consistency relative to the seriousness of the alleged crime.

Law enforcement officials are using increasingly aggressive strategies and sophisticated countermeasures as they seek to serve and protect, vigorously applauded by some interest groups and increasingly criticized by others.

Diverse groups are often polarizing around narrow self-interests, rather than working together to assure responsible practices and equitable policies.

About this Conference —
This is an intensive, multi-disciplinary survey Conference for those concerned with computing, teleconferencing, electronic mail, computerized personal information, direct marketing information and government data — and those concerned with computer-related legislation, regulation, law enforcement and international policies that impact civil liberties, responsible exercise of freedom and protection of privacy in the global Information Age.

A maximum of 600 applicants will be invited to attend. Balanced representation from the diverse interest groups is being encouraged.

To inform participants about topics beyond their specialties, half-day and full-day seminars are scheduled for the first day (Monday, Mar. 25th). These parallel tutorials will explore relevant issues in computing, networking, civil liberties, the law and law enforcement. Each seminar is designed for those who are experienced in one area, but are less knowledgeable in some of the other disciplines.

To explore the issues and their interactions and ramifications, conference talks and panel discussions are scheduled for the remaining three days (Tuesday-Thursday, Mar. 26th-28th). These will emphasize balanced representation of all major views, with ample opportunity for probing questions and discussion.

The opening conference session on Tuesday will include major policy proposals by one of the nation's best known Constitutional scholars: Laurence H. Tribe, Professor of Constitutional Law, Harvard University Law School: "The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier"

The Tuesday evening session will feature a leading expert in the areas of telecommunications regulation, international telecomm policies and economics: Professor Eli M. Noam, Professor & Director Center for Telecommunications and Information Studies, Columbia University Graduate School of Business

Tuesday-Thursday Conference sessions offering diverse speakers & panel discussions include:

- Computers & Network Trends
- Personal Information & Privacy
- International Perspectives & Impacts
- Law Enforcement Practices & Problems
- Law Enforcement & Civil Liberties
- Legislation & Regulation
- Computer-Based Surveillance of Individuals
- Ethics & Education
- Electronic Speech, Press, & Assembly
- Access to Government Information
- Where Do We Go From Here?

The conference is sponsored by Computer Professionals for Social Responsibility–A nonprofit educational corporation. Telephone: (415)322-3778 Fax: (415) 851-2814 Conference e-mail: cfp@well.sf.ca.us

Co-sponsors & cooperating organizations include: Electronic Frontier Foundation, Electronic Networking Association Association for Computing Machinery, American Civil Liberties Union, ACM Special Interest Group on Software, Videotex Industry Association, IEEE-USA Intellectual Property Committee Cato Institute, IEEE-USA Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers-USA, ACM Committee on Scientific Freedom and Human Rights, ACM Special Interest Group on Computers and Society, The WELL, Autodesk, Inc., Portal Communications.

March 25-28, 1991, Monday-Thursday in the Bicentennial Year of the Bill of Rights

Airport Marriott Hotel, Burlingame, California on the San Francisco Peninsula, near San Francisco International Airport

Sponsored by: Computer Professionals for Social Responsibility –A nonprofit educational corporation

Chair: Jim Warren, Autodesk & MicroTimes, fax/415-851-2814, e-mail/jwarren@well.sf.ca.us

Request for Invitation
To facilitate useful dialogue and balanced participation by representatives from all of the diverse groups that are interested in these issues, this First Conference on Computers Freedom & Privacy (March 25-28, 1991) is limited to 600 invited participants (Conference facility capacity is also limited). All interested parties are encouraged to apply for an invitation. To receive information about the 50-60 speakers & panelists, the tutorials and an Invitation Application form, forward the following information to: e-mail/cfp@well.sf.ca.us -or- fax/(415)851-2814 -or- CFP Conference, 345 Swett Road, Woodside CA 94062

Name:
Title (if any):
Organization (if any):
Mailing address:
City/state/ZIP:
Phone number:
Alternate phone (if any):
Fax number (if any):
Electronic-mail address (if any):
Your particular interests (maximum of one page, please):

Plans and Actions:

Current EFF Activities

The Len Rose cases
The EFF legal department has been working to provide litigation support in the two criminal cases involving Baltimore computer consultant Len Rose. In the first case, we have been particularly active in helping develop the factual and legal issues in the case, and in locating and screening potential witnesses. We believe Baltimore case raises important issues concerning both the application of the federal Computer Fraud and Abuse statute (which we have challenged on the basis of unconstitutional overbreadth), the federal wire-fraud statute, and the federal Interstate Transportation of Stolen Property statute (which we believe should not be applied in cases of unauthorized copying of copyrighted software).

We have been providing similar support in Rose's state criminal case in Illinois. Among the issues in that case is whether the Illinois "computer tampering" statute is overbroad, and whether it in fact criminalizes the activity that Rose is alleged to have committed. In both cases, we have relied extensively on communications over the Net to initiate and maintain contact with potential witnesses.

The RIPCO BBS case
We have also been giving significant time to reviewing the warrant affidavits in the RIPCO BBS seizure. In addition, we have been reviewing the available archived files from that BBS to determine what, if any, justification there was for seizing the equipment.

We believe the RIPCO case potentially raises important issues about the valid scope of searches and seizures, the chilling effect of such seizures on First Amendment-protected speech and association, and the limits of sysop liability for the activities of third parties.

Other matters
We have continued our ongoing investigations of cases that raise issues that may be of EFF interest. In many of these cases we have chosen either not to become involved, or to wait until the cases reach a procedural stage (such as an appeal) at which it would become more appropriate for the Foundation to intervene.

The EFF phone line has become, to some extent, a "hotline" for people who are curious and/or worried about how their rights as citizens and as computer users may be threatened specifically or generally by government action. We have been in contact with people who were convicted of computer crimes before the EFF came into existence, and occasionally have been able to provide useful information to the lawyers handling appeals of these cases. We also have become a center for general information, with phone calls, mail, and e-mail every day requesting information about EFF and its work.

Two versions of the Massachusetts Computer Crime Bill have been introduced in the Massachusetts legislature, one of which is identical to the EFF bill which didn't pass last year. Mike, Sharon, and Mitch will all be working toward passage of the bill this year.

Conferences and Meetings
On December 19th John and Mitch spent half a day at Lawrence Livermore National Labs in Livermore, California at the invitation of the computer security management there. The trip was arranged by Russell Brand. We spoke to a large general audience of lab employees as well as had meetings with smaller groups of security experts concerned with security both at Lawrence Livermore and on the large Department of Energy computer network generally.

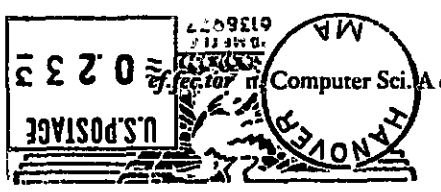
John and Mitch also appeared on a panel at Mac World at the Moscone Center on Friday, January 11th, which was chaired by Jim Warren. Also appearing was Alameda Country District Attorney Don Ingraham. John spoke in Los Angeles at a combined SIGGRAPH and ACM meeting in early January.

Compuserve
Scott Loftesness, who is a Well member, EFF supporter, and Compuserve veteran is about to open a Telecommunications forum on Compuserve which will feature an EFF sub-forum. Library materials from the Well have already been ported over. We will announce this in the EFF conference on the Well and encourage people to seed the Compuserve forum with their participation to help it get off to a good start.

EFFECTOR

The Electronic Frontier Foundation, Inc.
155 Second Street Cambridge, MA 02141

evy
Evelyn Pine
Community Memory
2617 San Pablo Avenue
Berkeley, CA 94702



ef.fec.tor n. Computer Sci. A device for producing a desired change in an object in response to input.

Contact

How to get in touch with the EFF:

Via Computer Networks:
Send requests to be added to or dropped from the EFF mailing list or other general correspondence to eff-request@well.sf.ca.us. We will periodically mail updates on EFF-related activities to this list.

If you receive USENET newsgroups, your site may carry two new newsgroups in the INET called comp.org.eff.news and comp.org.eff.talk. The former is a moderated newsgroup of announcements, responses to announcements, and selected discussion drawn from the unmoderated "talk" group and the mailing list.

Everything that goes out over the EFF mailing list will also be posted in comp.org.eff.news, so if you read the newsgroup you don't need to subscribe

Postings submitted to the moderated newsgroup may be reprinted by the EFF. To submit a posting, you may send mail to eff@well.sf.ca.us

There is an active EFF conference on the Well, as well as many other related conferences of interest to EFF supporters. As of August 1990, access to the Well is $8/month plus $3/hour. Outside the S.F. Bay area, telecom access for $5/hr. is available through CPN. Register online at (415) 332-6106.

A document library containing all of the EFF news releases, John Barlow's "Crime and Puzzlement" and others is available on the Well. We are working toward providing FTP availability into the document library through an EFF host system to be set up in Cambridge, Mass. Details will be forthcoming.

Via Mail or Telephone:
The Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141
Telephone: (617) 864-0665
Fax: (617) 864-0866

Jim Warren

Electronic frontier

Tribe — "cyberspace"

Maryland vs. Craig → closed circuit TV

forcible-testifying -

"one way mirror" analogy

"electronic trespassers" - Kenneth Rinaldo

"computer crackers" - download

credit history, viruses -

last Spring 1/4 of Treasury Dept Investigators

leaves dropping or computer

BBS's -

5 axioms of constitutional law

↳ "framework for all seasons"

check out → "Curvature of Constitutional Space" Harvard Law Review. Tribe -

decentralize & defuse gov. power → public & private

geographical

natural boundaries

Spheres of gov

Computer networks

rules of access

time shares

taxing

who can sub or -

political entities

Eli Noam - Ithiel De Poole

memorial lecture

"data havens"

individual

rights must be protected

also true of multi-national

corps, small town

communities -

shopping malls -

Pruneyard Case 1980 - access to

shopping malls to gather

signatures -

Constitution constrains Government

not private groups.

socially indispensible technology →
access as goal
- free legal assistance
- speedy trial
- desegregation

content
access
prices
} government should not intrude

bookstore vs. publisher
↓
BBS's
networks
gateways

① initial diff betw. gov. & private action

② person, mind body & property belong to person & not to groups as a whole -
(Richard Stallman: Free Software Foundation - everything in cyberspace free vs. Copyrights, patents, etc.)

private commodity → everything is not
what to privatize & what to socialize
not everything socialized –

② constitute only private property
& personality so beyond
profit & losses.

③ although info & ideas have
real effects in social world, it
is not for gov. to pick &
choose them –
info & ideas do have real
impact – so powerful &
important thing can't
be entrusted to government
? viruses as free speech –
constitutional principles can
bind –
Gov. may not control info
content as such.

4. Human spirit beyond electro
information process –

what goes on between human minds.

Penrose. The Emperor's New Mind

5th Amendment → self-incrimination

Perry vs. Mexico - what is "testimonial" evidence - using mind against you

Const. founded on normative conceptions of humanity which are not subj. to disproval.

5. Const. norms must be invariant under simple technological issues.

- wiretapping → search & seizure.

Katz vs. U.S.

Smith vs. Maryland - no search when you use PEN Register - it's you dial -

cable access to apartments →
city has to compensate
apt building

Red Lion - "scarcity" issue →
Const principles don't vary w/ technology
Const protects people not places.
9TH Amendment - enumeration of rights
doesn't deny others -
technologies don't exhaust threats
against which core values
must be defended.
22TH -
This const. protection
for speech
press
assembly
& of religion
like
liberty
property
shall be fully applicable w/out regard
to medium.

Trends in Computers and Networks -
Peter Denning - "Computers Under Attack"
Ontology: set of distinctions around which
actions are organized.

Information Ontology
- containers - documents, files, databases
- channels: wire, protocols, telephone lines
- receivers -
- transmitters -

Breakdowns
- "security as afterthought"
- ease of use
- legal ambiguities
- lack of privacy
- dossiers -
- intellectual property -
- free speech & assembly -
- insecure financial transactions.

Market Place Ontology

- conversations
- exchange transactions
- trust - authentication
- naming
- making public offers & requests
- who is in the conversation
- who can receive
- locating

John Quarterman - The Matrix as Volksnet
- ease of use of networks

Peter Neuman "Computers at Risk"
- computer security
protect personal privacy
undermine freedom of access -
defend against attacks -
make life miserable
monitor
spying on legitimate users.

Martin Hellman - Cryptography & Privacy —

- to much emphasis on technical & legislative remedies and not enough on human factor
- must admit limitations of technology
- Education by example - is social responsibility part of my approach to engineering - psychic numbing
- Export restrictions — 7 billion dollars of new weapons to Saudi
- need to include security in original def. of the problem -

David Chaum - Electronic money & beyond:

influences of technical
societal control
mechanisms
- irresistible trend toward some
new basic human rights
"informational rights"
- a mutually trusted party
of secure channels so best
to all
- the same problems are
solvable w/ and a mutually
trusted party - will
encrypted secrets

aspect "smart Cash System"

David Farber - Global Village
as Police State

large networks of security -
- across "legal" boundaries
"retroactive wiretapping" -
Transgate - O. North's Prof. Note

* * *

Areas?

International Perspectives & Impacts
European Commission Directives
about database privacy →
set of rules which EC states
will adopt as legislation
Tom Riley - Cameron
30,000 people send letters to
Lotus re: database -

Personal Information & Rights - I

Goldman ACLU -

- shift in public consciousness re: personal information → concern w/ second use
- Direct Marketing Assn.
- Equifax w/ Lotus Marketplace
- Caller ID -
- Control info personal information about themselves - loss of ability to define self in the world.

"Information Bargain" - give over certain info in order to receive something - but you're not always on equal footing, - AFDC needs SS# - not an = bargain -

- when we use info again will compensate you

- rights already exist in Bill of Rights → "reasonable expectation of privacy" is damaged
John Baker - Equifax - info services provider - explain value of services
info benefits -
- Better goods, services, prices
- convenience
- wider choices
- competition
- resource allocation
Privacy concerns -
Federal Fair Credit Reporting Act is 20 yrs. old -
- fears about Lotus Marketplace
• no good screen process for prospective users
• improper use -

- more data incorporated
- sensitive marketing info
- opt-out
- data encryption

value of info	Balance	Personal Privacy
No restriction	Some Restrictions	
Privacy is no issue	- impact of type of info	
	- sensitivity of data	
	- easy access	
	- dissemination	
	- where did info come from	

1

survey of consumer attitudes → about info practices — – widespread concern about privacy 4 out 5 strong a moderate concerns.

Buyers Market →

opin of op out based on survey –

should Indiv have absolute control over secondary use of their personal info?

Marc Rotenberg –

Alan Westin –

- kind of use
- "fair use"

issue is not about technology – technology is simply an opportunity.

Weeden

Consensual data breaches → consumers compensated for use → information Bargains is clear

Personal Info & Privacy II →

- Data mi → more developer doing privacy audits - networks - more regulation of users -

Evan Hendricks - Privacy Times

- Reagan era → explosion of use of personal info →
  - Cable TV
  - video records } videos past
  - medical records are not protected.
  - credit needs updating
  - direct marketing

"there's not enough evidence of abuse"
gene blacklisting
Tom Mandel - SRI -
ongoing study of
consumer beliefs
and values -
studies psychology
motivations for using
people buy things
future as "network society"
- collections of people
committed to specific
issues →
- increasingly fragments
social networks
- more educated the
more information
overloaded.
- more pressure on companies
to find new sources of
income

IIII 13 40.
IIIII 26 5
35

- more selling and value adding of information

1 ⊖

- 1990's - not much stability to the idea of privacy - us vs. them issues clear.

- shared disclosure will become more important and more valuable

- look for leverage for focusing on educated consumers - rest don't care about privacy

Willis Wine = Rand - Privacy developed as information use -

Tax data & census data confidential

government practices have shrunk, private practices have expanded -

privacy as "social equity"

- logging vs. conservation

privacy issues are persuasive.

use = socially accepted uses -

Simon Davies - Australian journalists - Campaign against Australian ID card -

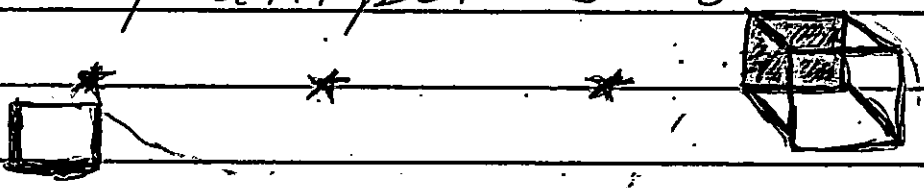
- privacy as adversarial issue

"niceness" is undermining the debate → "reasonable" "good" American corporate sector is white-out debate

new breed of privacy advocates →
pragmacate -
well trained
denounces extremes
sez debate. Has matured
this is a human rights
issue.
autonomy vs. power of
state &
corporation.
why has opting out
been taken
seriously -
you can't opt out of
your rights -
Coalition of American
Privacy Council
SEAsia → US computer
technology deals
must represent
regimes i.e. Thailand

Irving Rent

promoting technology
to Indonesia &
Philippines →



Esther Dyson —

Hal Sante — Buddhist Computer
Bulletin Board

Eric Hughes re: cognitive
response to computer
use.

Tobey - Hayes Modems →
Jim Schmidt - Freedom to Read

Tom Gillespie
(415) 528-9524 re: tutorial

Kate Chaitin re: volunteers
540-5482

Woody Weaver re: BBS
415-680-1986 / 415-631-4416
(data 1@376-8554 or wweaver@ucbcmsa)

SIGNS Fall 1990 re: Q & Computing

Eli Noam - Dir Center for Telecom & Information Studies
Columbia Univ. N.Y.

① policy report on Common Carriage

② telecom privacy

Public Service
NY Regulatory Comm.

Freedom & privacy are interlocked

new forms of media are always badly treated

electronic mail

BBS

electronic publishing -
900 #s

the last 20 inches -
display to human brain

M - 8:00 - 4:00 = 8
T - 9:00 - 10:00 = 13 hrs

issue is how to get rid of information

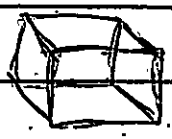
average cable TV household has set on 8 1/2 hrs/day -

change way info gets presented

information screen - common canvas →

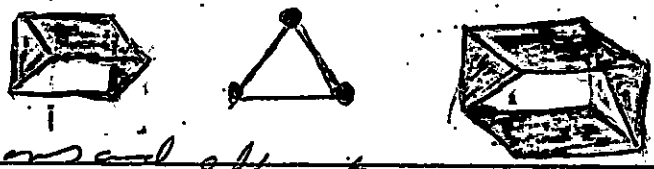
foster infrastructure of use -

network of networks -



Law Enforcement's Practices & Problems

- Glenn Tenney - Moderator
  Computer Consultant
  Hackers Conference -
- Don Ingraham - Alameda County -
  - comes of age in Cyberspace -
  myth of cyberspace -
  Victims of crime → those who have to pay costs for crime against banks & corporations -
  Cyberspace as precious -
  Widows & orphans dragged into info age → victims who don't know they are victims.
  High Tech Crime Unit set up -
  4th Amendment - the right of the people to the secure in



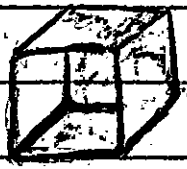
their personal effects
modest. of ethical standards
Robert Snyder - Colombia
Others -
- hardware
- intellectual property
- telecommunications
Dan Delaney - NJ State Police -
22 search warrants in past 12
months / 4 arrests -
"carding"
Dale Bull - US Secret Service
since 1985 10,000 arrests 99.9 -
are access device
fraud


BBS operators - encouraging the publishing of credit card & phone #s.

Lookups - monitoring of BBS-SS - users infamies on BBSs -

Operation Sun Devil -

- Sealed affadavits



Law Enforcement & Civil Liberties

Dorothy Denning →

Sheldon Zenner →

Mark Rasch - Dept of Justice —

— prosecuted internet of Robert Morris

- warrantless → agents have seized everything.

Cliff Figallo - The Well:

Concern of overuse of law enforcement & impact on computer community - Well as "active forum"

Sharon Beckman - att -

- represents Steve Jackson Games -

- redraft of computer crime bill -

- there is law pertaining to electronic search & seizure -

- no digression to indiv. officer → warrants have to be specific

Ken Rosenblatt – Santa Clara Co.

Mike Gibbons – FBI

Mitch Kapor – EFF

1. electronic frontier – you ain't see nothing yet –
2. don't know about 1st amendment –
3. search & seizure
4. law enforcement = black & white world
5. hacker conspiracy totally false
6. victims screwed-[illegible]

not just about civil liberties

network petri :

~~K~~ Keith Henson re: bombs ~~arti~~ [illegible] on nets.

"advocacy of imminent lawless advocacy.

Legislation & Regulation —

Jerry Berman ACLU

- electronic speech should not be granted less rights than the written word

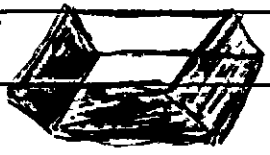
- Senator Leahy - update of FOIA act

- Video Privacy

- Gore Bill - pending - Natl & Research & Education Network

Subcommittee on Tech & the law -

Gwen Moore's staffer –
– need to define privacy policy –
– AB 4168 Personal Information –
Interns –
Steve McClellan – State of Washington
– caller ID.



① recognize that debate is about
Confidentiality but
about anonymity.
② individual ought to control
information –
③ fair use – no other kind of
use with consent
④ access to info about you

Elliott Maxwell - Pacific Telesis

Paul Bernstein →

Online BBS -

participatory democracy;

no compromise to rights
to privacy

forging custom &
usage.

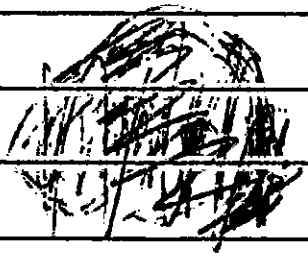
Concerns of Sysops -

- defamation of character
- copyright infringement
- obscenity
- viruses → products liability

"Electronic Networking Assn" -

1168 Bill - defines types of people who can be collected -

Jerry Berman on ACLU
are not to be accessible



"participatory democracy"
vs.
"interest group democracy."

"Intelligent Network Task force" → Pacific Bell.

7 percent contacts legislature during their lifetime.

Surveillance of individuals

FBI library awareness program —
Math/Sci Library at Columbia
University - librarian
asked to keep track of
what foreign nationals
were reading.
uses public makes of library
are private
1970 IRS visited Milwaukee
Public Library trying to
track down Weather
Underground.
Confidentiality of library
records - can't
identify individuals
w/ materials →
trying to extend to
services & facilities

court order which shows proper cause & is in order →
1200 pages of documentation of FBI - re: investigation of the Nazis —
Karen Nussbaum 9 to 5
26 million employees
same work.
tracked by
computers —
mail
nurses
phone operators
airline & hotel
readers —
newspaper reporter
invasive management
technique - monitors
mob-psych work,
but is others.

Supervision via real time -
drug testing
hand writing analysis
integrity tests

monitoring = "objective
evaluation"
= "improves
productivity"

the way to improve productivity
is double squeeze on workers
→ control & fear
Paul Simon - Bill to prohibit
abuse of monitoring

Gary Marx - MIT - Protest and
Prejudice
Undercover

9 forms of computer surveillance
① Ban
David Flaherty —

Electronic Speech, Press & Assembly

- Eric Lieberman:
  - Ellsberg - Pentagon Papers - NY Times never prosecuted - hassled on basis of "nat. security issue" - rather than that they were stolen -
  - Electronic Communicators - BBS's - are subject to search & seizure etc. on basis of liability for stolen information —
  - are BBS-s required to be censored.

How do you apply "core values" of First Amendment -

- Computer more than electronic file cabinet - it is means of exchange -

• Computers as poets muse -
• 1st amendment protects more of speech of large corporate media
• Broadcasters - limited access to media.
"Oppression like darkness does not come upon us suddenly." Justice Douglas.
- Jack Richard - Boardwatch Magazines -
• BBSs & small on-line services
• ability to access useable information out of cloud of "over information"
• BBS as specialty publishing medium
• "native librarian" -
• Dec 89 15,000 public dial up system
60,000 by end of the year
emerging cottage industry caters to technically inclined
Bob & Tracy Mahoney in

- core of people whose made to
  economically in bulletin
  board system
- other means for home-based
  business - dream is web,
  successstories to point to.
- "native librarians" standing to
  see BBS for passion
  - name coins
  - sailing ships
  - guns
  - home education
  - rights of adopted
    husbands
  - scuba diving
  - amateur radio
  - ferrets as pets
  - weather satellite
    images
  - politics
  - disabled

"Petri Dish of Experimentation"

networkers of BBS's on political issues —

- adoption issues →

industry in embryonic stage →
driven by individuals funding
it from out of pocket -

legal threats -

- legal systems best serves itself
- Craig Neidorf & Steve Jackson

-

John McMullen -

Bio - began w/ DOD -

- 60-78 - large commercial data processing
- 1978 - Consultants to computer users -
+ journalists

Electronic communications - Edits
East Coast news service - newsbytes
30 stories per day picked up
by dialog, American On-Line,
Computer Currents - commercial
activity - resp. to protect

copyrights - no plagerism
idea of plagerism is change
protects self thru libel,
slander, etc.
post stuff on Well →
- used newsletters on Prodigy -
for free but they stopped
doing it -
- EFF - not for profit →
Other newsletters — Phrack - Crazy
Neidorf - dist to 300 people -
NPO - suspended in 1989
when he was indicted &
his equipment - would not
have taken Genie equipment
or associated pers -
Email vs. Electronic publishing -
Nuances of issues make it
to difficult to forge job here.

David Hughes → on-line 5 hrs a day for 10 years -

- on-line communicated is unprecented

is debate discussion

~~speech~~

discourse -

- Electronic Privacy Act of 1986 -

- Mind to mind communication →

Absolute freedom of electronic

~~freedom of speech~~ -

Don't need to confuse - computers as place

or speech as data -

George Perry - Prodigy -

established seven years ago -

4 yrs - in developed

product on the market

2 1/2 years -

Nat. availability last September

wanted to play leading

role in development

of new media -

{info services
transaction of services -
affordable -
low cost -
"most user friendly
interface"
one to many communications -
"disinformation" campaign -
"it's not a common
carrier but a contract
carrier."

Lance Rose - attorney -
people remain people in cyberspace
you can contract away your right
to free speech
right of paternity → rights of
your name -
Trademark right →
Right of publicity
Trade Secret.

("duty to report")

banking services - truth in lending laws -

BBS ops - subject to criminal laws
dist. of viruses
obscenity
trafficking in access devices
pirating software
wire fraud
all laws relating to electronic systems should be national

* getting computer tools of telecommunications tools consumer-oriented printers

"diversity"

"Disinformation"
Products -
Since 1973 -
getting computer tools into the hands of a broad range of people -
to share info -
which people are most comfortable speaking

3/28/91

Harry Hammitt

FOI - statutory right to request records from Executive Agency

Ethics and Education — 3/

T. Winograd —

— teaches course ab Stanford on computers, ethics, and social responsibility.

(+ Sarah Freedman ab Mills College re: ethics & computers)

+ Richard Hollinger —

"why" questions

— rapid rise in criminalization of computer-related deviance —

— have we created a "criminogenic" culture when we teach computers →

• Robert Mason → background & education should know values

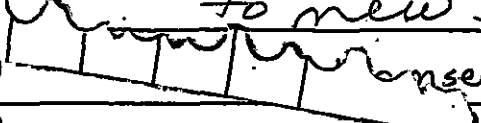
— reward values of intuitiveness, aggressiveness, push the envelope.

- no agreed upon morays
- legislative route is ineffective
- law enforcement can't stop unethical behavior
- burdens on industry
- "hackers ethics" - promise for a fundamentally different society.
- lag between new technology & then creation of moral / ethical norms
- laws will be made → criminality is created

Donn Parker - SRI -
2 studies on ethics in computer
14 yrs ago
3 yrs ago
Sample problem & then evaluating scenarios
- law

- law
- convention - codes of conduct
- ethics -

can't teach ethics → can teach application of ethics to new environment



- higher ethic principle - trade off
- use most restrictive principle
- Universal - what's not right for everyone, then it's not right for anyone.
- Descartes change rule → escalation of ethical violations
- owner's rule - assume that others are going to treat your service as in the public domain -
- user's rule - assume that it belongs to somebody else unless it explicitly in public domain

hacker ethic - info is free - system must be available to the people.

teaching ethics can be integrated

Dorothy Denning - moving to Georgetown to Chair computer science department -

Example →

- parents copy videos & software
- schools tell students to copy
- companies misuse information -
- not building secure system
- cation.
- parents don't give it - don't have time -
- quality of learning more engaging as it is at schools.

- Schools - Brian Harvey →
- Students mob given use of modems - as much abuse of phones as computers
deeper crisis of values →
John Gilmore - Sun Microsystems
EFF
believe in open society
belief in privacy.
id's
cash
free assn -
1 of people in jail →
worry about protecting diversity
financial privacy -
just laws need to be enforced -

stop building and supporting
false secure systems
Nat. Inst. of Justice - "Build -

✓October = Computer
learning
Month ✓

Corporate funding

- Not important -
- marginal cost

Don Parker - large scale computer
business world - SRI -
- Apple
- Siemens
- IBM
- Banks
- Chemicals
- Pharmaceuticals

Assn of Trial Lawyers
of America.

Thompson Pitts - case - stolen Pacific
Telephone etc.

Stir the pot.
Stake it up.

3/29/91
Computers, Privacy & Freedom.

Mitch Kapor - EFF Contin[illegible]

Co committments

to help in the civilization of cyberstation

- computer networks must be readily accessible to the average person -

2 new initiatives

① issue of national info infrastructure -
national public network -
new elements to policy discussion -
what are the social policies
own
control
access
diversity

as important as techn

issues –
computer & networks users
need a voice in
infrastructure
– virtually impossible
for non expert to
master the net
without extreme
work – The Big
Business Guide to
① the Net
– Going to continue
to engage in
legal work to
support and
defend – up
to & including
lawsuits.
② build on relationships
with other constituencies
to avoid going to court

development of research of designing guidelines —

(3) continue to fight misperceptions about inhabitants of cyberspace

(4) memberships → creating a forum for involvement.

On Engahan — Alameda County —

Penal Code 630 Calif.

EFFECTOR

Effector – The Newsletter of the Electronic Frontier Foundation

March 1991
Volume 1 Number 1

Goals of the EFF

1. To engage in and support educational activities that increase the popular understanding of the opportunities and challenges posed by computing and telecommunications.

2. To develop among policy-makers a clearer comprehension of the issues underlying free and open telecommunications.

3. To support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.

4. To raise public awareness about civil-liberties issues arising from rapid advances in computer-based communications media.

5. To support litigation in the public interest to preserve, protect, and extend Constitutional rights to the realm of computing and telecommunications technology.

6. To encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

A Man From the FBI:

The Origins of the Electronic Frontier Foundation

By John Perry Barlow

The Electronic Frontier Foundation was started by a visit from the FBI.

In late April of 1990, I got a call from Special Agent Richard Baxter of the Federal Bureau of Investigation. He asked if he could come by the next day and discuss a certain investigation with me. His unwillingness to discuss its nature over the phone left me with a sense of global guilt, but I figured turning him down would probably send the wrong signal.

On Mayday, he drove to Pinedale, Wyoming, a cow town 100 miles north of his Rock Springs office (where he ordinarily investigates livestock theft and other regional crimes). He brought with him a thick stack of documents from the San Francisco office and a profound confusion about their contents.

He had been sent to find out if I might be a member of the NuPrometheus League, a dread band of info-terrorists (or maybe just a disaffected former Apple employee) who had stolen and wantonly distributed source code normally used in the Macintosh ROMs. Agent Baxter's errand was complicated by a fairly complete unfamiliarity with computer technology. I realized right away that before I could demonstrate my innocence, I would first have to explain to him what guilt might be.

The three hours I passed doing this were surreal for both of us. Whatever this source code stuff was, and whatever it was that happened to it, had none of the cozy familiarity of a few yearling steers headed across the Wyoming border in the wrong stock truck.

What little he did know, thanks to the San Francisco office, was also pretty well out of kilter. He had been told, for example, that Autodesk, the publisher of AutoCAD, was a major Star Wars defense contractor and that its CEO was none other than John Draper, the infamous phone phreak also known as Cap'n Crunch. As soon as I quit laughing, I started to worry.

I realized in the course of this interview that I was seeing, in microcosm, the entire law enforcement structure of the United States. Agent Baxter was hardly alone in his puzzlement about the legal, technical, and metaphorical nature of datacrime.

I also found in his struggles a framework for understanding a series of recent Secret Service raids on some young hackers I'd met in a Harper's magazine forum on computers and freedom. And it occurred to me that this might be the beginning of a great paroxysm of governmental confusion during which everyone's liberties would become at risk.

When Agent Baxter had gone, I wrote an account of his visit and placed it on the WELL, a computer BBS in Sausalito which is digital home to a large collection of technically hip folks, including Mitch Kapor, the father of Lotus 1-2-3.

Turns out Mitch had also been visited by the FBI, owing to his having unaccountably received of one of the source code disks which NuPrometheus scattered around. Mitch's experience had been as dreamlike as mine. He had, in fact, filed the whole thing under General Inexplicability until he read my tale on the WELL. Now he had enough corroboration for his own strange sense of alarm to begin acting on it.

Several days later, he found his bizjet about to fly over Wyoming on its way to San Francisco. He called me from somewhere over South Dakota and asked if he might literally drop in for a chat about Agent Baxter and related matters.

So, while a late spring snow storm swirled outside my office, we spent several hours hatching what became the Electronic Frontier Foundation. I told him about the sweep of Secret Service raids that had taken place months before and their apparent disregard for the Bill of Rights.

Alarmed, he gave me the phone number of Harvey Silverglate, whose willingness to champion unpopular causes was demonstrated by his current defense of Leona Helmsley. He said that Harvey would probably know if this were as bad as it was starting to sound. He also said that he would be willing to pay the bills that generally start to appear whenever you call a lawyer.

I finally found Harvey in the New York offices of Rabinowitz, Boudin, Standard, Krinsky and Lieberman, a firm whose long list of successfully defended civil-liberties cases includes the Pentagon Papers case. I told him and Eric Lieberman what I knew about recent government flailings against cybercrime. They were even less sanguine than I had been.

The next day a trio code-named Acid Phreak, Phiber Optik, and Scorpion entered the walnut-panelled chambers of Rabinowitz, Boudin and told their tales to a lawyer there named Terry Gross. While EFF as a formal organization would not exist for two months, its legal arm was already flexing its muscle.

A few days later I received a phone call from the technology writer for the Washington Post. He was interested in following up on the Harper's forum, and knew nothing of Mitch's and my joint endeavors. I filled him in, hoping to expose the Secret Service. Several days later, the Post published the first of many newspaper stories, all of which could have shared the headline: "Lotus Founder Defends Hackers."

continued page 2

Why Defend Hackers?

By Mitchell Kapor

An all-too-common perception of the EFF that prevails in the computer industry and those who report on it—from John Sculley to the Wall Street Journal—is that the EFF is an organization that has "something to do with hackers." (They use "hackers" as a term not of approbation but of rebuke). Most of these sometime colleagues and associates of mine are puzzled as to why I would be doing such a thing. (A few think I've just become a loony.) Anyway, they've heard about the terrible problems caused by hackers who break into computer systems, they worry that I'm out to defend such practices, and they disapprove.

But their disapproval is based on the pure misconception that the EFF's purpose is to defend people's right to break into computer systems. Let me clear up that misconception now.

I regard unauthorized entry into computer systems as wrong and deserving of punishment. People who break into computer systems and cause harm should be held accountable for their actions. We need to make appropriate distinctions in the legal code among various forms of computer crime, based on such factors as intent and the degree of actual damage. In fact, the EFF has drafted a bill that has the backing

continued page 3

Washington Watch

by Marc Rotenberg

• *Computer Crime Legislation*

Several proposals to expand computer crime law were introduced in the past Congress. In the end, a modest proposal, introduced by Senator Leahy, passed the Senate but did not make it through the House. Senator Leahy's bill would have penalized reckless computer acts that place computer systems at risk and would have required that the Justice Department report annually to Congress on computer crime prosecutions

• *National ID Card*

A proposal to begin a national ID card pilot project, tucked into amendments to the Immigration Control and Reform Act, was knocked out when civil libertarians objected.

• *Electronic Dissemination Policy*

A proposal to establish principles for the dissemination of electronic information by the federal agencies narrowly failed to pass the Congress as last minute negotiations on a related measure collapsed. The proposal grows out of a report from the Office of Technology Assessment "Informing the Nation" that stressed the need to develop new information policy to promote the development of CD-ROMs and on-line information services.

• *Caller ID*

A bill to allow the offering of Caller ID by regional phone companies if a per-call blocking feature is also provided failed to gather support this past Congress. Several states have already adopted similar measures.

• *Computer Security Policy*

The Presidential directive on computer security policy was revised finally to comply with the Computer Security Act of 1987. The Act reestablished control for computer security at a civilian agency — the National Institute for Standards and Technology — after the previous administration attempted to place computer security authority at the National Security Agency.

• *Upcoming Policy*

CPSR hosted the first Computing and Civil Liberties policy roundtable on February 21 and 22, 1991 at the American Association for the Advancement of Science in Washington, DC. The purpose of the roundtable was to bring together leading experts to explore two issues: free speech and computer networks, and searches of computer bulletin boards. What speech restrictions currently exist? Should federal agencies or private companies be allowed to restrict the content of a computer message and, if so, in what circumstances? The second issue was the investigation of computer bulletin boards by law enforcement agents. Are there any restrictions on the ways that police may monitor computer communications and computer bulletin boards? If not, should such restrictions be developed? The conference was the first in a series of policy roundtables that will be held in Washington, DC and that are made possible with funding from the Electronic Frontier Foundation.

EFFECTOR

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

The Board of the Electronic Frontier Foundation:
Mitchell Kapor, John Barlow, John Gilmore, Stewart Brand, Steve Wozniak
Staff Counsel: Mike Godwin
Staff Volunteer: Leila Gallagher

EFFECTOR was edited and produced by Gerard Van der Leun

Art Direction and design by Lisa DeFrancis, DeFrancis Studio, 80 Trowbridge Street, Cambridge, MA 02138

FBI ***continued***

While this was an irritating misrepresentation, we were more interested in defending the Constitution than digital miscreants, the publicity produced a couple of major supporters: Steve Wozniak, who called and offered an unlimited match to Mitch's contributions, and John Gilmore (Sun Microsystems employee #5) who e-mailed me a six figure offer of support.

Operation Sundevil

Meanwhile, the list of apparent outrages lengthened. We learned about an Austin role-playing games publisher named Steve Jackson whose office equipment had been confiscated by the Secret Service in an apparent effort to restrain his publication of a game called Cyberpunk which they thought, with ludicrous inaccuracy, to be "a handbook for computer crime."

All over the country computer bulletin boards were being confiscated, undelivered e-mail and all. A Secret Service dragnet called Operation Sundevil seized more than 40 computers and 23,000 data disks from teenagers in 14 American cities, using levels of force and terror which would have been more appropriate to the apprehension of urban guerrillas than barely postpubescent computer nerds.

And there was the Craig Neidorf case. Neidorf, also known by the nom de crack Knight Lightning, had published an internal BellSouth document in his electronic magazine Phrack. For this constitutionally protected act, Neidorf was being charged with interstate transport of stolen property with a possible sentence of 60 years in jail and a $122,000 in fines.

I wrote a piece about these events called "Crime & Puzzlement." I did so at the request of the Whole Earth Review—it made its first print appearance in the Fall 1990 issue of WER—but I "published" it on the Net in June and was astonished by the response. It was like planting a fence-post and discovering that the ground into which you've driven it is actually the back of a giant animal that quivers and heaves at the irritation.

By July, I was receiving up to 100 e-mail messages a day. They came from all over the planet and expressed nearly universal indignation. I began to experience datashock, but I also realized that Mitch and I were not alone in our concerns. We had struck a chord.

The Law In Cyberspace

In Cambridge, Mitch was having something like the same experience. Since the Washington Post story, he found himself bathed in media glare. However, the more he learned about ambiguous nature of law in Cyberspace, the more of his considerable intellectual and financial resources he became willing to devote to the subject.

In late June, Mitch and I threw several dinners in San Francisco, to which we invited major figures from the computer industry. We weren't surprised to learn than many of them had exploits in their past which, undertaken today, would arouse plenty of Secret Service interest. It appeared possible that one side-effect of current government practices might be the elimination of the next generation of computer entrepreneurs and digital designers.

It also became clear that we were dealing with a set of problems which was a great deal more complex and far-reaching than a few cases of governmental confusion. The actions of the FBI and Secret Service were symptoms of a growing social crisis: Future Shock. America was entering the Information Age with neither laws nor metaphors for the appropriate protection and conveyance of information itself.

We realized that our legal actions on behalf of a few teen-age crackers would go on indefinitely without much result unless something were done to ease social tensions along the electronic frontier. The real task at hand was the civilization of Cyberspace. Such an undertaking would require more juice and stamina than two men could muster, even amplified by the Net and a solid financial supply. We would need some kind of organizational identity.

With this in mind, we hired a press coordinator, Cathy Cook (who had formerly done PR for Steve Jobs), set a squad of lawyers to work on investigating the proper organizational tax status, and, over a San Francisco dinner with Stewart Brand, Nat Goldhaber, Jaron Lanier, and Chuck Blanchard, we selected a name and defined a mission.

Founding the Foundation

We announced the formation of the Electronic Frontier Foundation at the National Press Club on July 10. Mitch and I were joined for the announcement by Harvey Silverglate, Terry Gross, and Steve Jackson.

We were also joined by Marc Rotenberg of the Washington office of Computer Professionals for Social Responsibility. One of our first official acts had been to grant that organization $275,000 for a project on computing and civil liberties. CPSR would keep a wary eye on developments "inside the Beltway" and work in conjunction with congressional staffers to see that any legislation dealing with access to information was sensibly drafted.

While in Washington, we also took inventory of the terrain, meeting with congressional staffers, the Washington civil liberties establishment, and officials from the Library of Congress and the White House. The area to be covered, from intellectual property to telecommunications policy to law enforcement technique, was daunting, as were the ambient levels of confusion and indifference.

We also generated an enormous amount of press. And it became apparent that not everyone was persuaded of our cause. Business Week called Mitch naive for his willingness to believe that computer crackers were somehow less dangerous that drug kingpins. Various burghers of the computer establishment, ranging from the executive director of the Software Publishers Association to a columnist for ComputerWorld, called us fools at best and, more likely, dangerous fools.

The Wall Street Journal printed a particularly hysterical piece which alleged that the document Craig Neidorf (into whose case we had entered a supporting amicus brief) had published was a computer virus capable of bringing down the emergency phone system for the entire country. In fact, the text file which Neidorf distributed dealt with the bureaucratic procedures of 911 administration in the Bell-South region and contained nothing which could be used to crack a system. Indeed, it contained nothing which could not be easily obtained through by legal means.

Neidorf's first major break came in late July. Thanks in part to the independent work of John Nagel, who was prepared to testify that the prosecutors had seriously overstated the value of the E911 document, the government was forced to abandon its case against Neidorf after 4 days in Chicago's Federal Court.

Although our briefs supporting Neidorf's activities under the First Amendment were not admitted, it became apparent, before such loftier matters could even be broached, that the government had indicted him with no clear understanding of the purpose or availability of the document he had distributed. Like Agent Baxter, they knew too little to critically examine the misinformation they had been given by the corporate masters, in this case, officials at Bellcore.

Following the resolution of the Neidorf case, and, to some extent because of it, skepticism of EFF has moderated considerably. If anything, the most recent press accounts of our activities have been almost fulsome in their praise. Recent favorable coverage has appeared in the New York Times, The Economist, Infoworld, Information Week, PCweek, and Boston Magazine.

Since July, we have been absurdly busy on numerous fronts: We've worked on raising public awareness of the issues at stake. We are organizing legal responses to the original and continuing intemperance of law enforcement. We have worked on the political front, developing and lobbying for rational computer security legislation. We have started to create a network of interested experts on computer security, intellectual property, telecommunications policy, and international information rights. And lately we've been attending to the organizational demands of the non-profit equivalent of a hyper-successful computer startup.

The Expanding Mission

When we first defined the mission of the Electronic Frontier Foundation, we saw our task as assuring the application of the U.S. Constitution to digital media. And this remains much of what we are about.

However, information has little natural regard for national borders or local ordinances. Cyberspace is transnational. During the tsunami of e-mail which Crime & Puzzlement elicited, there were many items from foreign countries. Their authors wanted to know how they could protect or establish their rights of free expression. And I had no idea what to tell them.

The question arose again at Esther Dyson's recent East-West Technology Conference in Budapest which Mitch and I attended. EFF was well-known among the Soviets at this meeting, some of whom were already involved in drafting what they called an Information Bill of Rights. (One young Moscow programmer had managed to hack together an Internet connection through Finland in order to contact me.)

Like intellectual property and telecom policy, the development of international principles of free digital speech is a large angel to wrestle with. We will have to be careful not to allow this immense task to divert EFF from its specific legal agenda. But neither can we ignore the fact that Cyberspace is hardly an American territory.

The Electronic Frontier Foundation grew from an effort to fight a specific legal brushfire into a full-fledged Cause much faster than we could have imagined. And, like any explosive start-up, it spends a lot of time playing catch-up.

Reaching Out

Electronically amplified, Mitch and I were able to personally conduct much of EFF's business in the first few months of operations. But gradually we had to confront the fact that while the Net is very broad, it is also quite shallow. Without even a sense of their physical location, we have been unable to marshal the hundreds of people who have e-mailed us with their volunteered services. Also, we found ourselves administering a significant cash-flow in both donations and expenditures. (By year's end, EFF will have spent around $220,000. Our tentative 1991 budget predicts expenses of almost half a million.)

So, despite a mutual terror of bureaucracy and organizational sclerosis, we have started to adopt some institutional trappings.

First, in order to satisfy the requirements for a 501c3 tax status (which we should have in about six months), we found that we needed something more substantial than two guys with modems. Thus, on October 9, we held our first official board meeting and formally elected Stewart Brand, Steve Wozniak, and John Gilmore to join us as board members.

And we have started to take on staff. We recently hired Mike Godwin, a freshly minted Texas lawyer and USENET adept, to sort through the factual and legal details of the many cases we are being asked to intervene in. In his short time with us, he has investigated several cases to determine their fit with EFF's constitutional mission, their winnability, and their likelihood of producing clear legal precedent.

We are determined that EFF will remain an agile, swift-moving sort of outfit. We will adopt any new bureaucratic manifestations with the greatest skepticism. But we are being bombarded with many legitimate requests for assistance, advice, and information. In order to respond rapidly and appropriately, the Electronic Frontier Foundation has had to become an institution. One method by which we hope to maintain organizational lightness involves keeping a clear distinction between strategy and tactics.

On the strategic level, EFF has a very broad mission involving such amorphous endeavors as defining intellectual property, helping establish a transnational culture of information, designing telecommunications policy, sponsoring humane software design... civilizing Cyberspace. With an appropriate sense of their limitations, the board members will remain responsible for these matters.

This will prevent the staff's losing tactical focus on more tangible action items like litigation, political action, communicating through the press and across the Net, and organizational care and feeding.

The problem with history is that it keeps happening. Today, as I was working on this EFF mini-biography, I learned that Mitch has just had his fingerprints subpoenaed by the FBI. Turns out they are now examining the NuPrometheus distribution disks for fingerprints and want to be able to sort his out. Or, perhaps, search for their appearance on other disks...

So the Wheels of Justice grind blindly on. And we will go on trying to prevent anyone's being ground up in them. ✍

Postcard from the Edge

"I went on to test the program in every way I could devise. I strained it to expose its weaknesses. I ran it for high-mass stars and low-mass stars, for stars born exceedingly hot and those born relatively cold. I ran it assuming the superfluid currents beneath the crust to be absent — not because I wanted to know the answer, but because I had developed an intuitive feel for the answer in this particular case. Finally I got a run in which the computer showed the pulsar's temperature to be less than absolute zero. I had found an error. I chased down the error and fixed it. Now I had improved the program to the point where it would not run at all."

George Greenstein,
"Frozen Star: Of Pulsars, Black Holes and the Fate of Stars"

How Prosecutors Misrepresented the Atlanta Hackers

Reading Between the Lines of the BellSouth Sentences

By Mike Godwin

Although the Electronic Frontier Foundation is opposed to unauthorized computer entry, we are deeply disturbed by the recent sentencing of Bell South hackers/crackers Riggs, Darden, and Grant. Not only are the sentences disproportionate to the nature of the offenses these young men committed, but, to the extent the judge's sentence was based on the prosecution's sentencing memorandum, it relied on a document filled with misrepresentations.

Robert J. Riggs, Franklin E. Darden, Jr., and Adam E. Grant were sentenced Friday, November 16, in federal court in Atlanta. Darden and Riggs had each pled guilty to a conspiracy to commit computer fraud, wire fraud, access-code fraud, and interstate transportation of stolen property. Grant had pled guilty to a separate count of possession of access codes with intent to defraud.

All received prison terms; Grant and Darden, according to a Department of Justice news release, "each received a sentence of 14 months incarceration (7 in a halfway house) with restitution payments of $233,000." Riggs, said the release, "received a sentence of 21 months incarceration and $233,000 in restitution." In addition, each is forbidden to use a computer, except insofar as such use may be related to employment, during his post-incarceration supervision.

The facts of the case, as related by the prosecution in its sentencing memorandum, indicate that the defendants gained free telephone service and unauthorized access to BellSouth computers, primarily in order to gain knowledge about the phone system. Damage to the systems was either minimal or nonexistent. Although it is well-documented that the typical motivation of phone-system hackers is curiosity and the desire to master complex systems, the prosecution attempts to characterize the crackers as major criminals, and misrepresents facts in doing so.

Examples of such misrepresentation include:

1. Misrepresenting the E911 file.

The E911 file, an administrative document, was copied by Robert Riggs and eventually published by Craig Neidorf in the electronic magazine PHRACK. Says the prosecution: "This file, which is the subject of the Chicago [Craig Neidorf] indictment, is noteworthy because it contains the program for the emergency 911 dialing system. As the Court knows, any damage to that very sensitive system could result in a dangerous breakdown in police, fire, and ambulance services. The evidence indicates that Riggs stole the E911 program from BellSouth's centralized automation system (i.e., free run of the system). Bob Kibler of BellSouth Security estimates the value of the E911 file, based on R&D costs, is $24,639.05."

This statement by prosecutors is clearly false. Defense witnesses in the Neidorf case were prepared to testify that the E911 document was not a program, that it could not be used to disrupt 911 service, and that the same information could be ordered from Bell South at a cost of less than $20. Under cross-examination, the prosecution's own witnesses admitted that the information in the E911 file was available in public documents, that the notice placed on the document stating that it was proprietary was placed on all Bell South documents (without any prior review to determine whether the notice was proper), and that the document did not pose a danger to the functioning of the 911 system.

2. Guilt by association.

The prosecution begins its memorandum by detailing two crimes: 1) a plot to plant "logic bombs" that would disrupt phone service in several states, and 2) a prank involving the rerouting of calls from a probation office in Florida to "a New York Dial-A-Porn number."

Only after going to some length describing these two allegations does the prosecution state, in passing, that *the defendants were not implicated in these crimes.*

Elsewhere in the memorandum, the prosecution attempts to suggest the defendants' responsibility in a third offense—another person's crime. Because the defendants "freely and recklessly disseminated access information they had stolen," says the memorandum, a 15-year-old hacker committed $10,000 in electronic theft. Even though the prosecution does not say the defendants intended to facilitate that 15-year-old's alleged theft, the memorandum seeks to implicate the defendants in that theft.

3. Guilt by knowing too much.

The prosecution goes to great lengths describing the crimes the defendants *could* have committed with the kind of knowledge they had gathered: "During the course of the conspiracy, the defendants and other LOD [Legion of Doom] members illegally amassed enough knowledge about the telecommunications computer systems to jeopardize the entire telephone industry!"

The prosecution does not mention, however, that the mere possession of dangerous knowledge is not a crime, nor does it state, explicitly, that the defendants never conspired to cause such damage to the phone system.

4. Misrepresentation of motives.

As noted above, it has been documented that young phone-system hackers are typically motivated by the desire to understand and master large systems, not to inflict harm or to enrich themselves materially. Although the prosecution concedes that "[d]efendants claimed that they never personally profited from their hacking activities, with the exception of getting unauthorized long distance and data network service," the prosecutors nevertheless characterize the hackers' motives as similar to those of extortionists: "Their main motivation [was to] obtain power through information and intimidation."

5. Failure to acknowledge the outcome of the Craig Neidorf case.

In evaluating defendants' cooperation in the prosecution of Craig Neidorf, the government singles out Riggs as being less helpful than the other two defendants, and recommends less leniency because of this. Says the memorandum: "The testimony was somewhat helpful, though the prosecutors felt defendant Riggs was holding back and not being as open as he had been in the earlier meeting." The memorandum fails to mention, however, that Riggs's testimony tended to support Neidorf's defense that he had never conspired with Riggs to engage in the interstate transportation of stolen property or that the case against Neidorf was dropped.

Perhaps the most egregious aspect of the governments's memorandum is the argument that Riggs, Grant, and Darden should be imprisoned, not for what *they* have done, but to send the right "message to the hacking community." The government focuses on the case of Robert J. Morris Jr., the computer-science graduate student who was sentenced to a term of probation in May of this year for his release of the worm program that disrupted many computers connected to the Internet. Urging the court to imprison the three defendants, the government remarked that "hackers and computer experts recall general hacker jubilation when the judge imposed a probated sentence. Clearly, the sentence had little effect on defendants Grant, Riggs, and Darden."

The government's criticism is particularly unfair in light of the fact that the Morris sentencing took place almost a year *after* the activities leading to the defendants' convictions!

The memorandum raises other questions besides those of the prosecutors' biased presentation of the facts. The most significant of these is the government's uncritical acceptance of BellSouth's statement of the damage the defendants did to its computer system. The memorandum states that "In all, [the defendants] stole approximately $233,880 worth of logins/passwords and connect addresses (i.e., access information) from BellSouth. BellSouth spent approximately $1.5 million in identifying the intruders into their system and has since then spent roughly $3 million more to further secure their network."

It is unclear how these figures were derived. For one thing, the stated cost of the passwords is highly questionable: What is the dollar value of a password?

And it's similarly unclear that the defendants caused BellSouth to spend $4.5 million more than they normally would have spent in a similar period to identify intruders and secure their network. Although the government's memorandum states that "[t]he defendants ... have literally caused BellSouth millions of dollars in expenses by their actions," the actual facts as presented in the memorandum suggest that BellSouth had already embarked upon the expenditure of millions of dollars *before* it had heard anything about the crimes the defendants ultimately were alleged to have committed.

Not only are there questions about the justice of the restitution requirement in the sentencing of Riggs, Darden, and Grant, but there also are Constitutional issues raised by the prohibition of access to computers. The Court's sentencing suggests a belief that anything the defendants do with computers is likely to be illegal; it ignores the fact that computers are a communications medium, and that the prohibition goes beyond preventing future crimes by the defendants—it treads upon their rights to engage in lawful speech and association.

EFF does not support the proposition that computer intrusion and long-distance theft should go unpunished. But we find highly disturbing the misrepresentations of facts in the prosecutors' sentencing memorandum as they seek disproportionate sentences for Riggs, Darden, and Grant—stiff sentences that supposedly will "send a message" to the hackers and crackers.

The message this memorandum really sends is that the government's presentation of the facts of this case has been heavily biased by its eagerness to appear to be deterring future computer crime.

Why Defend Hackers *continued*

of the Governor and Attorney General of Massachusetts and that embodies these principles.

But if the EFF isn't trying to advance the cause of computer hackers, you may ask, what is it doing and why? What is it that was sufficiently powerful to motivate me to help start a whole organization?

As I began to find out the real story behind government raids and indictments last summer, I became incensed at the fact that innocent individuals were getting caught up in the blundering machinations of certain law enforcement agencies and large corporations. These were kids really, young people with whom I identified, who faced the prospect of having their lives ruined.

Take Craig Neidorf for example. Neidorf, a defendant in one case and the publisher of an electronic newsletter, was indicted on felony charges of wire fraud and interstate transportation of stolen property. Neidorf had published a document about administrative procedures used in the 911 emergency response telephone system that someone else had removed from a BellSouth computer. On the fourth day of the trial, the prosecution dropped the case after it became clear that the information in the "highly confidential" BellSouth document at issue was publicly available for less than $20.

Justice was served by the government's decision to drop the case, but it was expensive justice. Neidorf and his family face $100,000 in legal bills, to say nothing of the disruption and suffering caused by the trial for an action that should never have been brought against him to begin with.

In a second case, the EFF continues to assist Steve Jackson, a game manufacturer in Austin, Texas, who has suffered substantial business losses after a Secret Service raid in early March. The seizure of Jackson's computer equipment caused him to lay off nearly half of his staff and threatened the survival of the business. As subsequent revelations have showed, there was no good reason for this raid. It never should have been permitted to occur in the first place.

While helping defend the innocent is one role for the EFF to play, there is more at stake than trying to prevent individuals from being wronged. It is also a matter of rights for all of us.

The legal protections afforded Craig Neidorf's electronic newsletter and its publisher and the computer bulletin board system (BBS) seized in the Steve Jackson raid are neither clear nor well-established. I believe it is terribly important to extend to these new digital media the same strong First Amendment protections of freedom of speech and freedom of expression which we enjoy in our own lives and in the print media. The government should not be able to seize a BBS any more easily than they can seize a printing press. We must find ways for law enforcement to do its job in protecting the property of some of us without violating the freedom of speech of the rest of us. This is clearly a matter of protecting civil liberties and familiar to those who take an interest in upholding the Bill of Rights, but it is also more than that.

These embryonic media of electronic mail, BBSs, and conferencing systems, provide open forums of communication. They are an antidote to the corrosive effects of the power of large, centralized institutions, private and public, and to the numbness induced by one-way, least-common-denominator mass media.

In the global suburbs in which more and more of us live, one's horizon is limited to the immediate family. Even close neighbors are often anonymous.

In the realities that can be created within digital media there are opportunities for the formation of virtual communities—voluntary groups who come together not on the basis of geographical proximity but through a common interests. Computer and telecommunications systems represent an enabling technology for the formation of community, but only if we make it so. I believe it is urgent, as a matter of national policy, that we encourage and further stimulate the social experiments and developing infrastructure that are taking place on the Net every day. The ultimate mission of the EFF is to help articulate this vision and play a constructive role in the working out of the new legal and social norms which we are faced with developing.

As John Barlow and I meditated together last June on the broader implications of the initial events—a meditation that catalyzed the formation of the EFF—we could see that what was at stake was not merely seeing justice be served in the case of a few individuals, nor simply the preservation of the civil liberties of all of us, although these goals are vitally important.

The larger issue is how our society will come to terms with the onrush of transformative technology. If we take the right steps now—and EFF is working to take those steps—new and increasing access to information technology will enhance rather than inhibit the positive growth and development of individuals, of communities, and of society as a whole.

20 Things You Can Do to Advance Electronic Freedom

1. Spread the word about EFF as widely as possible, both on and off the Net.

2. Be alert for any local, state or national legislation that effect electronic freedom.

3. Put the immense processing horsepower of your mind to the task of finding new metaphors for the realities of the physical world which seem up for grabs in these less tangible regions.

4. Try to communicate to technically unsophisticated friends the extent to which their future freedoms depends on understanding digital communication.

5. If you are online, spread the word to local boards.

6. If you are at a school, inform interested people about the goals of the EFF.

7. Connect responsibly.

8. Work locally for an understanding of what the electronic frontier means in a global sense.

9. Learn and use the technology. Only by having an understanding of computers can one evaluate statements about computer *crime*.

10. Stop and think, about the many ways in which we rely on information in our lives, and what the effect might be if that information were distorted, corrupted, limited, or denied us.

11. Remember that words on a computer are SPEECH, protected by the Constitution.

12. Help your non-computerized friends see the potential of the net: search out a low airline fare for them, or send a fast cheap message to friends across the country.

13. Check to see if your local and state representatives understand the potential of electronic communication.

14. Reject techno-elitism and recognize that entry into the networking domain is a rite of passage and that someone else probably helped you with it.

15. Do your backups.

16. Educate your local librarians about electronic freedoms.

17. Welcome all interested participants.

18. Argue in a way that informs all the participants in the argument.

19. Develop better tools for linking people and networks.

20. Keep in touch with us. Pass on your thoughts, concerns, insights, contacts, and news.

CPSR Announces the First Conference on Computers, Freedom & Privacy

Tutorials & Invitational Conference, Limited to 600 Participants

About Computers, Freedom & Privacy —
We are at a crossroads, as individuals and organizations conduct more and more of their activity using computers and computer networks. By the end of the 1990s, most information will be collected, distributed and utilized electronically.

Thus far, an uncoordinated jumble of policies and procedures is rapidly developing as each group develops ways of collecting, manipulating, extracting, sharing and protecting information in its computers and exchanged on its networks.

Information on individuals and groups is being computerized by numerous organizations, agencies and special interests, often without the knowledge or approval of those it concerns.

Computerization can greatly assist individuals, organizations and government in making sound decisions based on efficient access to adequate information.

Or, it can seriously threaten the fundamental freedoms, personal privacy, and democratic processes that are at the very foundation of this nation.

More and more people are concerned about how organizations handle personal, family and lifestyle information about individuals. Many feel powerless to prevent private organizations and government from building, marketing and distributing confidential dossiers on them. Valuable information about government is increasingly computerized in government systems, but freedom of access to it in useful, computerized form by interested citizens, researchers and the press remains difficult and often prohibited.

Governments' regulation of national and international information exchange is increasing, often restricting it in the name of protecting competitiveness or confidentiality. There are increasing protests from business leaders unable to conduct effective business in a global economy.

Businesses are losing millions of dollars and thousands of work-hours, annually, to computerized mischief, vandalism, fraud and theft. Perpetrators are usually individuals abusing their authorized access.

Instances of computer misuse by young people raise special questions about the values that adults are practicing and passing along to these children.

Each year, new laws are proposed responding to the latest type of abuse or misuse of computers. Penalties applied to uncharged suspects and convicted computer criminals vary wildly from case to case, with little consistency relative to the seriousness of the alleged crime.

Law enforcement officials are using increasingly aggressive strategies and sophisticated countermeasures as they seek to serve and protect, vigorously applauded by some interest groups and increasingly criticized by others.

Diverse groups are often polarizing around narrow self-interests, rather than working together to assure responsible practices and equitable policies.

About this Conference —
This is an intensive, multi-disciplinary survey Conference for those concerned with computing, teleconferencing, electronic mail, computerized personal information, direct marketing information and government data — and those concerned with computer-related legislation, regulation, law enforcement and international policies that impact civil liberties, responsible exercise of freedom and protection of privacy in the global Information Age.

A maximum of 600 applicants will be invited to attend. Balanced representation from the diverse interest groups is being encouraged.

To inform participants about topics beyond their specialties, half-day and full-day seminars are scheduled for the first day (Monday, Mar. 25th). These parallel tutorials will explore relevant issues in computing, networking, civil liberties, the law and law enforcement. Each seminar is designed for those who are experienced in one area, but are less knowledgeable in some of the other disciplines.

To explore the issues and their interactions and ramifications, conference talks and panel discussions are scheduled for the remaining three days (Tuesday-Thursday, Mar. 26th-28th). These will emphasize balanced representation of all major views, with ample opportunity for probing questions and discussion.

The opening conference session on Tuesday will include major policy proposals by one of the nation's best known Constitutional scholars: Laurence H. Tribe, Professor of Constitutional Law, Harvard University Law School: "The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier"

The Tuesday evening session will feature a leading expert in the areas of telecommunications regulation, international telecomm policies and economics: Professor Eli M. Noam, Professor & Director Center for Telecommunications and Information Studies, Columbia University Graduate School of Business

Tuesday-Thursday Conference sessions offering diverse speakers & panel discussions include:

- Computers & Network Trends
- Personal Information & Privacy
- International Perspectives & Impacts
- Law Enforcement Practices & Problems
- Law Enforcement & Civil Liberties
- Legislation & Regulation
- Computer-Based Surveillance of Individuals
- Ethics & Education
- Electronic Speech, Press, & Assembly
- Access to Government Information
- Where Do We Go From Here?

The conference is sponsored by Computer Professionals for Social Responsibility–A nonprofit educational corporation. Telephone: (415)322-3778 Fax: (415) 851-2814 Conference e-mail: cfp@well.sf.ca.us

Co-sponsors & cooperating organizations include: Electronic Frontier Foundation, Electronic Networking Association Association for Computing Machinery, American Civil Liberties Union, ACM Special Interest Group on Software, Videotex Industry Association, IEEE-USA Intellectual Property Committee Cato Institute, IEEE-USA Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers-USA, ACM Committee on Scientific Freedom and Human Rights, ACM Special Interest Group on Computers and Society, The WELL, Autodesk, Inc., Portal Communications.

March 25-28, 1991, Monday-Thursday in the Bicentennial Year of the Bill of Rights

Airport Marriott Hotel, Burlingame, California on the San Francisco Peninsula, near San Francisco International Airport

Sponsored by: Computer Professionals for Social Responsibility –A nonprofit educational corporation

Chair: Jim Warren, Autodesk & MicroTimes, fax/415-851-2814, e-mail/jwarren@well.sf.ca.us

Request for Invitation
To facilitate useful dialogue and balanced participation by representatives from all of the diverse groups that are interested in these issues, this First Conference on Computers Freedom & Privacy (March 25-28, 1991) is limited to 600 invited participants (Conference facility capacity is also limited). All interested parties are encouraged to apply for an invitation. To receive information about the 50-60 speakers & panelists, the tutorials and an Invitation Application form, forward the following information to: e-mail/cfp@well.sf.ca.us -or- fax/(415)851-2814 -or- CFP Conference, 345 Swett Road, Woodside CA 94062

Name: _____
Title (if any): _____
Organization (if any): _____
Mailing address: _____
City/state/ZIP: _____
Phone number: _____
Alternate phone (if any): _____
Fax number (if any): _____
Electronic-mail address (if any): _____
Your particular interests (maximum of one page, please): _____

Plans and Actions:

Current EFF Activities

The Len Rose cases
The EFF legal department has been working to provide litigation support in the two criminal cases involving Baltimore computer consultant Len Rose. In the first case, we have been particularly active in helping develop the factual and legal issues in the case, and in locating and screening potential witnesses. We believe Baltimore case raises important issues concerning both the application of the federal Computer Fraud and Abuse statute (which we have challenged on the basis of unconstitutional overbreadth), the federal wire-fraud statute, and the federal Interstate Transportation of Stolen Property statute (which we believe should not be applied in cases of unauthorized copying of copyrighted software).

We have been providing similar support in Rose's state criminal case in Illinois. Among the issues in that case is whether the Illinois "computer tampering" statute is overbroad, and whether it in fact criminalizes the activity that Rose is alleged to have committed. In both cases, we have relied extensively on communications over the Net to initiate and maintain contact with potential witnesses.

The RIPCO BBS case
We have also been giving significant time to reviewing the warrant affidavits in the RIPCO BBS seizure. In addition, we have been reviewing the available archived files from that BBS to determine what, if any, justification there was for seizing the equipment.

We believe the RIPCO case potentially raises important issues about the valid scope of searches and seizures, the chilling effect of such seizures on First Amendment-protected speech and association, and the limits of sysop liability for the activities of third parties.

Other matters
We have continued our ongoing investigations of cases that raise issues that may be of EFF interest. In many of these cases we have chosen either not to become involved, or to wait until the cases reach a procedural stage (such as an appeal) at which it would become more appropriate for the Foundation to intervene.

The EFF phone line has become, to some extent, a "hotline" for people who are curious and/or worried about how their rights as citizens and as computer users may be threatened specifically or generally by government action. We have been in contact with people who were convicted of computer crimes before the EFF came into existence, and occasionally have been able to provide useful information to the lawyers handling appeals of these cases. We also have become a center for general information, with phone calls, mail, and e-mail every day requesting information about EFF and its work.

Two versions of the Massachusetts Computer Crime Bill have been introduced in the Massachusetts legislature, one of which is identical to the EFF bill which didn't pass last year. Mike, Sharon, and Mitch will all be working toward passage of the bill this year.

Conferences and Meetings
On December 19th John and Mitch spent half a day at Lawrence Livermore National Labs in Livermore, California at the invitation of the computer security management there. The trip was arranged by Russell Brand. We spoke to a large general audience of lab employees as well as had meetings with smaller groups of security experts concerned with security both at Lawrence Livermore and on the large Department of Energy computer network generally.

John and Mitch also appeared on a panel at Mac World at the Moscone Center on Friday, January 11th, which was chaired by Jim Warren. Also appearing was Alameda Country District Attorney Don Ingraham. John spoke in Los Angeles at a combined SIGGRAPH and ACM meeting in early January.

Compuserve
Scott Loftesness, who is a Well member, EFF supporter, and Compuserve veteran is about to open a Telecommunications forum on Compuserve which will feature an EFF sub-forum. Library materials from the Well have already been ported over. We will announce this in the EFF conference on the Well and encourage people to seed the Compuserve forum with their participation to help it get off to a good start.

EFFECTOR

The Electronic Frontier Foundation, Inc.
155 Second Street Cambridge, MA 02141

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

Contact

How to get in touch with the EFF:

Via Computer Networks:
Send requests to be added to or dropped from the EFF mailing list or other general correspondence to eff-request@well.sf.ca.us. We will periodically mail updates on EFF-related activities to this list.

If you receive USENET newsgroups, your site may carry two new newsgroups in the INET called comp.org.eff.news and comp.org.eff.talk. The former is a moderated newsgroup of announcements, responses to announcements, and selected discussion drawn from the unmoderated "talk" group and the mailing list.

Everything that goes out over the EFF mailing list will also be posted in comp.org.eff.news, so if you read the newsgroup you don't need to subscribe

Postings submitted to the moderated newsgroup may be reprinted by the EFF. To submit a posting, you may send mail to eff@well.sf.ca.us

There is an active EFF conference on the Well, as well as many other related conferences of interest to EFF supporters. As of August 1990, access to the Well is $8/month plus $3/hour. Outside the S.F. Bay area, telecom access for $5/hr. is available through CPN. Register online at (415) 332-6106.

A document library containing all of the EFF news releases, John Barlow's "Crime and Puzzlement" and others is available on the Well. We are working toward providing FTP availability into the document library through an EFF host system to be set up in Cambridge, Mass. Details will be forthcoming.

Via Mail or Telephone:
The Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141
Telephone: (617) 864-0665
Fax: (617) 864-0866

rec. 5/16/91

EFF

Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141
Phone: (617) 864-0665
FAX: (617) 864-0866
Internet address:
eff@well.sf.ca.us

8 May 1991

Evelyn Pine
Executive Director
Community Memory
2617 San Pablo Avenue
Berkeley, CA 94702

Dear Ms. Pine,

Mr. Kapor has asked me to convey his regrets that the EFF can not, at this time, participate in the support of Community Memory. While we admire all systems like CM, and are acutely aware of the role of open access systems, the changing nature of EFF has caused us to curtail all grants to outside projects for the foreseeable future.

At its inception, it is true that EFF made a number of grants to various organizations that it felt were both worthy and within the charter of the EFF at that time. Currently, however, we are becoming more involved in direct advocacy . As a result, our commitments to ongoing projects and future actions are making strong demands on our budget.

I hope you will understand our position, and that this necessity does not ultimately hamper Community Memory.

All the best,

Gerard Van der Leun
Director of Communications/ EFF
GV/si

cc: M. Kapor

June 12, 1991

Gerard Van der Leun
Director of Communications
Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141

Dear Mr. Van der Leun:

Thank you for your kind letter regarding the Community Memory Project.

Of course, we appreciate the Electronic Frontier Foundation's efforts in direct advocacy. However, we also believe that support for projects which demonstrate the potential of these networks -- particulary to constituencies who are cut out of the debate -- is crucial to the development of a regulatory and legal framework that doesn't merely benefit those who already have access to mass communications.

As organizations that understand what's at stake in the development of telecommunications policy, we bear a special responsibility. Because these issues are so new and complex, the resources directed toward them are limited. The Electronic Frontier Foundation is unique, in our experience, in its ability to garner resources and energy to the exploration of these crucial issues. If there are other organizations that support projects that take on the practical realities of electronic freedom, please let us know.

Because we are allies with a shared mission, we look forward to working with the Electronic Frontier Foundation to shape a future in which communications tools allow individuals and communities to forge new ways of living and being which serve the common good.

Of course, I'll be delighted to keep you updated on the Community Memory Project's progress.

Best wishes,

Evelyn Pine
Executive Director

Village Design

P.O. Box 996
Berkeley, CA. 94701

EFFECTOR

Effector – The Newsletter of the Electronic Frontier Foundation

March 1991
Volume 1 Number 1

Goals of the EFF

1. To engage in and support educational activities that increase the popular understanding of the opportunities and challenges posed by computing and telecommunications.

2. To develop among policy-makers a clearer comprehension of the issues underlying free and open telecommunications.

3. To support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.

4. To raise public awareness about civil-liberties issues arising from rapid advances in computer-based communications media.

5. To support litigation in the public interest to preserve, protect, and extend Constitutional rights to the realm of computing and telecommunications technology.

6. To encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

A Man From the FBI:

The Origins of the Electronic Frontier Foundation

By John Perry Barlow

The Electronic Frontier Foundation was started by a visit from the FBI.

In late April of 1990, I got a call from Special Agent Richard Baxter of the Federal Bureau of Investigation. He asked if he could come by the next day and discuss a certain investigation with me. His unwillingness to discuss its nature over the phone left me with a sense of global guilt, but I figured turning him down would probably send the wrong signal.

On Mayday, he drove to Pinedale, Wyoming, a cow town 100 miles north of his Rock Springs office (where he ordinarily investigates livestock theft and other regional crimes). He brought with him a thick stack of documents from the San Francisco office and a profound confusion about their contents.

He had been sent to find out if I might be a member of the NuPrometheus League, a dread band of info-terrorists (or maybe just a disaffected former Apple employee) who had stolen and wantonly distributed source code normally used in the Macintosh ROMs. Agent Baxter's errand was complicated by a fairly complete unfamiliarity with computer technology. I realized right away that before I could demonstrate my innocence, I would first have to explain to him what guilt might be.

The three hours I passed doing this were surreal for both of us. Whatever this source code stuff was, and whatever it was that happened to it, had none of the cozy familiarity of a few yearling steers headed across the Wyoming border in the wrong stock truck.

What little he did know, thanks to the San Francisco office, was also pretty well out of kilter. He had been told, for example, that Autodesk, the publisher of AutoCAD, was a major Star Wars defense contractor and that its CEO was none other than John Draper, the infamous phone phreak also known as Cap'n Crunch. As soon as I quit laughing, I started to worry.

I realized in the course of this interview that I was seeing, in microcosm, the entire law enforcement structure of the United States. Agent Baxter was hardly alone in his puzzlement about the legal, technical, and metaphorical nature of datacrime.

I also found in his struggles a framework for understanding a series of recent Secret Service raids on some young hackers I'd met in a Harper's magazine forum on computers and freedom. And it occurred to me that this might be the beginning of a great paroxysm of governmental confusion during which everyone's liberties would become at risk.

When Agent Baxter had gone, I wrote an account of his visit and placed it on the WELL, a computer BBS in Sausalito which is digital home to a large collection of technically hip folks, including Mitch Kapor, the father of Lotus 1-2-3.

Turns out Mitch had also been visited by the FBI, owing to his having unaccountably received of one of the source code disks which NuPrometheus scattered around. Mitch's experience had been as dreamlike as mine. He had, in fact, filed the whole thing under General Inexplicability until he read my tale on the WELL. Now he had enough corroboration for his own strange sense of alarm to begin acting on it.

Several days later, he found his bizjet about to fly over Wyoming on its way to San Francisco. He called me from somewhere over South Dakota and asked if he might literally drop in for a chat about Agent Baxter and related matters.

So, while a late spring snow storm swirled outside my office, we spent several hours hatching what became the Electronic Frontier Foundation. I told him about the sweep of Secret Service raids that had taken place months before and their apparent disregard for the Bill of Rights.

Alarmed, he gave me the phone number of Harvey Silverglate, whose willingness to champion unpopular causes was demonstrated by his current defense of Leona Helmsley. He said that Harvey would probably know if this were as bad as it was starting to sound. He also said that he would be willing to pay the bills that generally start to appear whenever you call a lawyer.

I finally found Harvey in the New York offices of Rabinowitz, Boudin, Standard, Krinsky and Lieberman, a firm whose long list of successfully defended civil-liberties cases includes the Pentagon Papers case. I told him and Eric Lieberman what I knew about recent government flailings against cybercrime. They were even less sanguine than I had been.

The next day a trio code-named Acid Phreak, Phiber Optik, and Scorpion entered the walnut-panelled chambers of Rabinowitz, Boudin and told their tales to a lawyer there named Terry Gross. While EFF as a formal organization would not exist for two months, its legal arm was already flexing its muscle.

A few days later I received a phone call from the technology writer for the Washington Post. He was interested in following up on the Harper's forum, and knew nothing of Mitch's and my joint endeavors. I filled him in, hoping to expose the Secret Service. Several days later, the Post published the first of many newspaper stories, all of which could have shared the headline: "Lotus Founder Defends Hackers."

continued page 2

Why Defend Hackers?

By Mitchell Kapor

An all-too-common perception of the EFF that prevails in the computer industry and those who report on it—from John Sculley to the Wall Street Journal—is that the EFF is an organization that has "something to do with hackers." (They use "hackers" as a term not of approbation but of rebuke). Most of these sometime colleagues and associates of mine are puzzled as to why I would be doing such a thing. (A few think I've just become a loony.) Anyway, they've heard about the terrible problems caused by hackers who break into computer systems, they worry that I'm out to defend such practices, and they disapprove.

But their disapproval is based on the pure misconception that the EFF's purpose is to defend people's right to break into computer systems. Let me clear up that misconception now.

I regard unauthorized entry into computer systems as wrong and deserving of punishment. People who break into computer systems and cause harm should be held accountable for their actions. We need to make appropriate distinctions in the legal code among various forms of computer crime, based on such factors as intent and the degree of actual damage. In fact, the EFF has drafted a bill that has the backing

continued page 3

Washington Watch

by Marc Rotenberg

• *Computer Crime Legislation*

Several proposals to expand computer crime law were introduced in the past Congress. In the end, a modest proposal, introduced by Senator Leahy, passed the Senate but did not make it through the House. Senator Leahy's bill would have penalized reckless computer acts that place computer systems at risk and would have required that the Justice Department report annually to Congress on computer crime prosecutions

• *National ID Card*

A proposal to begin a national ID card pilot project, tucked into amendments to the Immigration Control and Reform Act, was knocked out when civil libertarians objected.

• *Electronic Dissemination Policy*

A proposal to establish principles for the dissemination of electronic information by the federal agencies narrowly failed to pass the Congress as last minute negotiations on a related measure collapsed. The proposal grows out of a report from the Office of Technology Assessment "Informing the Nation" that stressed the need to develop new information policy to promote the development of CD-ROMs and on-line information services.

• *Caller ID*

A bill to allow the offering of Caller ID by regional phone companies if a per-call blocking feature is also provided failed to gather support this past Congress. Several states have already adopted similar measures.

• *Computer Security Policy*

The Presidential directive on computer security policy was revised finally to comply with the Computer Security Act of 1987. The Act reestablished control for computer security at a civilian agency — the National Institute for Standards and Technology — after the previous administration attempted to place computer security authority at the National Security Agency.

• *Upcoming Policy*

CPSR hosted the first Computing and Civil Liberties policy roundtable on February 21 and 22, 1991 at the American Association for the Advancement of Science in Washington, DC. The purpose of the roundtable was to bring together leading experts to explore two issues: free speech and computer networks, and searches of computer bulletin boards. What speech restrictions currently exist? Should federal agencies or private companies be allowed to restrict the content of a computer message and, if so, in what circumstances? The second issue was the investigation of computer bulletin boards by law enforcement agents. Are there any restrictions on the ways that police may monitor computer communications and computer bulletin boards? If not, should such restrictions be developed? The conference was the first in a series of policy roundtables that will be held in Washington, DC and that are made possible with funding from the Electronic Frontier Foundation.

EFFECTOR

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

The Board of the Electronic Frontier Foundation:
Mitchell Kapor, John Barlow, John Gilmore, Stewart Brand, Steve Wozniak
Staff Counsel: Mike Godwin
Staff Volunteer: Leila Gallagher

EFFECTOR was edited and produced by Gerard Van der Leun

Art Direction and design by Lisa DeFrancis, DeFrancis Studio, 80 Trowbridge Street, Cambridge, MA 02138

FBI *continued*

While this was an irritating misrepresentation, we were more interested in defending the Constitution than digital miscreants, the publicity produced a couple of major supporters: Steve Wozniak, who called and offered an unlimited match to Mitch's contributions, and John Gilmore (Sun Microsystems employee #5) who e-mailed me a six figure offer of support.

Operation Sundevil

Meanwhile, the list of apparent outrages lengthened. We learned about an Austin role-playing games publisher named Steve Jackson whose office equipment had been confiscated by the Secret Service in an apparent effort to restrain his publication of a game called Cyberpunk which they thought, with ludicrous inaccuracy, to be "a handbook for computer crime."

All over the country computer bulletin boards were being confiscated, undelivered e-mail and all. A Secret Service dragnet called Operation Sundevil seized more than 40 computers and 23,000 data disks from teenagers in 14 American cities, using levels of force and terror which would have been more appropriate to the apprehension of urban guerrillas than barely post-pubescent computer nerds.

And there was the Craig Neidorf case. Neidorf, also known by the nom de crack Knight Lightning, had published an internal BellSouth document in his electronic magazine Phrack. For this constitutionally protected act, Neidorf was being charged with interstate transport of stolen property with a possible sentence of 60 years in jail and a $122,000 in fines.

I wrote a piece about these events called "Crime & Puzzlement." I did so at the request of the Whole Earth Review—it made its first print appearance in the Fall 1990 issue of WER—but I "published" it on the Net in June and was astonished by the response. It was like planting a fence-post and discovering that the ground into which you've driven it is actually the back of a giant animal that quivers and heaves at the irritation.

By July, I was receiving up to 100 e-mail messages a day. They came from all over the planet and expressed nearly universal indignation. I began to experience datashock, but I also realized that Mitch and I were not alone in our concerns. We had struck a chord.

The Law in Cyberspace

In Cambridge, Mitch was having something like the same experience. Since the Washington Post story, he found himself bathed in media glare. However, the more he learned about ambiguous nature of law in Cyberspace, the more of his considerable intellectual and financial resources he became willing to devote to the subject.

In late June, Mitch and I threw several dinners in San Francisco, to which we invited major figures from the computer industry. We weren't surprised to learn than many of them had exploits in their past which, undertaken today, would arouse plenty of Secret Service interest. It appeared possible that one side-effect of current government practices might be the elimination of the next generation of computer entrepreneurs and digital designers.

It also became clear that we were dealing with a set of problems which was a great deal more complex and far-reaching than a few cases of governmental confusion. The actions of the FBI and Secret Service were symptoms of a growing social crisis: Future Shock. America was entering the Information Age with neither laws nor metaphors for the appropriate protection and conveyance of information itself.

We realized that our legal actions on behalf of a few teen-age crackers would go on indefinitely without much result unless something were done to ease social tensions along the electronic frontier. The real task at hand was the civilization of Cyberspace. Such an undertaking would require more juice and stamina than two men could muster, even amplified by the Net and a solid financial supply. We would need some kind of organizational identity.

With this in mind, we hired a press coordinator, Cathy Cook (who had formerly done PR for Steve Jobs), set a squad of lawyers to work on investigating the proper organizational tax status, and, over a San Francisco dinner with Stewart Brand, Nat Goldhaber, Jaron Lanier, and Chuck Blanchard, we selected a name and defined a mission.

Founding the Foundation

We announced the formation of the Electronic Frontier Foundation at the National Press Club on July 10. Mitch and I were joined for the announcement by Harvey Silverglate, Terry Gross, and Steve Jackson.

We were also joined by Marc Rotenberg of the Washington office of Computer Professionals for Social Responsibility. One of our first official acts had been to grant that organization $275,000 for a project on computing and civil liberties. CPSR would keep a wary eye on developments "inside the Beltway" and work in conjunction with congressional staffers to see that any legislation dealing with access to information was sensibly drafted.

While in Washington, we also took inventory of the terrain, meeting with congressional staffers, the Washington civil liberties establishment, and officials from the Library of Congress and the White House. The area to be covered, from intellectual property to telecommunications policy to law enforcement technique, was daunting, as were the ambient levels of confusion and indifference.

We also generated an enormous amount of press. And it became apparent that not everyone was persuaded of our cause. Business Week called Mitch naive for his willingness to believe that computer crackers were somehow less dangerous that drug kingpins. Various burghers of the computer establishment, ranging from the executive director of the Software Publishers Association to a columnist for ComputerWorld, called us fools at best and, more likely, dangerous fools.

The Wall Street Journal printed a particularly hysterical piece which alleged that the document Craig Neidorf (into whose case we had entered a supporting amicus brief) had published was a computer virus capable of bringing down the emergency phone system for the entire country. In fact, the text file which Neidorf distributed dealt with the bureaucratic procedures of 911 administration in the Bell-South region and contained nothing which could be used to crack a system. Indeed, it contained nothing which could not be easily obtained through by legal means.

Neidorf's first major break came in late July. Thanks in part to the independent work of John Nagel, who was prepared to testify that the prosecutors had seriously overstated the value of the E911 document, the government was forced to abandon its case against Neidorf after 4 days in Chicago's Federal Court.

Although our briefs supporting Neidorf's activities under the First Amendment were not admitted, it became apparent, before such loftier matters could even be broached, that the government had indicted him with no clear understanding of the purpose or availability of the document he had distributed. Like Agent Baxter, they knew too little to critically examine the misinformation they had been given by the corporate masters, in this case, officials at Bellcore.

Following the resolution of the Neidorf case, and, to some extent because of it, skepticism of EFF has moderated considerably. If anything, the most recent press accounts of our activities have been almost fulsome in their praise. Recent favorable coverage has appeared in the New York Times, The Economist, Infoworld, Information Week, PCweek, and Boston Magazine.

Since July, we have been absurdly busy on numerous fronts: We've worked on raising public awareness of the issues at stake. We are organizing legal responses to the original and continuing intemperance of law enforcement. We have worked on the political front, developing and lobbying for rational computer security legislation. We have started to create a network of interested experts on computer security, intellectual property, telecommunications policy, and international information rights. And lately we've been attending to the organizational demands of the non-profit equivalent of a hyper-successful computer startup.

The Expanding Mission

When we first defined the mission of the Electronic Frontier Foundation, we saw our task as assuring the application of the U.S. Constitution to digital media. And this remains much of what we are about.

However, information has little natural regard for national borders or local ordinances. Cyberspace is transnational. During the tsunami of e-mail which Crime & Puzzlement elicited, there were many items from foreign countries. Their authors wanted to know how they could protect or establish their rights of free expression. And I had no idea what to tell them.

The question arose again at Esther Dyson's recent East-West Technology Conference in Budapest which Mitch and I attended. EFF was well-known among the Soviets at this meeting, some of whom were already involved in drafting what they called an Information Bill of Rights. (One young Moscow programmer had managed to hack together an Internet connection through Finland in order to contact me.)

Like intellectual property and telecom policy, the development of international principles of free digital speech is a large angel to wrestle with. We will have to be careful not to allow this immense task to divert EFF from its specific legal agenda. But neither can we ignore the fact that Cyberspace is hardly an American territory.

The Electronic Frontier Foundation grew from an effort to fight a specific legal brushfire into a full-fledged Cause much faster than we could have imagined. And, like any explosive start-up, it spends a lot of time playing catch-up.

Reaching Out

Electronically amplified, Mitch and I were able to personally conduct much of EFF's business in the first few months of operations. But gradually we had to confront the fact that while the Net is very broad, it is also quite shallow. Without even a sense of their physical location, we have been unable to marshal the hundreds of people who have e-mailed us with their volunteered services. Also, we found ourselves administering a significant cash-flow in both donations and expenditures. (By year's end, EFF will have spent around $220,000. Our tentative 1991 budget predicts expenses of almost half a million.)

So, despite a mutual terror of bureaucracy and organizational sclerosis, we have started to adopt some institutional trappings.

First, in order to satisfy the requirements for a 501c3 tax status (which we should have in about six months), we found that we needed something more substantial than two guys with modems. Thus, on October 9, we held our first official board meeting and formally elected Stewart Brand, Steve Wozniak, and John Gilmore to join us as board members.

And we have started to take on staff. We recently hired Mike Godwin, a freshly minted Texas lawyer and USENET adept, to sort through the factual and legal details of the many cases we are being asked to intervene in. In his short time with us, he has investigated several cases to determine their fit with EFF's constitutional mission, their winnability, and their likelihood of producing clear legal precedent.

We are determined that EFF will remain an agile, swift-moving sort of outfit. We will adopt any new bureaucratic manifestations with the greatest skepticism. But we are being bombarded with many legitimate requests for assistance, advice, and information. In order to respond rapidly and appropriately, the Electronic Frontier Foundation has had to become an institution. One method by which we hope to maintain organizational lightness involves keeping a clear distinction between strategy and tactics.

On the strategic level, EFF has a very broad mission involving such amorphous endeavors as defining intellectual property, helping establish a transnational culture of information, designing telecommunications policy, sponsoring humane software design... civilizing Cyberspace. With an appropriate sense of their limitations, the board members will remain responsible for these matters.

This will prevent the staff's losing tactical focus on more tangible action items like litigation, political action, communicating through the press and across the Net, and organizational care and feeding.

The problem with history is that it keeps happening. Today, as I was working on this EFF mini-biography, I learned that Mitch has just had his fingerprints subpoenaed by the FBI. Turns out they are now examining the NuPrometheus distribution disks for fingerprints and want to be able to sort his out. Or, perhaps, search for their appearance on other disks...

So the Wheels of Justice grind blindly on. And we will go on trying to prevent anyone's being ground up in them.

Postcard from the Edge

"I went on to test the program in every way I could devise. I strained it to expose its weaknesses. I ran it for high-mass stars and low-mass stars, for stars born exceedingly hot and those born relatively cold. I ran it assuming the superfluid currents beneath the crust to be absent — not because I wanted to know the answer, but because I had developed an intuitive feel for the answer in this particular case. Finally I got a run in which the computer showed the pulsar's temperature to be less than absolute zero. I had found an error. I chased down the error and fixed it. Now I had improved the program to the point where it would not run at all."

George Greenstein,
"Frozen Star: Of Pulsars, Black Holes and the Fate of Stars"

How Prosecutors Misrepresented the Atlanta Hackers

Reading Between the Lines of the BellSouth Sentences

By Mike Godwin

Although the Electronic Frontier Foundation is opposed to unauthorized computer entry, we are deeply disturbed by the recent sentencing of Bell South hackers/crackers Riggs, Darden, and Grant. Not only are the sentences disproportionate to the nature of the offenses these young men committed, but, to the extent the judge's sentence was based on the prosecution's sentencing memorandum, it relied on a document filled with misrepresentations.

Robert J. Riggs, Franklin E. Darden, Jr., and Adam E. Grant were sentenced Friday, November 16, in federal court in Atlanta. Darden and Riggs had each pled guilty to a conspiracy to commit computer fraud, wire fraud, access-code fraud, and interstate transportation of stolen property. Grant had pled guilty to a separate count of possession of access codes with intent to defraud.

All received prison terms; Grant and Darden, according to a Department of Justice news release, "each received a sentence of 14 months incarceration (7 in a halfway house) with restitution payments of $233,000." Riggs, said the release, "received a sentence of 21 months incarceration and $233,000 in restitution." In addition, each is forbidden to use a computer, except insofar as such use may be related to employment, during his post-incarceration supervision.

The facts of the case, as related by the prosecution in its sentencing memorandum, indicate that the defendants gained free telephone service and unauthorized access to BellSouth computers, primarily in order to gain knowledge about the phone system. Damage to the systems was either minimal or nonexistent. Although it is well-documented that the typical motivation of phone-system hackers is curiosity and the desire to master complex systems, the prosecution attempts to characterize the crackers as major criminals, and misrepresents facts in doing so.

Examples of such misrepresentation include:

1. Misrepresenting the E911 file.

The E911 file, an administrative document, was copied by Robert Riggs and eventually published by Craig Neidorf in the electronic magazine PHRACK. Says the prosecution: "This file, which is the subject of the Chicago [Craig Neidorf] indictment, is noteworthy because it contains the program for the emergency 911 dialing system. As the Court knows, any damage to that very sensitive system could result in a dangerous breakdown in police, fire, and ambulance services. The evidence indicates that Riggs stole the E911 program from BellSouth's centralized automation system (i.e., free run of the system). Bob Kibler of BellSouth Security estimates the value of the E911 file, based on R&D costs, is $24,639.05."

This statement by prosecutors is clearly false. Defense witnesses in the Neidorf case were prepared to testify that the E911 document was not a program, that it could not be used to disrupt 911 service, and that the same information could be ordered from Bell South at a cost of less than $20. Under cross-examination, the prosecution's own witnesses admitted that the information in the E911 file was available in public documents, that the notice placed on the document stating that it was proprietary was placed on all Bell South documents (without any prior review to determine whether the notice was proper), and that the document did not pose a danger to the functioning of the 911 system.

2. Guilt by association.

The prosecution begins its memorandum by detailing two crimes: 1) a plot to plant "logic bombs" that would disrupt phone service in several states, and 2) a prank involving the rerouting of calls from a probation office in Florida to "a New York Dial-A-Porn number."

Only after going to some length describing these two allegations does the prosecution state, in passing, that *the defendants were not implicated in these crimes.*

Elsewhere in the memorandum, the prosecution attempts to suggest the defendants' responsibility in a third offense—another person's crime. Because the defendants "freely and recklessly disseminated access information they had stolen," says the memorandum, a 15-year-old hacker committed $10,000 in electronic theft. Even though the prosecution does not say the defendants intended to facilitate that 15-year-old's alleged theft, the memorandum seeks to implicate the defendants in that theft.

3. Guilt by knowing too much.

The prosecution goes to great lengths describing the crimes the defendants *could* have committed with the kind of knowledge they had gathered: "During the course of the conspiracy, the defendants and other LOD [Legion of Doom] members illegally amassed enough knowledge about the telecommunications computer systems to jeopardize the entire telephone industry!"

The prosecution does not mention, however, that the mere possession of dangerous knowledge is not a crime, nor does it state, explicitly, that the defendants never conspired to cause such damage to the phone system.

4. Misrepresentation of motives.

As noted above, it has been documented that young phone-system hackers are typically motivated by the desire to understand and master large systems, not to inflict harm or to enrich themselves materially. Although the prosecution concedes that "[d]efendants claimed that they never personally profited from their hacking activities, with the exception of getting unauthorized long distance and data network service," the prosecutors nevertheless characterize the hackers' motives as similar to those of extortionists: "Their main motivation [was to] obtain power through information and intimidation."

5. Failure to acknowledge the outcome of the Craig Neidorf case.

In evaluating defendants' cooperation in the prosecution of Craig Neidorf, the government singles out Riggs as being less helpful than the other two defendants, and recommends less leniency because of this. Says the memorandum: "The testimony was somewhat helpful, though the prosecutors felt defendant Riggs was holding back and not being as open as he had been in the earlier meeting." The memorandum fails to mention, however, that Riggs's testimony tended to support Neidorf's defense that he had never conspired with Riggs to engage in the interstate transportation of stolen property or that the case against Neidorf was dropped.

Perhaps the most egregious aspect of the governments's memorandum is the argument that Riggs, Grant, and Darden should be imprisoned, not for what *they* have done, but to send the right "message to the hacking community." The government focuses on the case of Robert J. Morris Jr., the computer-science graduate student who was sentenced to a term of probation in May of this year for his release of the worm program that disrupted many computers connected to the Internet. Urging the court to imprison the three defendants, the government remarked that "hackers and computer experts recall general hacker jubilation when the judge imposed a probated sentence. Clearly, the sentence had little effect on defendants Grant, Riggs, and Darden."

The government's criticism is particularly unfair in light of the fact that the Morris sentencing took place almost a year *after* the activities leading to the defendants' convictions!

The memorandum raises other questions besides those of the prosecutors' biased presentation of the facts. The most significant of these is the government's uncritical acceptance of BellSouth's statement of the damage the defendants did to its computer system. The memorandum states that "In all, [the defendants] stole approximately $233,880 worth of logins/passwords and connect addresses (i.e., access information) from BellSouth. BellSouth spent approximately $1.5 million in identifying the intruders into their system and has since then spent roughly $3 million more to further secure their network."

It is unclear how these figures were derived. For one thing, the stated cost of the passwords is highly questionable: What is the dollar value of a password?

And it's similarly unclear that the defendants caused BellSouth to spend $4.5 million more than they normally would have spent in a similar period to identify intruders and secure their network. Although the government's memorandum states that "[t]he defendants ... have literally caused BellSouth millions of dollars in expenses by their actions," the actual facts as presented in the memorandum suggest that BellSouth had already embarked upon the expenditure of millions of dollars *before* it had heard anything about the crimes the defendants ultimately were alleged to have committed.

Not only are there questions about the justice of the restitution requirement in the sentencing of Riggs, Darden, and Grant, but there also are Constitutional issues raised by the prohibition of access to computers. The Court's sentencing suggests a belief that anything the defendants do with computers is likely to be illegal; it ignores the fact that computers are a communications medium, and that the prohibition *goes* beyond preventing future crimes by the defendants—it treads upon their rights to engage in lawful speech and association.

EFF does not support the proposition that computer intrusion and long-distance theft should go unpunished. But we find highly disturbing the misrepresentations of facts in the prosecutors' sentencing memorandum as they seek disproportionate sentences for Riggs, Darden, and Grant—stiff sentences that supposedly will "send a message" to the hackers and crackers.

The message this memorandum really sends is that the government's presentation of the facts of this case has been heavily biased by its eagerness to appear to be deterring future computer crime.

Why Defend Hackers *continued*

of the Governor and Attorney General of Massachusetts and that embodies these principles.

But if the EFF isn't trying to advance the cause of computer hackers, you may ask, what is it doing and why? What is it that was sufficiently powerful to motivate me to help start a whole organization?

As I began to find out the real story behind government raids and indictments last summer, I became incensed at the fact that innocent individuals were getting caught up in the blundering machinations of certain law enforcement agencies and large corporations. These were kids really, young people with whom I identified, who faced the prospect of having their lives ruined.

Take Craig Neidorf for example. Neidorf, a defendant in one case and the publisher of an electronic newsletter, was indicted on felony charges of wire fraud and interstate transportation of stolen property. Neidorf had published a document about administrative procedures used in the 911 emergency response telephone system that someone else had removed from a BellSouth computer. On the fourth day of the trial, the prosecution dropped the case after it became clear that the information in the "highly confidential" BellSouth document at issue was publicly available for less than $20.

Justice was served by the government's decision to drop the case, but it was expensive justice. Neidorf and his family face $100,000 in legal bills, to say nothing of the disruption and suffering caused by the trial for an action that should never have been brought against him to begin with.

In a second case, the EFF continues to assist Steve Jackson, a game manufacturer in Austin, Texas, who has suffered substantial business losses after a Secret Service raid in early March. The seizure of Jackson's computer equipment caused him to lay off nearly half of his staff and threatened the survival of the business. As subsequent revelations have showed, there was no good reason for this raid. It never should have been permitted to occur in the first place.

While helping defend the innocent is one role for the EFF to play, there is more at stake than trying to prevent individuals from being wronged. It is also a matter of rights for all of us.

The legal protections afforded Craig Neidorf's electronic newsletter and its publisher and the computer bulletin board system (BBS) seized in the Steve Jackson raid are neither clear nor well-established. I believe it is terribly important to extend to these new digital media the same strong First Amendment protections of freedom of speech and freedom of expression which we enjoy in our own lives and in the print media. The government should not be able to seize a BBS any more easily than they can seize a printing press. We must find ways for law enforcement to do its job in protecting the property of some of us without violating the freedom of speech of the rest of us. This is clearly a matter of protecting civil liberties and familiar to those who take an interest in upholding the Bill of Rights, but it is also more than that.

These embryonic media of electronic mail, BBSs, and conferencing systems, provide open forums of communication. They are an antidote to the corrosive effects of the power of large, centralized institutions, private and public, and to the numbness induced by one-way, least-common-denominator mass media.

In the global suburbs in which more and more of us live, one's horizon is limited to the immediate family. Even close neighbors are often anonymous.

In the realities that can be created within digital media there are opportunities for the formation of virtual communities—voluntary groups who come together not on the basis of geographical proximity but through a common interests. Computer and telecommunications systems represent an enabling technology for the formation of community, but only if we make it so. I believe it is urgent, as a matter of national policy, that we encourage and further stimulate the social experiments and developing infrastructure that are taking place on the Net every day. The ultimate mission of the EFF is to help articulate this vision and play a constructive role in the working out of the new legal and social norms which we are faced with developing.

As John Barlow and I meditated together last June on the broader implications of the initial events—a meditation that catalyzed the formation of the EFF—we could see that what was at stake was not merely seeing justice be served in the case of a few individuals, nor simply the preservation of the civil liberties of all of us, although these goals are vitally important.

The larger issue is how our society will come to terms with the onrush of transformative technology. If we take the right steps now—and EFF is working to take those steps—new and increasing access to information technology will enhance rather than inhibit the positive growth and development of individuals, of communities, and of society as a whole.

20 Things You Can Do to Advance Electronic Freedom

1. **Spread the word about EFF as widely as possible, both on and off the Net.**
2. **Be alert for any local, state or national legislation that effect electronic freedom.**
3. **Put the immense processing horsepower of your mind to the task of finding new metaphors for the realities of the physical world which seem up for grabs in these less tangible regions.**
4. **Try to communicate to technically unsophisticated friends the extent to which their future freedoms depends on understanding digital communication.**
5. **If you are online, spread the word to local boards.**
6. **If you are at a school, inform interested people about the goals of the EFF.**
7. **Connect responsibly.**
8. **Work locally for an understanding of what the electronic frontier means in a global sense.**
9. **Learn and use the technology. Only by having an understanding of computers can one evaluate statements about computer crime.**
10. **Stop and think, about the many ways in which we rely on information in our lives, and what the effect might be if that information were distorted, corrupted, limited, or denied us.**
11. **Remember that words on a computer are SPEECH, protected by the Constitution.**
12. **Help your non-computerized friends see the potential of the net: search out a low airline fare for them, or send a fast cheap message to friends across the country.**
13. **Check to see if your local and state representatives understand the potential of electronic communication.**
14. **Reject techno-elitism and recognize that entry into the networking domain is a rite of passage and that someone else probably helped you with it.**
15. **Do your backups.**
16. **Educate your local librarians about electronic freedoms.**
17. **Welcome all interested participants.**
18. **Argue in a way that informs all the participants in the argument.**
19. **Develop better tools for linking people and networks.**
20. **Keep in touch with us. Pass on your thoughts, concerns, insights, contacts, and news.**

CPSR Announces the First Conference on Computers, Freedom & Privacy

Tutorials & Invitational Conference, Limited to 600 Participants

About Computers, Freedom & Privacy —

We are at a crossroads, as individuals and organizations conduct more and more of their activity using computers and computer networks. By the end of the 1990s, most information will be collected, distributed and utilized electronically.

Thus far, an uncoordinated jumble of policies and procedures is rapidly developing as each group develops ways of collecting, manipulating, extracting, sharing and protecting information in its computers and exchanged on its networks.

Information on individuals and groups is being computerized by numerous organizations, agencies and special interests, often without the knowledge or approval of those it concerns.

Computerization can greatly assist individuals, organizations and government in making sound decisions based on efficient access to adequate information.

Or, it can seriously threaten the fundamental freedoms, personal privacy, and democratic processes that are at the very foundation of this nation.

More and more people are concerned about how organizations handle personal, family and lifestyle information about individuals. Many feel powerless to prevent private organizations and government from building, marketing and distributing confidential dossiers on them. Valuable information about government is increasingly computerized in government systems, but freedom of access to it in useful, computerized form by interested citizens, researchers and the press remains difficult and often prohibited.

Governments' regulation of national and international information exchange is increasing, often restricting it in the name of protecting competitiveness or confidentiality. There are increasing protests from business leaders unable to conduct effective business in a global economy.

Businesses are losing millions of dollars and thousands of workhours, annually, to computerized mischief, vandalism, fraud and theft. Perpetrators are usually individuals abusing their authorized access.

Instances of computer misuse by young people raise special questions about the values that adults are practicing and passing along to these children.

Each year, new laws are proposed responding to the latest type of abuse or misuse of computers. Penalties applied to uncharged suspects and convicted computer criminals vary wildly from case to case, with little consistency relative to the seriousness of the alleged crime.

Law enforcement officials are using increasingly aggressive strategies and sophisticated countermeasures as they seek to serve and protect, vigorously applauded by some interest groups and increasingly criticized by others.

Diverse groups are often polarizing around narrow self-interests, rather than working together to assure responsible practices and equitable policies.

About this Conference —

This is an intensive, multi-disciplinary survey Conference for those concerned with computing, teleconferencing, electronic mail, computerized personal information, direct marketing information and government data — and those concerned with computer-related legislation, regulation, law enforcement and international policies that impact civil liberties, responsible exercise of freedom and protection of privacy in the global Information Age.

A maximum of 600 applicants will be invited to attend. Balanced representation from the diverse interest groups is being encouraged.

To inform participants about topics beyond their specialties, half-day and full-day seminars are scheduled for the first day (Monday, Mar. 25th). These parallel tutorials will explore relevant issues in computing, networking, civil liberties, the law and law enforcement. Each seminar is designed for those who are experienced in one area, but are less knowledgeable in some of the other disciplines.

To explore the issues and their interactions and ramifications, conference talks and panel discussions are scheduled for the remaining three days (Tuesday-Thursday, Mar. 26th-28th). These will emphasize balanced representation of all major views, with ample opportunity for probing questions and discussion.

The opening conference session on Tuesday will include major policy proposals by one of the nation's best known Constitutional scholars: Laurence H. Tribe, Professor of Constitutional Law, Harvard University Law School: "The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier"

The Tuesday evening session will feature a leading expert in the areas of telecommunications regulation, international telecomm policies and economics: Professor Eli M. Noam, Professor & Director Center for Telecommunications and Information Studies, Columbia University Graduate School of Business

Tuesday-Thursday Conference sessions offering diverse speakers & panel discussions include:

- Computers & Network Trends
- Personal Information & Privacy
- International Perspectives & Impacts
- Law Enforcement Practices & Problems
- Law Enforcement & Civil Liberties
- Legislation & Regulation
- Computer-Based Surveillance of Individuals
- Ethics & Education
- Electronic Speech, Press, & Assembly
- Access to Government Information
- Where Do We Go From Here?

The conference is sponsored by Computer Professionals for Social Responsibility–A nonprofit educational corporation. Telephone: (415)322-3778 Fax: (415) 851-2814 Conference e-mail: cfp@well.sf.ca.us

Co-sponsors & cooperating organizations include: Electronic Frontier Foundation, Electronic Networking Association Association for Computing Machinery, American Civil Liberties Union, ACM Special Interest Group on Software, Videotex Industry Association, IEEE-USA Intellectual Property Committee Cato Institute, IEEE-USA Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers-USA, ACM Committee on Scientific Freedom and Human Rights, ACM Special Interest Group on Computers and Society, The WELL, Autodesk, Inc., Portal Communications.

March 25-28, 1991, Monday-Thursday in the Bicentennial Year of the Bill of Rights

Airport Marriott Hotel, Burlingame, California on the San Francisco Peninsula, near San Francisco International Airport

Sponsored by: Computer Professionals for Social Responsibility –A nonprofit educational corporation

Chair: Jim Warren, Autodesk & MicroTimes, fax/415-851-2814, e-mail/jwarren@well.sf.ca.us

Request for Invitation

To facilitate useful dialogue and balanced participation by representatives from all of the diverse groups that are interested in these issues, this First Conference on Computers Freedom & Privacy (March 25-28, 1991) is limited to 600 invited participants (Conference facility capacity is also limited). All interested parties are encouraged to apply for an invitation. To receive information about the 50-60 speakers & panelists, the tutorials and an Invitation Application form, forward the following information to: e-mail/cfp@well.sf.ca.us -or- fax/(415)851-2814 -or- CFP Conference, 345 Swett Road, Woodside CA 94062

Name:

Title (if any):

Organization (if any):

Mailing address:

City/state/ZIP:

Phone number:

Alternate phone (if any):

Fax number (if any):

Electronic-mail address (if any):

Your particular interests (maximum of one page, please):

Plans and Actions:

Current EFF Activities

The Len Rose cases

The EFF legal department has been working to provide litigation support in the two criminal cases involving Baltimore computer consultant Len Rose. In the first case, we have been particularly active in helping develop the factual and legal issues in the case, and in locating and screening potential witnesses. We believe Baltimore case raises important issues concerning both the application of the federal Computer Fraud and Abuse statute (which we have challenged on the basis of unconstitutional overbreadth), the federal wire-fraud statute, and the federal Interstate Transportation of Stolen Property statute (which we believe should not be applied in cases of unauthorized copying of copyrighted software).

We have been providing similar support in Rose's state criminal case in Illinois. Among the issues in that case is whether the Illinois "computer tampering" statute is overbroad, and whether it in fact criminalizes the activity that Rose is alleged to have committed. In both cases, we have relied extensively on communications over the Net to initiate and maintain contact with potential witnesses.

The RIPCO BBS case

We have also been giving significant time to reviewing the warrant affidavits in the RIPCO BBS seizure. In addition, we have been reviewing the available archived files from that BBS to determine what, if any, justification there was for seizing the equipment.

We believe the RIPCO case potentially raises important issues about the valid scope of searches and seizures, the chilling effect of such seizures on First Amendment-protected speech and association, and the limits of sysop liability for the activities of third parties.

Other matters

We have continued our ongoing investigations of cases that raise issues that may be of EFF interest. In many of these cases we have chosen either not to become involved, or to wait until the cases reach a procedural stage (such as an appeal) at which it would become more appropriate for the Foundation to intervene.

The EFF phone line has become, to some extent, a "hotline" for people who are curious and/or worried about how their rights as citizens and as computer users may be threatened specifically or generally by government action. We have been in contact with people who were convicted of computer crimes before the EFF came into existence, and occasionally have been able to provide useful information to the lawyers handling appeals of these cases. We also have become a center for general information, with phone calls, mail, and e-mail every day requesting information about EFF and its work.

Two versions of the Massachusetts Computer Crime Bill have been introduced in the Massachusetts legislature, one of which is identical to the EFF bill which didn't pass last year. Mike, Sharon, and Mitch will all be working toward passage of the bill this year.

Conferences and Meetings

On December 19th John and Mitch spent half a day at Lawrence Livermore National Labs in Livermore, California at the invitation of the computer security management there. The trip was arranged by Russell Brand. We spoke to a large general audience of lab employees as well as had meetings with smaller groups of security experts concerned with security both at Lawrence Livermore and on the large Department of Energy computer network generally.

John and Mitch also appeared on a panel at Mac World at the Moscone Center on Friday, January 11th, which was chaired by Jim Warren. Also appearing was Alameda Country District Attorney Don Ingraham. John spoke in Los Angeles at a combined SIGGRAPH and ACM meeting in early January.

Compuserve

Scott Loftesness, who is a Well member, EFF supporter, and Compuserve veteran is about to open a Telecommunications forum on Compuserve which will feature an EFF sub-forum. Library materials from the Well have already been ported over. We will announce this in the EFF conference on the Well and encourage people to seed the Compuserve forum with their participation to help it get off to a good start.

EFFECTOR

The Electronic Frontier Foundation, Inc.
155 Second Street Cambridge, MA 02141

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

Contact

How to get in touch with the EFF:

Via Computer Networks:

Send requests to be added to or dropped from the EFF mailing list or other general correspondence to eff-request@well.sf.ca.us. We will periodically mail updates on EFF-related activities to this list.

If you receive USENET newsgroups, your site may carry two new newsgroups in the INET called comp.org.eff.news and comp.org.eff.talk. The former is a moderated newsgroup of announcements, responses to announcements, and selected discussion drawn from the unmoderated "talk" group and the mailing list.

Everything that goes out over the EFF mailing list will also be posted in comp.org.eff.news, so if you read the newsgroup you don't need to subscribe

Postings submitted to the moderated newsgroup may be reprinted by the EFF. To submit a posting, you may send mail to eff@well.sf.ca.us

There is an active EFF conference on the Well, as well as many other related conferences of interest to EFF supporters. As of August 1990, access to the Well is $8/month plus $3/hour. Outside the S.F. Bay area, telecom access for $5/hr. is available through CPN. Register online at (415) 332-6106.

A document library containing all of the EFF news releases, John Barlow's "Crime and Puzzlement" and others is available on the Well. We are working toward providing FTP availability into the document library through an EFF host system to be set up in Cambridge, Mass. Details will be forthcoming.

Via Mail or Telephone:

The Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141
Telephone: (617) 864-0665
Fax: (617) 864-0866

"Chaos. It's more than just a name. It's our way of doing business!"

Germany's Chaos Computer Club is known in the US primarily for its incursions into U.S. military and NASA computers (see Clifford Stoll's *The Cuckoo's Egg*). Then there was the well-publicized information-for-money deal with the KGB that got busted. The latter was perpetrated by persons who, while not official club members, are at least within the Chaos Computer Club's ambit. Little more is known about the Chaos group outside Germany.

Chaos members who might enlighten the rest of the world as to the nature of their organization seem to be nonexportable. One of their better-known members, Steffen Wernery, was arrested on charges of computer vandalism on his arrival in Paris where he had a speaking engagement. He was imprisoned for months. Other well-known members are understandably loathe to leave Germany.

Contact between the Chaos Computer Club and the East Berlin Computer Club was established at the CCC's Christmastime '89 Kongress in Hamburg. When I received calls from Hamburg and Amsterdam alerting me that the next CCC Kongress was imminent and to be held in the "East Zone," as the West German computer security journal *Daterschutz-Berate* quaintly termed it, I immediately left for Europe.

Arriving in Amsterdam, I learned that I was a full month early. I suspect my informant was a bit hazy on the exact dates simply because he wanted an *Amerikan* around to talk to. No matter. I purposefully occupied my time doing preliminary fieldwork in Amsterdam, checking out its hacker underground, squatters' movement, pirate radio and TV, and the newly identified Anti-Media Movement

"DESTROY MEDIA!"

—Battle-cry of the Anti-Media Movement

I got my first glimmer of the Anti-Media Movement talking to a member of a group known as ADILKNO (The Foundation for the Advancement of Illegal Knowledge). ADILKNO publishes manifestoes in a hyperintellectual art and media journal, *Mediamatic*. A magazine for the well-read polyglot, its matter is well-nigh impenetrable without a thorough knowledge of Baudrillard, Virilio, Bataille, and Eco, *for starters*. Its motto is, "We watch media like others watch TV."

ADILKNO first proposed its attack on media in a Squatters' Movement document: "By isolating the media, we will reach many *more* people! Within the movement, many feel we must give our opinions to the press. The time in which we can reach our goals through public opinion has long been over!"

ADILKNO believes a "massive defection to reality" is occurring now that *everything* seems to be covered by the media. "The increasing need to make history in a hobby or tourist atmosphere, away from work, is consciously placing the media in the shadow of the event. For the moment, people have no more time for the media... Beyond the media traps, people clear the way for themselves to *do the right thing* elsewhere. In Western museum cities, an avant-garde has formed the anti-media movement, which puts an end to all connections under the slogan, 'Let's pull down another media!' With disappearing acts, it creates temporary and local media-free spaces... It is a preëminently secret movement because it carefully keeps itself out of the press and makes its existence known only through jamming and sabotage. All events that don't appear in the media are claimed as a victory by the movement... The survival strategy of the media is to remain more interesting than reality." Like that.

In the newly published *Movement Teachings: Squatting Beyond the Media* (as yet available only in Dutch), Geert Lovink and Arjen Mulder describe the "outer-medial experience" as "making history on the streets through 'immediate' (i.e. 'media-free') contact."

The Anti-Media Movement is contentless. It can only be discerned, in Lovink and Mulder's formulation, as "curious cuts in the data stream." It is a question of "how we should read the gaps. Is it an accident or the Anti-Media Movement?" One needs "an eye for it."

Hoping to catch traces of the meaningful gaps of the "AMM" at the CCC Kongress, I mobilize special forces: DFM Radio-Televisie.

"YOU WANT INFORMATION OR DEFORMATION?"

DFM stands for "Deformation." DFM Radio-Televisie is the most

Illustration by John Burruss

Amsterdam's most unplugged performer, he could always manage with bullhorns, a bayonet on his guitar, and twenty kilos of fresh dog turds

radical of the pirate broadcasters in Amsterdam. It's staff brands the other pirate broadcasters, (whom anyone else would describe as anarchists), as "proto-yuppies." Confronted with anything short of total chaos of the airwaves, they sneer derisively, "That's what central heating will do to you!", flip on their 180-watt transmitter, tune to the frequency of the offending ten-watt station, and give it a lesson in the beauty and purity of Noise.

For the moment, DFM is housed in "Warner Squat," the former Warner Brothers building in Amsterdam. "Warner Squat" is a three-story, tile-roofed, brick building with all the amenities: screening room, walk-in film vaults, marble, stained glass. This turns out to be my base of operations for my month in Amsterdam.

Test-Case is the director of DFM. In his "industrial" phase, Test-Case was famed for staging "fake riots." For years, he collected sounds at real riots: rolling tanks, snarling police-dogs, cries of panic and anguish, and frenzied barricade-building. At his performances he would blast the crowd with these sounds, highly amplified. He would exhort them to riot, often successfully, and then would record the resulting riot for future recycling.

In his punk-revival period, Test-Case was the most frequently unplugged performer on the streets of Amsterdam. He could always manage, however, without electricity, using such simple expedients as bullhorns, a bayonet on his guitar, and no less than twenty kilos of fresh dog turds to fling.

You can see now why his DFM Radio Televisie was the video crew to take with me to East Berlin. After all, it may take the Anti-Media to catch the Anti-Media.

The "People's Police"

An East German policeman is standing in the bloody middle of the Autobahn fast-lane somewhere near Potsdam, waving a white baton. We are blithely hurtling towards him in a happily screaming, rented Peugeot traveling 150 km/hour. Chanting Tibetan monks, in reverse and overlaid with speedmetal passages and telephone exchange noise, are pumping from a portable cassette deck on the dash. Test-Case is at the wheel. He's a tightly sprung, angular young man in a "Mutoid Waste Company" T-shirt with a grown-out blonde mohawk lying dormant on his crown like a cockatoo's folded crest. Test-Case decelerates dramatically as the cop imitates a finalist in a baton-twirling competition. Our abrupt stop, a bare meter from the cop's knees, sends our fellow traveller, the somnambulant DFMer Bastiaan, onto the floor and into a fresh spate of scabies-scratching. We are directed to a rest area.

We pull up beside a curtained *Volkspolizei* ("People's Police") microbus with a large DDR seal (a compass superimposed on a hammer in a ring of ribboned grain which many say actually depicts a secret police spyglass) emblazoned on its side. A family nervously packs up the picnic lunch they'd been sharing 'round the open trunk of their "Trabbie." A man wearing mirrored aviator shades peers 'round a curtain edge from the interior of the police microbus while his companion, an obvious steroid abuser, takes our papers, growls that we've been travelling grossly in excess of the 100 km/hour speed limit, and returns to the microbus. We wait as the "People's Police" examine our papers and do more peering.

"Maybe I just tell this wanker this car doesn't go that fast," says Test-Case with inappropriate swagger as the cop with the Louisville Slugger stride beats it back to our car. This story would be highly suspect. Our velocity had been such that the string of particolored, plastic-bodied Trabants we had been passing had looked like a strand of Mardi Gras beads. I am irresistibly reminded of the *last* ride I took with this crew. Dutch police in a fluorescent-orange, turbocharged Mercedes had appeared suddenly, pulled us over, and confiscated our car.

I steer Test-Case away from a prompt pulping with "Nee, Test-Case! Nee! Nee!! Just *look* at him! He's wearing the head of a Rotweiler!"

The House of Young Talent

For the balance of the drive to East Berlin, Test-Case fills my dyspeptic silence with assurances that the 150 mark ticket can be paid in Eastmarks, the currency that looks as if it's come from a Monopoly game—tiny bills with grain threshers depicted on them and aluminum coins that can be bent with your bare hands. They are worth one-fifth the value of the redoubtable Westmark. The subject changes only as we reach East Berlin, where Test-Case scrutinizes the buildings closely. "Look at *that* one! It's perfect!" What he means is "eminently squattable." I feel as if I'm riding with a real estate broker as he points out the squatterly possibilities of numerous (far *too* numerous) properties.

We finally arrive at our destination: das Haus der Junger Talente (the House of Young Talent). Test-Case feels our chances for free admission are directly proportional to the bulk of equipment we haul in with us. Burdened with an impressive array of lights, tripods, cameras, cables, and equipment bags, and some personal luggage for good measure, we stagger in.

At the door, a person armed with a walkie-talkie looks us over.

After we pay the full admission, Polaroid photos are taken of us, stapled onto name tags bearing the Chaos emblem, and stamped with the Chaos seal.

Knowing that Chaos events swarm with intelligence agents, I leave the line for my name blank—at least until I can get inside and evaluate the scene. Wandering through the immense labyrinth, I find hundreds of people wearing blank name tags. The ones that *are* filled-in bear highly improbable names. No one is going to make an intelligence agent's job easy here. Such anonymical measures are second-nature in a country where one of every four people were informers on the Stasi (Secret Police) payroll. Some rooms have signs reading "PHOTOGRAPHIEREN VERBOTEN!" posted outside their doors.

I pause to consider what appearance I'm presenting to the other Kongress attenders. A mirror reveals a man of roughly thirty with a hat pulled down to the top of his dark glasses, wearing an extra-long, buttoned Burberry trenchcoat extending to his boot-tops and a blank press badge. In short, I've arrived with *all* the spook-accoutrements, save a Minox subminiature, handcuffed Halliburton attaché, and an underarm bulge from a Walther PPK. No *real* agent would dare dress this way, in full Spion-drag. Bolstered by the realization that it will be taken for a pseudonym anyway, I add my real name to the badge.

I've arrived with all the spook accoutrements save a Minox subminiature and an underarm bulge from a Walther PPK

"This is 'Reality Hacking!'"

—Steffen Wernery

The Kongress opens with the statement, "Holding a CCC Kongress in East Berlin is true 'Reality Hacking.' " R. U. Sirius' expression has gained currency over here.

There are few computers in East Germany and no laws against hacking yet. East German officials are not nearly as concerned with a large gathering of hackers as the humorless and paranoid Western authorities. They have other things to worry about.

East German life is in total flux. Turbulence, uncertainly, and improvisatory reality is attractive to hackers. Chaos is their very medium. ("Chaos. It's more than just a name. It's our way of doing business!")

There are approximately 600 people attending the Kongress. None of the Chaos members I ask knows how many people are in the organization. I'm told that the name tags are deceptive. They merely give the *appearance* of organization, camouflaging a deeper chaos. If pressed, most attenders describe themselves as "interested observers" rather than official Chaos members. Nearly everyone is a "computer security expert." No distinction is made between designing and cracking security systems.

One room has been set up as an archive where hacker and anarchist literature in French, German, and English can be read and photocopied. Other rooms are filled with computer equipment and telephones. There are lectures, panels, and workshops on The Creative Use of Technology, Data Security as Human Security, Information Ecology, the Power of the Media, Freedom of Information, Copyright, Viruses, Enlargement of Civil Communication Structures in the DDR, Mind Machines, and Virtual Reality.

Cognitive Dissidents

The house phones were made in 1963 (their vintage stamped on their underbellies), and it's extremely difficult to place a call to the West from them. It may take an hour to get a line out *if* one can get a line out. The lines are pretty much all bugged. Some, with multiple bugs, have seriously degraded sound quality. The phone company runs newspaper ads offering free bug-removal. Used Stasi surveillance equipment is available in modestly priced, sealed case-lots.

"Chaos organizers" sounds like walking oxymorons. They manage, however, to keep uninterrupted communication with the West as they stroll the halls with 10,000-Westmark cellular phones operating on gold-plated chip-cards. "Be careful with that card! Someone could easily give me a mega-phonebill," warns the person who lends me his unit.

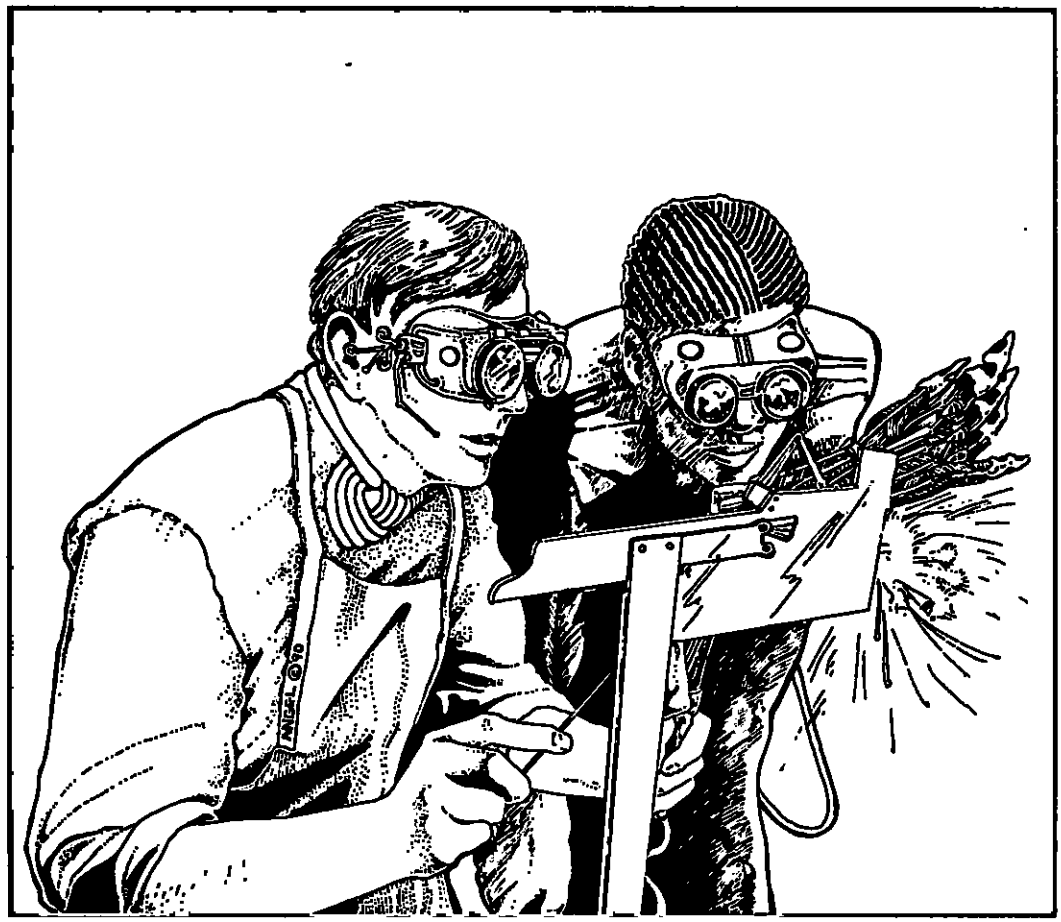
Every presentation draws a silently listening capacity crowd. Information on "brain machines" and the "Data Glove" is eagerly drunk in by the East Germans. The idea of Virtual Reality is readily embraced as a better telephone system

Appropriately, at this point in the transmission, Mr. Russell—who has taken to living in Transylvania—disappeared. Last we heard, he had sponsored a VR congress in Linz, Austria, where he stayed in A. Hitler's old favorite hotel room. (Rumors that he happened upon the actual *Spear of Longinus while digging up the floorboards after having ingested too many Ritalins are—we assure you— total hype. R. U. Sirius has the genuine article himself, having spotted it unrecognized at the auctioning of Andy Warhol's personal affects.)*

Anyway, who are we to say that the Anti Media Movement should *be covered in the media? But, perhaps, if Mr. Russell emerges from his Transylvanian hideaway, we will present this saga in a future issue.* M

The World's Oldest

SECRET CONSPIRACY



Fronted by Steve Jackson Games, Inc.

Thanks to the Secret Service, Steve Jackson Games has gotten plenty of hard-won press. But what about Steve Jackson himself? Who is he and what was his adventure game company up to before all this started? What effect has the Great Hacker Raids of 1990 had on them and what are their plans for the future?
Gareth Branwyn

IT'S ALL IN THE GAME

MONDO 2000: How did you get started in game publishing?

STEVE JACKSON: Well, I got started playing games in college. When I got out of college, while going to law school, I answered an ad in the paper from a local gaming company called Metagaming. I didn't get the job, but later they accepted an original design of mine called Ogre, which was about a giant futuristic killer tank.

M2: So when did you start Steve Jackson Games?

SJ: In 1980.

M2: What was the first SJ Games release?

SJ: *Raid on Iran*, which dealt with the question of what would have happened if they had actually gone in. Then there was *Kung Fu 2100*, which was way-out science fiction. And then we did a game called *One*

Page Bulge. It was a wargame covering the Battle of the Bulge with all the rules on one sheet of paper.

M2: Oh yeah, that was a great game. What's your biggest selling game? Is it still *Car Wars*?

SJ: Yeah, *Car Wars* and the *GURPS (Generic Universal Role Playing System) Basic* are our biggest sellers.

M2: What are some of the other games in the SJ Games line?

SJ: Well, of course there's *Illuminati*.

M2: How did that come about? Were you a fan of *The Illuminatus Trilogy?*

SJ: Oh yes! That came about when Dave Martin [the guy who did the cover art for the game] and I were drinking wine and talking about life, the universe and everything.

M2: Ooh, one of my favorite drinking conversations!

SJ: Right. Anyway, the subject got around to how you could make a game out of the Shea and Wilson books. I didn't think you could do a game based on the actual characters and events... what with yellow submarines, Discordians and a giant octopus running all over the place. It would be too tough. A few days later, I was driving someplace when it occurred to me that you could build it all around a deck of cards. After I got the car under control...

M2: (Laughs)

SJ: No really! I sat there in the front seat and started taking notes. I realized that rather than trying to use the world that Shea and Wilson had envisioned, I would go back to their source material.

M2: You mean basic fear and paranoia?

SJ: Yeah right. No, I mean the *Principia Discordia*. Did you know that it actually exists?

M2: Oh yes.

SJ: A lot of people don't. Anyway, we decided to focus just on the conspiracy theory aspects of *Illuminatus*. After that, the creation of the game became absolutely simple.

M2: I heard you're developing a GURPS worldbook based on *The Prisoner*.

SJ: It's already out.

M2: Oh really. How's it doing?

SJ: People seem to like it and it's doing well, considering it's a sub-genre of a sub-genre. We only printed 8000 copies and when they're gone, I doubt we'll do another run.

M2: Do you still get a chance to play games for fun, or is it all business?

SJ: It's all for business now. The only time I really get to game is when we go to game conventions.

M2: What are your favorites?

SJ: Well, in terms of my own, *Ogre* and *Illuminati*. And, I like *Axis and Allies* from Milton Bradley quite a bit.

M2: How did the Generic Universal Roleplaying System (GURPS) concept come about?

SJ: Well, the basic idea behind GURPS was this: any roleplaying game, regardless of genre, has a system for making decisions about how the characters behave in the game. There's a system for creating the characters and resolving various kinds of tasks—things like: was the character successful at jumping across the ditch... or whatever. Now each game system, unless they totally swipe from D&D, comes up with a different way of dealing with all this. I found this totally obnoxious. I realized that most games, regardless of the genre (fantasy, sci-fi, horror,

GURPS Cyberpunk

by Gareth Branwyn

So what is the game that caused all this controversy really like? Well it's probably not what the Secret Service had in mind. (One can imagine the Feds sitting around late at night, playing Cyberpunk, waiting to be taken over by some spell of subversion hidden within its pages.)

GURPS Cyberpunk isn't really a game at all. It's a "Sourcebook" for a larger game called GURPS (Generic Universal Role Playing System). GURPS is a set of roleplaying game rules that apply to any adventure setting or time period. Most roleplaying games are specific to a genre (fantasy, sci-fi, horror, super heroes) and you need to learn a whole new set of (usually complex) rules for each game. The GURPS Basic Set covers all the rules that are universal to these different genres and then presents genre-specific rules in supplemental books. GURPS Basic includes the main game mechanics of character creation, combat, and methods of task resolution. The rules are structured so that you can start simply and add more detail as you go. Sections cover character advantages/disadvantages, skills, vehicles and equipment, and information on creating your own adventures.

GURPS Basic is clearly designed, heavily indexed, and arranged to allow easy access to the rules while playing. All you need to play is a pile of six-sided dice, some paper and pencils and a small group of willing eggheads.

GURPS Cyberpunk is a sourcebook that can be used with any of the SF oriented GURPS worlds. It includes a set of additional rules specific to cyberpunk adventuring, such as cyberwear technology, net running, and brain implants. Character types include techs, reporters, spies, mercenaries, and net runners. The writing in GURPS Cyberpunk is excellent and obviously penned by a fan of the genre. There are extensive side-bars on many aspects of the milieu, ingenious rules for navigating and adventuring in cyberspace, and a bibliography of cyberpunk material.

GURPS is available at most hobby/game stores and should be available at your local Waldenbooks or B. Dalton. You can also write the company directly at SJ Games, PO Box 18957, Austin, TX 78760. M

As soon as they announce that skull implants are available, I'm gonna line up for mine. I'd like to add a few languages, be able to go without sleep...

etc.), need pretty much the same rules, so you could get that out of the way easily and start playing. So why not make one generic system of rules and a series of worldbooks that tailor those rules to specific genres?

M2: So the Cyberpunk game is one of these modules?

SJ: Well, I don't like the term "module." It implies a kind of faceless interchangeability. We call the publications that describe a gaming background a worldbook, and those that provide information that can be used in a variety of worlds, a sourcebook. Since the Cyberpunk information can be used in any of the GURPS Sci-fi worlds, it's a sourcebook. I don't like the word "scenario" either, which comes from wargaming.

THE CYBERPUNK

M2: Why did you do a *GURPS Cyberpunk?*

SJ: We had a bunch of cyberpunk fans around here and we really wanted to play in a cyberpunk-type world. It went through three different writers. The project kept going out and not coming back. Finally, I said: "Lloyd (*Ed. note:* Lloyd Blankenship is author of *GURPS Super* and a legendary hacker), why don't you just do it?"

M2: Is Cyberpunk—not the game, but the whole genre—of personal interest to you?

SJ: Oh yes. I think we'd better read about that world because we're probably going to be living in it. It lays out a very clear path to our future.

M2: Well, that was going to be my next question. I too believe that the worldview running through Cyberpunk has a lot to say about surviving an increasingly alienating world. To me it's good cultural criticism.

SJ: I don't know if the future is necessarily going to be cyberpunk or cyberprep, but it's going to be cyber-something. And as soon as they announce that skull implants are available, I'm gonna line up for mine.

M2: Oh yeah? What "moddies" do you want?

SJ: I'd like to add a few languages, be able to go without sleep, and obviously, I'd like to get a direct neural interface with my computer. That would be great.

M2: What cyberpunk books or movies have you found inspiring?

SJ: Definitely *Blade Runner*—for the look more than the writing or the acting. *Max Headroom* for everything except Max himself. I think they could have just dropped Max out of the show altogether and we wouldn't have lost anything. I of course liked *Neuromancer* and *Count Zero* and Gibson's short stories. *Mona Lisa Overdrive* didn't add anything for me. And Sterling is great... absolutely.

M2: I hear that you went to the Cyberspace Conference in Austin?

SJ: No, I was planning on it, but I wasn't able to. Lloyd was there.

THE SECRET SERVICE RAIDS

M2: How bad a blow has this whole affair been to SJ Games?

SJ: It's been really bad. We've lost an estimated $125,000 in sales and we had to lay off eight of our employees. We're now on the verge of bankruptcy. If we don't get $20,000 in the next few weeks, I'm going to have to file.

M2: Do you feel that you've been dealt with fairly in the media? With all the other distortions that have been rampant, the information about your part in this drama seems rather straightforward.

SJ: I think so. In general, some of the press coverage has been grossly ignorant—written by people who don't know what they're talking about. And they insist on quoting people like Gail Thackery, Assistant Attorney General from Arizona, who lumps all types of hackers and computer users together and then insists on calling them white-collar criminals.

M2: The first time I talked to you, early in the course of all this, everyone seemed to be scratching their heads trying to figure out why on earth the Secret Service would be bothering SJ Games. But as the weeks wore on and more information began to emerge, I found out that the author of GURPS Cyberpunk, Lloyd Blankenship, was a "reformed hacker" who still ran a hacker BBS out of his home and was alleged to have been "connected" with the Legion of Doom...

SJ: Well, he ran the Phoenix Project for a long time, but it wasn't really a hacker's board. It was meant to be a forum where hackers, security professionals and feds could get together and talk. He had that type of dialogue going on there.

M2: But did the Feds actually log on there? I heard that he invited them. Did they ever show up?

SJ: I don't know. They were definitely invited in. I can't believe that they weren't at least monitoring it. Every other board seems to have been monitored.

M2: Anyway, when I read that about him, it wasn't as hard to figure. The Secret Service gets wind of the fact that Lloyd is publishing a book, so they decide they'd better have a little look-see before that thing hits the streets.

SJ: That may very well have been it. We're waiting for that warrant to be unsealed so we can find out what the reasoning was behind it... if any. (general laughter)

It seems likely that they started to come after Lloyd and, for some reason, decided to come after us too. Or it could be that they decided

our Illuminati BBS, which we run for our customers, was in fact a hacker's board. Or another possibility is that they heard about Project Phoenix and wanted to crack down on it. Those are three very good possibilities.

M2: Well, here's another wrinkle. Somebody recently told me that phone companies, corporations, and government agencies, are hiring people to scan boards looking for signs of criminal activity. When they find something that looks suspicious they spoonfeed it back to their bosses. Can you imagine some dumb kid stumbling onto the Illuminati BBS and finding material on cyberpunk and data cowboys, thinking it's all real and sending it, out of context, to the Service? Boy, talk about playing into their paranoid fantasies of an organized hacker cult.

SJ: Yeah, when you log onto the Illuminati board it says: "Welcome to THE ILLUMINATI, Online home of the world's oldest and largest secret conspiracy. Fronted by Steve Jackson Games Incorporated." (Laughter)

M2: I guess that would just about do it. Did the Secret Service really confiscate your laser printers?

SJ: They took one laser printer from here and one from Lloyd's house.

M2: What on earth did they think you were going to do with them?

SJ: There've been several theories about that, each assuming different levels of intelligence. First of all, they may just be in the habit of grabbing everything. Someone suggested that, since it's a printer, they might have thought they could read the ribbon on it. Of course, a laser printer has no ribbon. Or, maybe they took the full setup of equipment so that they could use it in their offices.

From GURPS Cyberpunk: The Sourcebook

Electronic Addiction

With direct access to the brain, a wide variety of psychedelic effects can be produced without actually having to ingest chemicals. A character can never experience any physical damage because of withdrawal from an electronic drug addiction— psychological dependency, however, can be real.

The most dangerous form of electronic drug is direct stimulation of the pleasure center of the brain. This is commonly referred to as "wireheading." Wireheading is cheap, totally addictive, and may be legal or illegal depending on the campaign world.

Wireheading is much like any other form of implant. Electrodes in the brain, connected to a pleasure center, are hooked to a jack in the back of the skull. A small transformer, plugged into normal house wiring, provides the trickle of current necessary to stimulate the pleasure center. While a wirehead is hooked in, he becomes impervious to everything except the stimulation and will forego food, water, sex or anything else. To help circumvent this, transformers may be required by law to time out after 10 minutes and not reset for 12 hours. (This timer can only be defeated with the proper, sophisticated tools—a soldering iron, for instance.)

For graphic descriptions of wireheading, see Spider Robinson's short story, "God Is an Iron" (or its novelization, *Mindkiller*) and Larry Niven's novel *The Ringworld Engineers*.

Corporations

In a *corporocracy*, or corporate-dominated society, there is a sharp division between haves and have-nots, between those who belong to the corporate world and are protected within it, and those who are locked out in the cold and dark. To those on the outside, the corporations appear to be a heartless, oligarchic tyranny, crushing all in their path. To those on the inside, the corporation is seen as a protector which holds off the ravening horde outside the gates.

Some corporations may have generous intentions and will donate to worthy causes, but they have to stay in business and make a profit before they can indulge in such luxuries. As the world becomes tougher, the corporations adapt by becoming tougher themselves, out of necessity. This "we protect our own" attitude is sometimes called *techno-feudalism* Like feudalism, it is a reaction to a chaotic environment, a promise of service and loyalty from the workers in exchange for a promise of support and protection from the corporation. It is similar to the Japanese concept of "lifetime employment."

Prayerware

With computers pervading the households of the world, it is only natural that they will begin to be used in religious observances in day-to-day life.

Simple programs might do nothing more than sound the call to prayer five times a day for an Islamic family, or help a Mormon do genealogical research. By the mid-1980s, several versions of the Bible were available on computer disks.

But what about interactive software? A devout Catholic could say several hundred Hail Marys per second if plugged into a fast enough computer with the appropriate software. There would also be a great demand for behavior chips of a "proper" member of the church. And how much could you get for a braintape of someone who claimed to have spoken to an angel or a god?

Endangered Species

In a cyberpunk future, it may be assumed that many of today's endangered species are extinct, while many more creatures that are common today have become threatened. "Save the Whales" may be an obsolete slogan; "Save the Dolphins" or even "Save the Tuna" may be heard instead. As the protectors of endangered species lose battle after battle, they become ever more desperate and fanatic.

Groups like the "Wadical Wabbit Pwotectows" have been responsible for the destruction of automated farms, fishing platforms, and similar food-harvesting devices worldwide. Sportsmen, and even scientists and museum collectors, have been harassed or murdered by ambush.

We Don't Need No Steenkin' Standards!

One of the connectivity problems facing the networks of the 90s is interface standards. Right now, there is no universal method of data exchange — there are literally *dozens* of protocols in the networking community.

Most cyberpunk nets are based on the idea that, eventually, one standard will arise from the multitude and become accepted worldwide. The malicious (or perhaps just realistic) Game Master will not assume this to be the case. If networks are broken up by region (whether along international, corporate or local bounds), the GM could make each area's networks use a different communication protocol. This can evolve into several interesting game sessions as the frustrated netrunner discovers that, no matter how hard he tries, he just can't get any of the computers in Mexico to speak to his cyberdeck. Of course, he might have a few ideas about where to look for a ROM deck that will permit such communication...

But what about interactive software? A devout Catholic could say several hundred Hail Marys per second if plugged into a fast enough computer.

M2: Yeah! That's something that's being discussed currently on the WELL's hacker board. Police departments who don't have enough funds to purchase more computer equipment are using confiscated gear. Is that a conflict of interest or what!?!

SJ: Well, if they're going to be pulling stunts like that they'd better learn more about computers and disk management. If they think that they can use someone's stuff and then simply hit *del* to get rid of their files—which they probably don't want seen out of their office—they're in for a surprise.

M2: An issue that dovetails with that is whether the government has the right to read the files on the computers they seize. And, if the data is encrypted, do they have the right to force the owner to de-encrypt it?

SJ: That's a very interesting question. I mean, the only reason I can imagine they'd confiscate the computers in the first place is in order to read the files. Is it required that you show them how to read them if they're encrypted? I don't know, but it seems like you could take the Fifth on the grounds that de-encrypting the files might incriminate you. You'd better have some damn good encryption though.

The problem is, having them devote so many man-hours to decoding your files is only going to prolong the ordeal. One of the reasons they gave for holding our stuff so long was that they didn't have the time to go through it all.

M2: I guess not, when they're confiscating things like printers, boom boxes and audio tapes. I love what Julian Dibbell said in his *Village Voice* article about the seizure of Acid Phreak's tapes: "the incriminating evidence fell into four basic categories: salsa, merengue, house and lambada."

SJ: Next thing you know, the Secret Service will say they need more funds to hire agents to go through the thousands of disks they've confiscated.

M2: What kind of help are you getting from the Electronic Frontier Foundation?

SJ: They're going to continue to press for the return of the rest of our stuff. Most of it was returned, but we're still missing some important things like a hard drive that was not backed up. And basically they're going to try to get some answers as to why the search and seizure happened in the first place.

M2: You were in DC for the press conference announcing EFF.

SJ: Yes. It was fascinating. We spent several days in DC meeting with EFF, Congresspeople and Computer Professionals for Social Responsibility. The press conference itself was pretty good. People asked intelligent questions.

THE END?

M2: How do you define hacker?

SJ: When I hear the word hacker, I still think of the old idea of the fanatical, dedicated, almost *monastic* computer programmer who sits up all night, eating Cheetos, drinking Coke and working on programs.

M2: (laughs) And an expanding waistline. What are your feelings about the hacking underground?

SJ: I'm sympathetic to some individuals and some aspects of the so-called underground. As in any underground, you have some people who are involved for wholesome reasons and others who aren't. Most of it seems pretty tame. But those kids who do break into systems better be darned sure they don't break anything.

M2: Do you think that the publicity will help you sell games? How are the GURPS Cyberpunk sales doing?

SJ: Cyberpunk sales are doing OK. The problem with the argument that the publicity will help us sell games is that we have such a small potential market to begin with. The gamers already knew about the game before any of this. I have no doubt that we have sold a *few* more, but I don't think it's a significant amount. The mass market that reads the mass media that we've been in aren't going to buy it anyway because they're not roleplaying gamers.

M2: What are your plans for the company's future?

SJ: If we don't come up with that $20,000, our company isn't going to have a future. So my first goal is to try and come up with that.

M2: Optimistically, what would you like to do?

SJ: Well, I'd like to continue to produce role-playing games, do some computer games, and I'd like to try some experimental games.

M2: What do you mean by "experimental?"

SJ: Exploring different approaches to roleplaying that haven't been tried yet. Lloyd and I have been working on a Bulletin Board System. We've been talking about it a lot, but we haven't written a line of code for it yet. I don't have any money to put into R&D. We're strapped. I'll tell you what I'd like. I'd like B. Dalton and Walden Books to carry *GURPS*. They keep saying that they're going to, but they never get around to it. Maybe if people started calling their local Walden or B. Dalton bookstores and clamored for it. That could definitely help us financially!

Guess Work

An Interview with August Bequai

by Gareth Branwyn

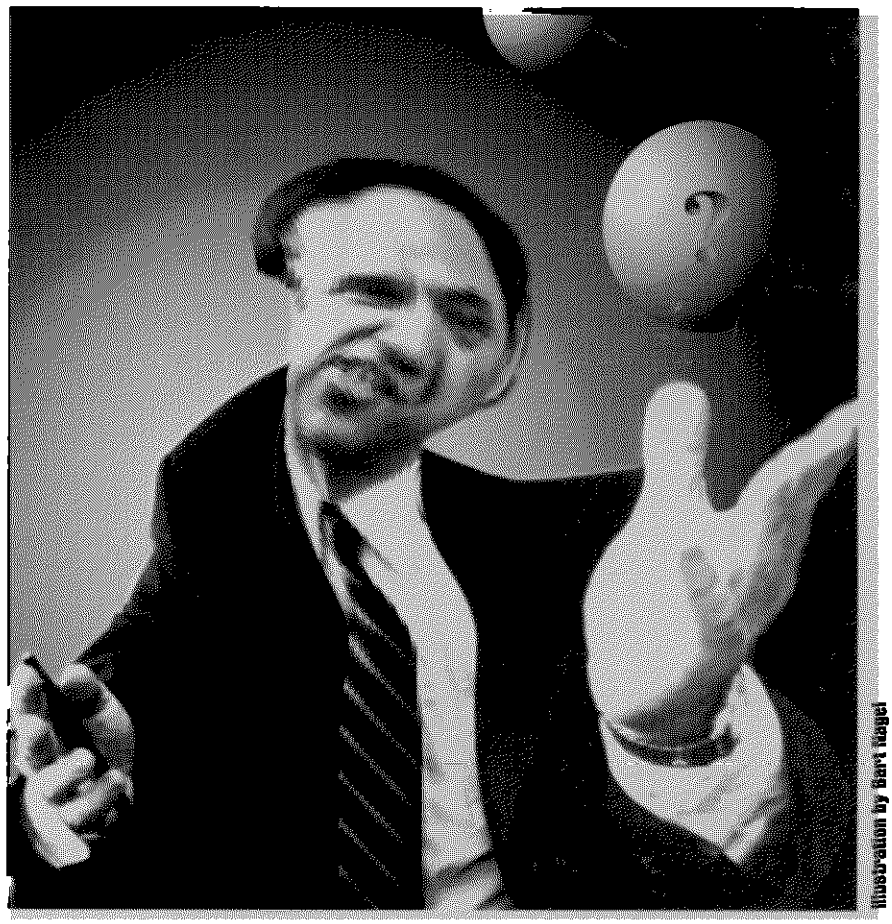


Illustration by Barton Stabler

August Bequai has been recognized (at least on his book jackets) as one of America's foremost authorities on computer security. He plays both sides of the legal fence, having taught at the Secret Service Academy and having represented hackers in court as a defense attorney. Author of over 200 articles and nine books; including Computer Crime *and* Technocrimes: the Computerization of Crime and Terrorism, *he lectures internationally on computer and white-collar crime and holds several teaching positions.*

—Gareth Branwyn

DEFINING HACKERS, DEFINING GOD

MONDO 2000: I'd like to talk to you about Operation Sun Devil and what's going on with that. Things seems to be happening fast.

AUGUST BEQUAI: You mean Operation Sun Devil itself?

M2: Yes, that and the response—the Electronic Frontier Foundation, the media coverage... I'm on one of the computer networks where there's a daily discussion on the implications.

AB: That's interesting, because when you look at it from the point of view of criminal law, it's not one of the more important cases in America today.

M2: It is for those people who are concerned about technological development and telecommunications! You've said that you've defended some hackers. How do you define "hacker" in your work?

AB: That's like asking "How do you define God?" Or, "How do you define good?" You know what I mean?

M2: No, not really. There are perfectly reasonable definitions of "hacker" being kicked around these days. The discussion seems to be centered on making clear distinctions between hackers and computer criminals. Hacker might simply refer to a computer enthusiast.

AB: Well, I would just call them white collar criminals. If an individual violates a criminal statute using a computer, as far as the courts are concerned, they're not going to call him a hacker, they're going to call him a defendant.

TAKING ON THE SECRET SERVICE: CHEAP, EASY AND FUN?

M2: Members of the computer networking community are concerned about the misperception of their community, who comprises it, and what they use the networks for.

AB: Let me tell you this. I think they can all go home and sleep pretty safely tonight. From a criminal lawyer's point of view, the government doesn't have the resources to put all the techno-players in jail and I just don't see the government's efforts being at the scale that some of the literature and some of the individuals involved see it.

M2: But what do you think about the criticism that, with Operation Sun Devil, they've unconstitutionally confiscated equipment such as public bulletin boards? This sort of thing has struck fear in the hearts of many systems operators. The seizure of the Steve Jackson Games BBS is a case in point. They were, by the admission of the Secret Service, not the target of the investigation. And yet their BBS was confiscated.

AB: Then they have the option to go to court and challenge it. We have laws and a legal system, and they work!

M2: *If* you have the resources!

AB: You don't necessarily need a lot of resources. It doesn't take a heck of a lot of money to go to court and challenge some of these things.

M2: You're telling me it doesn't take a lot of time and money to challenge the US Secret Service!?

AB: *No sir*, it does *not*. If you hire a small firm, no.

M2: But wouldn't you want a big, powerful firm to represent you against the US government?

AB: Honest to God, I can't believe it! I've taught at the Secret Service

ON THE ROAD TO CHAOS IN EAST BERLIN

by Morgan Russell

A Message to You from Legion of Doom Member "The Mentor"

Who or what exactly is this "conspiratorial hackers gang" that calls itself "The Legion of Doom?" According to those in the know, legend of the Legion has been exaggerated in accordance with authorities' need for a major threat. LoD is really just a loose alliance of a very few young computer hackers. I was told by several people that the one who calls himself "The Mentor" is the Legion's most eloquent spokesperson and that I could find a couple of manifestos in back issues of Phrack. *The following is a segment from "The Conscience of a Hacker," written in 1986.*

R. U. Sirius

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it weren't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can't stop us all.

The Mentor

Illustration by Michael Swaine


We interrupt this program for a message from "The Mentor"

I mean, I was accused of conspiring to *destroy* the 911 system in the United States!

M2: In all your dealings with crackers, did you ever run across anyone who willingly destroyed or changed files?
CN: I've been told many a tale about unauthorized access to computers, but if anyone willingly damaged or changed files, they kept it a secret from me.
M2: Where does the public perception that crackers are driven by malign intent come from?
CN: Government press releases and reporters who don't understand what the computer subculture or computer underground is all about.

I mean, I was accused of conspiring to *destroy* the 911 system in the United States! This could not have been further from the truth.

A BUREAUCRATIC DOCUMENT

CN: On January 18, 1990 my life changed forever. On that afternoon, I was met by agents from the United States Secret Service and Southwestern Bell security. Believing I had nothing to hide, I answered all of their questions truthfully and was given the impression that I wasn't in trouble. I later learned that what you say doesn't really matter, it's what they want to make out of it. They'll interpret it to fit their own preconceived notion.

So the following day, I got my first look at a real federal search warrant. It was for my room.
M2: Did you have any idea what they were busting you for?
CN: No, not at first.
M2: Let's talk about the E911 file. What was it and why'd ya wind up publishing it in *Phrack*?
CN: It was a bureaucratic document describing the administrative procedures and responsibilities of some of the departments in the phone company. I got it late '88 and early '89 from a hacker named Robert Riggs, as an article submission. Although infinitely confusing and full of transmission errors, I edited the file back together and trimmed it down. The text file appeared in the February 1989 issue of *Phrack* (24).
M2: What about the file made it interesting enough for you to publish?
CN: We'd never received an article concerning E911 service before, so originality was in itself a good enough reason. I was hoping that the file might help provide a better understanding of ANI (Automatic Number Identification). The most interesting part of the document was the glossary of terms.
M2: Was there anything there that would've made it possible for anyone to disrupt 911 service?
CN: Although the folks at Bellcore and BellSouth would like to have everyone believe otherwise, the simple answer is *absolutely* no. The article had no computer information, no access codes, and no telephone numbers to any system or office in the phone company. Every piece of information printed in *Phrack* concerning 911 was already publicly available in *many* places... not least of which are documents sold (at *very* low cost) to the general public by Bellcore itself.

M2: I got interested in your case as a violation of the First Amendment. Do you think that the Secret Service would have confiscated your equipment and put you on trial if that equipment had been a printing press instead of a modem?
CN: Maybe not. But I think it may have more to do with the fact that *Phrack* was a very small publication. Law and justice often seems to come down to: "how much justice can you afford?"

I think they tried to step on my First Amendment rights because they thought they could get away with it.
M2: There's been a lot of confusion about the agreement you eventually did reach with the government... the so-called "pre-trial diversion." Could you explain that?
CN: The pace of the trial was so slow that it appeared that I'd be at it for *at least* two more weeks, probably more. The financial expense was enormous, as was the emotional stress.

The pre-trial diversion allowed me to maintain my innocence and I had little to lose by agreeing to it. I'm supposed to speak with a pre-trial officer once a month to verify that I'm not in new legal trouble. That's pretty much it. The government can re-file the original charges against me if I'm arrested for fraud or computer related crimes over the course of the next year. I've kept out of trouble for roughly 20 years so I think I can handle one more.
M2: OK, you published an innocent document, which you had a constitutional right to publish. You demonstrated as much in court. The government essentially turned tail in the middle of the trial and fled. You're vindicated. Yet this episode has cost you and your parents.
CN: I was forced to sever ties with my closest friend during the course of events surrounding my case. I was suspended by my fraternity and nearly expelled. I was threatened with disciplinary action from the University of Missouri. My parents and sister were emotionally devastated. I had to drop over half my course load in school. I may never overcome the resulting financial grief. I've yet to see a final breakdown on my legal fees, but I'm told that my bill peaked at over $100,000 and that is not including the $8,000 that went to my first attorney in St. Louis or the expenses of travelling to and from Chicago. M

Parties interested in contributing to Craig Neidorf's defense costs can send their contributions to:
Katten, Muchin, & Zavis
525 West Monroe Street Suite 1600
Chicago, Illinois 60606-3693
Attn: Sheldon T. Zenner

Anyone who does decide to send in a check, should be sure to make a notation in the memo section that the donation is to be credited to Craig Neidorf's account. Craig would like to express his sincere appreciation for any contributions. •

If a system allows access to one valid user, then it's possible to break in. Just like with a room: if it has doors, you can break in

clude your data—the balance sheets, the payroll records, corporate data, and more, especially if you're a computer company. Having a virus in your core on a dead-man's switch might not be a bad idea. Whoops, here comes a hostile takeover. Just let them know that if they don't cease and desist, you'll suicide the computer system.

I Have Seen The Future and it is Unstable:
Right now, if a virus goes off, you have backups, or at least paper. But soon, we'll be dealing with things that are too data dense to make backup viable. It's getting to the point where some dataspaces are so sophisticated that they're not representable in any form outside themselves. Then what will you do when your data dies?

On Access Security:
As Uncle Sam is fond of telling me: "Integrity is like a balloon. No matter how good the rubber, the air still goes out the hole." If a system allows access to one valid user, then it's possible to break in. Just like with a room: if it has doors, you can break in. Data security is best, using a good cryptographic scheme and erasure prevention. Forget access security. It doesn't work.

On New Viruses:
I just worked out a hardcore worm. A nice feature of current networks is that there are networks hanging *off* of networks. This worm breaks into a computer and seeds itself into all the component systems. Once seeded, the worms mutate into a specific configuration and grab any new resources available on each machine. Then the worms bounce back out into the main network. The growth rate with mutations would allow for a few hundred new worms, minimum, on the network per hour. Considering that the Internet worm crippled so many machines for so long without trying, a few thousand distinct worms would shut the whole show down. Goodbye banks, goodbye telephones, goodbye welfare checks. How much money do you carry around in your wallet? It might be all you have left.

Tech Talk

On Virtual Reality:
Let me tell you a parable. Remember Smalltalk? Smalltalk was created for two reasons: to prove that computation could occur simply by manipulation of objects and communication between objects, and that the process of computation should become visible. Great goals. But the industry couldn't figure out what to do after this was accomplished, it was too big a conceptual leap. It took the concept of a graphical user interface (GUI) to make the concept accessible to the folks at home, and then comes the sudden onslaught and acceptance of object-oriented systems. The concept of 'cyberspace' needs the same intermediate step. There has to be perceived value for the everyday user on an everyday box to help this concept get moving. Right now, nobody has the faintest clue as to how to deal with data in three dimensions. You have to walk before you can run.

On Intelligence:
The first person who invented a bow and arrow was really amazing. Not only did this individual make a great conceptual leap, but also helped others along. Intelligence is the communication of processed information. This means 'value added,' boys and girls. It means that people should stop sitting on their brains, and stop trying to make money by shuffling paper, and instead get out there and *do something*.

People to Watch:
Pay attention to what these people do, since they're pushing the envelope... Nicholas Negroponte and the crew at the Media Lab, Scott Fisher and Brenda Laurel with their projects in Telepresence, Eric Gullichsen (who will find his way to market with something one of these days), Todd Rundgren, Mitch Kapor with his advocacy of software design, Danny Hillis at Thinking Machines, Eric Drexler and his nanodevices, and the mysterious stranger in the garage with a new product that nobody expects.

And me, of course... M

On Cliff Stoll:
(Author of *The Cuckoo's Egg*, a book chronicling his keystone kops adventures with the intelligence community in pursuit of a German computer hacker.) Stoll, if you ask his friends, is a mediocre astronomer and a mediocre computer person. I think they're being generous. Cliff is unconscious. He sees the world only as it affects him. Because of what he did, a guy I knew ended up dead, burned to death on a riverbank. Cliff needs to grow up and try to grok the big picture. [ed. note: the computer hacker in Germany who was arrested by the authorities was, according to Synergy, selling the Soviets information which would have been available 'over the counter' with a good research service. 'Hagbard Celine'—as he called himself—showed up immolated on a riverbank, an apparent 'suicide'.]

On the Debate Over the Term 'Hacker' or 'Cracker':
The people who are debating over the terms hacker and cracker oughtta just get a life. The only difference is that one is employed. Or owns the company.

On Modern Justice:
Is it a criminal act to read something on a hacked computer? First, under common law, the object of a tort is to compensate the 'victim' for 'damages' caused by the action of the defendant. After establishing intent, always a nebulous concept, we have to establish actual 'damages' caused. Simply reading a file is potentially bad. On credit services like TRW, pulling someone's credit report can hurt the credit rating of that individual. What about using the information gathered from browsing to run an 'insider trading' scam? Buy stock or short it depending on what you read in the corporate mail system.

What we need here is what the justice system was set up for *in theory*: an individual analysis of each case as it pertains under the law. What we've ended up with *in fact* is a system that *extends* the law based on the analysis of the individual case, the system of precedents. It's the cart before the horse. It's also a damned stupid system.

On Criminal Evidence:
Remember the phrase "beyond a reasonable doubt?" With the wonders of the modern age, this is the end of the current legal system. No witness testimony is valid, sound recordings are manufacturable, photos are manufacturable, video is manufacturable. The jury isn't a judicial process, it's the new audience. The rules of criminal evidence are out of date, killed off by the microchip. I can see a future trial. The Defending Attorney comes into court armed with a recording of the Judge committing the crime, photos of the Prosecuting Attorney committing the crime, and a video of members of the jury committing the crime. It could easily be done. Don't you just *love* multimedia?

Viruses & Nightmare Scenarios

On Viruses:
Welcome to the H-Bomb of the Information Age. The ultimate lever action: remote, numerous, targetable, anonymous. It makes certain individuals just as powerful as government agencies. Or governments. Big deal. People oughtta just grow up instead. Viruses raise an important issue though... freedom through personal empowerment. What if we all had H-Bombs? Why should that big abstract organization known as government have one and not you? Do you trust them more than yourself? What if everybody had a weapon? What if we all had to take responsibility for ourselves and our actions? The only discipline is self-discipline.

Blackmail: for Fun and Profit
The blackmailer writes a worm that insinuates itself into a system and automatically encodes and decodes all access for the users. One day, maybe a few months after it comes in, it commits suicide and erases itself. All your files, all your data, is encrypted, and you don't have the key to make sense of it. But if you pay $$$ to the perpetrator, surely they will give you the key. If the worm is written using a public-key crypto system, it doesn't even matter if you catch a copy, you still can't decode your data on your own.

How Not to Play Fair in the World of High Finance:
Your corporate assets in-

Goodbye banks, goodbye telephones, goodbye welfare checks. How much money do you carry around in your wallet? It might be all you have left

Welcome to the H-Bomb of the Information Age. The ultimate lever action: remote, numerous, targetable, anonymous

I read a book a day. I listen to music, compose music, watch movies. I write screenplays, read magazines, give interviews. I talk on the phone for interaction—being the interactivist. And when I crack into computers, I browse and read peoples' mail, papers, notes, programs, etc. I'm an enquiring mind and I want to know. This is a *real* issue. I want to learn and *they* want to impose 'need to know' on everything.

POLITICS LAW & SOCIETY

ON MONEY:
You know who the most important President was? Richard Milhous Nixon. You know why? Because he took us off the gold standard. Once upon a time, money in a bank had to be related to a real world object. Arbitrarily, this was gold, since it was rare and since most people are packrats. But suddenly, the governor was removed. Money was just a bunch of bits and bytes in computers. Money became the first exploration into cyberspace. This is why the economy is messed up. This is why banks are messed up. This is why computer crime is growing exponentially. This is why the damage that can be caused electronically is so much greater. Because we stopped using reality as the 'acid test' for what was represented in our machines.

ON 'OPERATION SUN DEVIL':
Once again, the cowboys in the Secret Service have gone off half cocked. The telephone company gets them all riled up and they start loading the shotguns and Uzis. The chain of events looks something like this: a telephone switching center shut itself down, taking a lot of other switching centers with it. For hours it stopped telephone service, costing an immense amount of money. There was a bug in the revised code running the switch, a bug that was just waiting to go off and cause this problem. Now the phone companies acknowledge the bug is their fault, but they also believe that the original switch may have had some help shutting down. There is no audit trail to use as evidence, so that's pure speculation on their part. So they got scared because they finally realized that what I've been telling people for years is true—one person *can* shut down the whole phone system. So they call the stormtroopers at Secret Service and get them all rabid, and the rest is history. Except that on the phone company's part, it's not history, it's histrionics. They were scared not by the actions of a real person or group, but by the implications of their own sudden realization.

ON THE ELECTRONIC FRONTIER FOUNDATION:
I think that John Barlow, Mitch Kapor, and Steve Wozniak are good guys, but I have some doubts about their methods. The 'education' they want to bring regarding the issues is more like preaching to the choir—the only people listening right now are those who already understand the issue. And if they try to get the government involved, they'll make matters worse by validating more legislation. I would happily approve if they went strictly after the removal of *all* government involvement. But they're only increasing the FUD—Fear Uncertainty Doubt—factor. I can't see any positive consequence of remaining in or attempting to alter the existing political system. We share the same desire for freedom, but they believe that we still have a workable system, or—I might say—that politics is still workable. They seem to want to approach all the important issues as Constitutional ones. I think they should read the *Anti-Federalist Papers* for a good set of reasons why that'll never work. Remember, the Constitution was a mechanism of Big Government, with the Bill of Rights hastily added on years later. The government is *not* your friend.

Have you read Atwood's *The Handmaiden's Tale*? In the book, a Religious Right takes over the country. Since most women were infertile, the 'power elite' forced women who were fertile to bear their children. The 'radical' women, women who had had abortions, or who took a feminist stance, were sent to the wall. I think the book, an outstanding piece of literature, shows the real issue: data that you and I don't want seen by *anybody*, let alone a government official (hostile by definition), is there for the taking in computers across the country. I think that personal data, like credit reports or medical records, should be encrypted, with only the owner of the information (the person the data is about, not the owner of the machine) in possession of the key. A person wants to read your credit report? Great, *you* decide to give them the key.

Synergy Speaks:

Goodbye Banks, Goodbye Telephones, Goodbye Welfare Checks

Michael Synergy may be the first person I ever met who actually described himself as a cyberpunk—way back in the days of Reality Hackers. *"Do you want an article on how to stay free of computer viruses?" he asked. A couple of weeks later, he was up at the* RH *office. "Do you mind if it's a little subversive?" We immediately made him an assistant editor.*

Michael is probably the most explicitly political (anarchist division) of the young hackers. While the people in and around the Electronic Frontier Foundation are trying to gently reassure the body politic that the onslaught of information technology is not *a threat to the stability of the system, Synergy will tell us how it* is *indeed an assault on all fronts. His message is simply "Surrender!" What follows is a pastiche of comments he made at a conference called* Forbidden Knowledge in the Technological Era *and notes added later by Synergy in response to questions he was asked about his talk.*

R. U. Sirius

INFORMATION

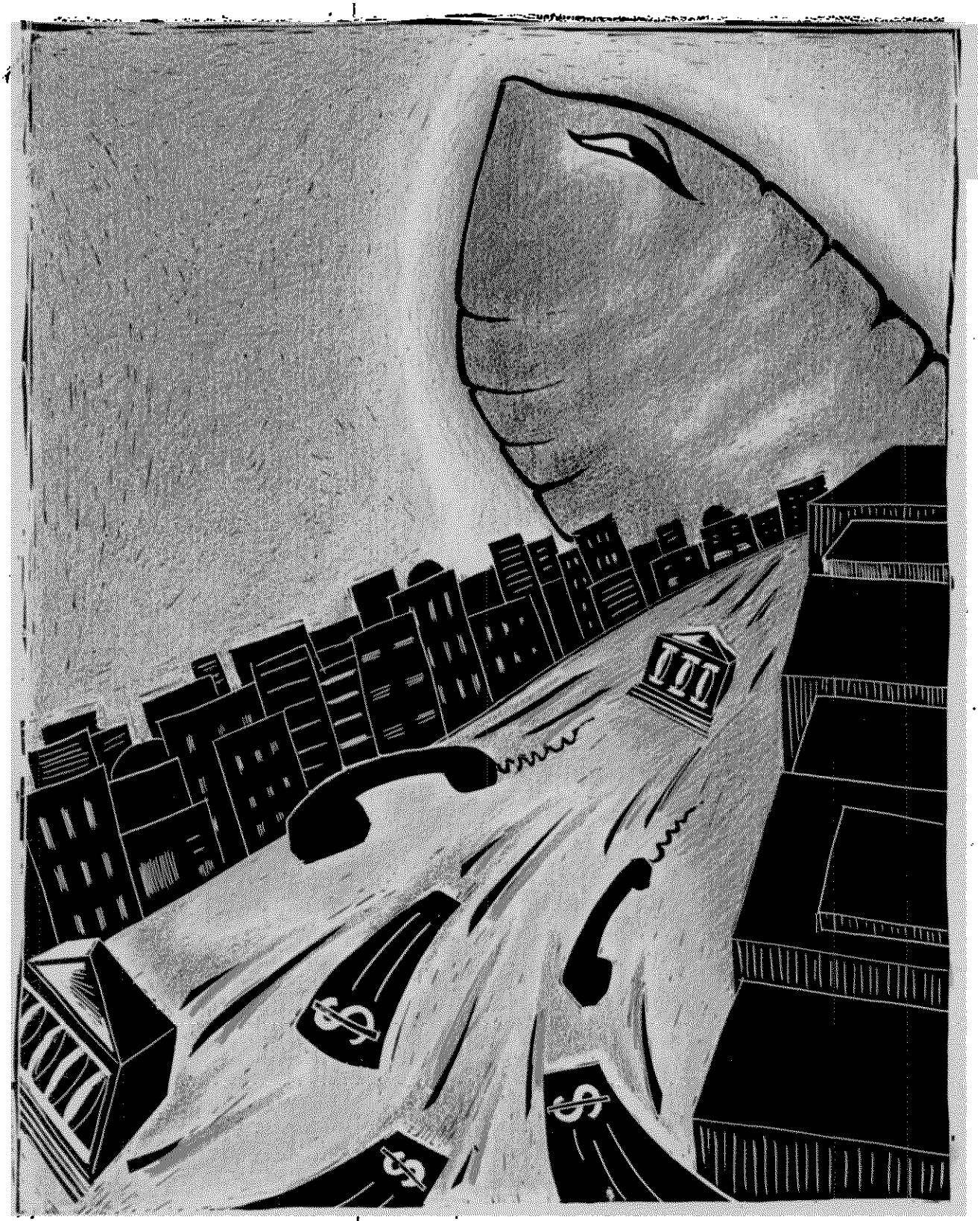
ON INFORMATION
Information is true capital. I can't eat gold. I can't use it to heat my house. I can't use it to cure my cold. It's only a medium of exchange. Exchange for what? Time. Skill. Information. The information economy is here and now. Ever hear the old Eskimo proverb? "Give a man a fish and you feed him for a day, teach a man to fish and you feed him for life." Education and freedom of information are the path to the future. Some of us are already trailblazing it. It's fun living on the edge.

ON THEFT OF INFORMATION:
Information can't be stolen. Unless they've come up with something new, phenomenologically speaking. If I tell someone a fact, I still know the fact. Property laws were set up to handle tangible objects. We're dealing with raw data, information, the stuff of dreams. The whole system to handle 'ownership' is obsolete. Any system that gets set up to handle 'ownership' will already be obsolete. In a world where you can copy information, leaving the original intact, and wind up with a perfect copy, the debate over ownership is over. Remember the old joke about the drunk and the fool? How do you tell which is the drunk and which is the fool when you see the argument? Easy. Wait until morning. The drunk will sober up. The other guy is the fool, since only a fool would argue with a drunk. Only fools are arguing over 'ownership' of ideas.

ON INTELLECTUAL PROPERTY:
Speaking as an inventor with some pretty sexy items both on and off the boards, this is a near and dear topic. I work hard, have a brilliant (if I may be self-serving for a moment) idea, I should make money off it, right? Certainly I should, by getting to market first and still working my ass off to come up with yet a better idea. Let's cut the crap of 'one good idea per company, OK?' Competitive edge means *staying* at the technical and marketing cutting edge, not bashing the competition with patent suits.

ON THE SPREAD OF INFORMATION:
Once the word is out, you can't stop it. When I tell someone a fact, I can't be sure if the person will keep it to themselves or whether it'll end up front page news. Non-disclosures are shit, totally unenforceable. You can't tell who leaked what, when, where, and to whom. Let's give up trying.

ON BROWSING:
I am an information addict, a sensory junkie. I want stimulus, and I want it now! So what do I do?



Photograph by Bart Nagel

John Barlow

setting effect regarding digital media. So we'd have a fundamentally limited application of the Constitution to the world of bits and bytes. And if you think about it, it's *all* pretty much taking place now in bits and bytes, at least at the developmental level. If you can restrict free speech just because it happens to occur in a magnetic medium, then it's all up for grabs.

M2: We're faced with the possibility that the Bill of Rights will be left behind with hot lead.

JPB: Much of the Bill of Rights is already gone. I was shocked to find out that the Fourth Amendment had pretty much disappeared since the last time I'd looked. I called up some lawyers regarding one of these cases and said, "As I read the Fourth Amendment, this is unreasonable search and seizure to a 'T'." And they said, "Well, you've got to understand what's happened in terms of precedents on Fourth Amendment issues. We've basically lost it." It's the death of a thousand torts. We're still pursuing it though, because most of these Operation Sun Devil search warrants were unsigned, sealed, and completely broad. They just said, "Get everything that has electronics in it and get everything that has magnetism on it."

The Fourth Amendment is supposed to prevent the authorities from taking anything from you that doesn't have a direct instrumentality in the alleged crime. So they know what a gun is, right? But they don't know what a computer virus is or where it might reside in 25,000 disks, so they take them all.

A New Market for the Secret Service

JPB: The Secret Service wants to expand into a new market. The old market—which contrary to popular belief wasn't protecting presidents, it was busting counterfeiters—moved offshore. So in order to have a reason to exist as an organization with a budget—to feed itself as a critter—they had to find some new food. They've gone into computer crime and they're doing a rather bad job of it. They're getting terrible advice from the telcos, who are using the Secret Service in much the same way that the FBI is being used by Apple. If you call the telcos and ask them a question about computer crime, you'll find yourself talkin' to somebody from the Secret Service. The Secret Service agents showed up at all these busts with telco security people. You couldn't tell them apart.

See, the government is now grinding to a complete halt, and what's actually running stuff—to the extent that things are getting run—is corporations. They're mediating the economy. They're passing the goods and services around. *And* they're doing all the control stuff, they're managing the consciousness, and now they're moving into law enforcement.

RUS: That's very much the cyberpunk vision.

JPB: Yeah, exactly.

Move the Homesteaders In

M2: So what specific areas is the EFF getting involved in?

MK: We think it's really important to do something about improving people's access to the public network. Electronic mail and conferencing has substantially expanded the scope and reach of our contacts and our community. There's one catch. You kind of have to be a Unix weenie to be able to use those particular tools to full capacity. We need to lower the barriers to entry and let ordinary folks participate in this worldwide discussion.

JPB: What we're doing is "civilizing the digital frontier." Cyberspace—or whatever you want to call that region that is defined by electronic communications and information—is presently inhabited almost exclusively by mountain men, desperados and vigilantes, kind of a rough bunch... oh, and Unix weenies [laughter]. And as long as that's the case, it's gonna be the Law of the Wild in there. And it's going to continue to have this extremely uneasy relationship with the rest of society which is growing more and more dependent on it in a very material way. You can't believe the number of things that you do every day that involve activity in cyberspace.

MK: When you use an automatic teller machine, for instance.

JPB: Whenever you make a financial transaction, really, it involves electronic data representing money. So we feel that the way to minimize anxiety, and to make certain that the freedoms we have in the so-called real world stay intact in the virtual world, is to make it inhabitable by ordinary settlers. You know, move the homesteaders in.

Individuals who work in institutions are no longer individuals. It's like slime mold

WELL, and it reverberated very deeply within me because it enabled me to come to terms with my visit from the FBI, which had happened earlier. It was, of course, a very disturbing experience that I hadn't been able to process. So I just sort of repressed it. It had sort of been lying in an undigested state in some empty chamber of my brain.

My experience was remarkably similar to John's. They were asking a lot of the same questions. It was hard work just getting them to understand the sequence of events I described here earlier. You know, "I had this diskette and I looked at it and I saw that it was Apple source code and I sent it back." And *that* took a couple of hours to get across. It was exhausting. And I felt bad, because it was clear to me that they weren't in a position to do what they were supposed to be doing.

I sensed danger. When you have a powerful force with a charter and a history and they're fundamentally lost—they don't understand the territory they're in at all—it's a recipe for disaster.

JPB: Meanwhile, some other things had been happening that weren't directly connected to this case, but were certainly connected to the underlying cause. I had been part of an online *Harper's* magazine forum on computer hackers. In the course of this, I'd met these cracker kids from New York and elsewhere. They were young and brash, and there had been a kind of nasty symmetry that set itself up over the course of the conference between the old techno-hippies and these young sort of digital skateboarders. It culminated in one of them downloading my TRW file with my credit history—with the implication that he could change it if he wanted to...

MK: Which wasn't true.

JPB: But I didn't know that. I was looking at life without credit. Pretty scary.

So I E-mailed this kid and said, "We've just exceeded the bandwidth of this medium. Why don't you give me a call? And I won't insult your intelligence by giving you my phone number." He called me up about 20 minutes later.

The kid that I encountered on the phone was not at all the kid who'd been strutting about in full digital regalia on the WELL. He was a kid, you know? Smart, brash, New York street-kid, but not dissimilar from what I'd been at his age. And I got to know his colleagues. They were unquestionably inclined to trespass, but I tend to think that's sort of a testosterone-based endeavor that has long been with us.

I met them in New York, and I didn't find them to be any particular threat, in spite of their willingness to go where uninvited. But at a certain point I found out that the government had moved in on one of my young colleagues and had smashed down his door one afternoon while he was out and held his 12-year-old sister at gunpoint for an hour until he showed up.

I heard about this before I had my visit from the FBI and I thought, "Well, I don't know what they did. They're probably much worse than I thought." So I didn't do anything about it until I had the visit from the FBI.

MK: Yeah, and I came along and talked to John, also. I just thought that these kids should have a good lawyer. I saw that there were powerful forces moving against them. My sense of fairness dictated that they have adequate legal representation to protect their rights. That's where it started.

M2: What does a software multimillionaire feel in common with these "digital skateboarders?"

MK: You know, I'm the same digital skateboarder that they are, only I'm a little bit older and have more life experience. I was sort of a smart, nerdy, somewhat undersocialized kid. If I'd had the opportunity to do what they'd done, I probably would have done it.

JPB: A very important point that we have to make over and over and over again is that the Electronic Frontier Foundation is not a crackers' defense fund. Trespass is, and should be, against the law for a variety of reasons, not the least of which is that you can get in there and inadvertently create mayhem.

Robert Morris [creator of the Internet worm] is an excellent case in point. Morris wanted to do something that was really kind of cool. I wish he'd succeeded. He wanted to map the net. The Morris worm was like an explorer. It was going to go around to every node on the net and report back in and tell you just how big this sucker was. Which is something that nobody knows, right? It's a cool thing to do. Somebody ought to do it. Trouble is, he screwed up. His worm wasn't well-written, so the effect was viral rather than exploratory.

That's why it probably ought to be illegal to trespass. These people are entering into sensitive places where things are fragile. But it's also important that you don't go around busting joyriders for grand theft auto. Trying to impose a million-dollar fine and thirty years in jail on them just because they've trespassed digitally rather than physically is completely out of scale. That has to be dealt with.

Where'd the Fourth Amendment Go?

M2: At the same time that your effort to bring rights and justice to the electronic frontier is happening, there's an immense tide of repression going on in all of the old traditional realms and modes of communication.

JPB: No. If you check it out, you'll find that print and speech are still pretty well protected. Where you're running into trouble is in every other medium. You're running into trouble with records, CDs, photographs, art, broadcast media, digital media...

We lost radio and television in the 20's and 30's... not a big civil libertarian time. They said, "Well there's a limited amount of bandwidth so we've got to regulate it. And in regulating it, we've got to make certain that it meets the requirements of a wide audience."

RUS: Could the Electronic Frontier Foundation possibly step back a couple of decades and try to deal with that situation?

JPB: No, because of the way in which the legal system works. It's all organized by precedent. You build up a body of case law over a period of time and pretty soon it has the same authority as it would if it were part of the Constitution. I don't think there's a damn thing we can do about the broadcast media now. And what scared Mitch and me is that we could have cases that would establish the same kind of precedent-

But *now* we're talking about that dislocation that occurs when an *entire* society looks up and finds that it doesn't know where it is, and it doesn't know how anything works anymore, and doesn't know how to deal with the reality that most of the standard, nurturing concepts that have managed to provide for us since the Neolithic Age—things like place and embodiment and community— are basically suddenly gone.
MK: I like John's one-sentence definition of cyberspace: "the place you are when you're on the telephone." It brings it home to people.
JPB: As a society, we're leaving the landscape and moving onto the map, without paying much attention to the process or the destination.
M2: Mitch, you've gone from being an acid head in the 60's to being one of the new heroes of digital capitalism. What's the view like from there?
MK: Well, before I was a digital capitalist, I taught meditation. Then I was a counselor in the psych unit of a local community hospital. I have a Master's degree in counseling psychology. So I've been all over the map. I just kind of fell into computers. I didn't set out to be Bill Gates. Bill Gates set out to be Bill Gates. My perspective wasn't shaped by needing to build a big company and make a lot of money. In a nutshell, I started this little company called Lotus and made this software product that several million people wound up buying. The little company turned into this enormous thing with thousands of employees making hundreds of millions of dollars a year. And it felt awful to me. So I left. I just walked away one day.
M2: Did it occur to you, when you walked away, that you were turning that large capitalist organism loose to do its will and...
JPB: It was already a lot bigger than he was.
M2: But if your values were offended by it, wasn't there some way to turn it around?
JPB: You're still stuck in the notion that people run these things and that they don't run themselves. Companies become their market, not their maker. Lotus is a beautiful case in point. To say that Mitch could have somehow directed Lotus in some benign way is like assuming a coral polyp can run a reef. Large businesses are collective organisms.
M2: How are they driven?
MK: They're not! That's something that John and I both keyed in on. We have this assumption that because something exists and acts, it has some central controller, some little homunculus inside it that makes the thing go. But physics is dead as a model for organizations. Biology is in the ascendant. And if you study biology, things are very decentralized, very distributed. You get emergent behaviors coming out of the workings of a whole bunch of little pieces. Each piece is pretty dumb. Organizations are like that. Still and all, I agonized over my responsibilities toward Lotus before I left.
JPB: Individuals who work in institutions are no longer individuals. I mean, there's a big difference between a solitary wasp and a wasp's nest. It's like slime mold. Institutions are paramecium-style, one-celled organisms, mostly. When it decides that it wants to cover some country because conditions are changing, all the local slime molds get together and create an organism that grows stalks with eyes on the ends, and grows cilia to move with, and suddenly it's a critter.
R. U. SIRIUS: It's called "grexing."
JPB: Yeah! It's an animal then. It's no longer a one-celled organism. And then it goes someplace and devos. It goes back down to its original constituents. This is really the perfect metaphor for what a corporation is. And to say that the individuals inside that corporation are individuals when they're acting in their corporate form is like saying that slime mold is still a whole bunch of slime mold cells. We still have this sort of Newtonian, causal, deterministic notion that organizations are machines. The CEO is up in the wheel house and there's a direct connection between the chairman's desk and the rudder.

By the way, there's also this lingering assumption that there's some disjuncture between being a digital pioneer and being an acid head. It's my perception, on the basis of having interviewed a lot of the first wave, that this is actually quite a common phenomenon.
M2: In that case, is there a reaction of old corporate America against new corporate America?
JPB: Well, the reaction is to meet it, to infect it with itself, and to create—through the use of itself as a market—a perfect replica of what was pre-existing.
M2: Apple is becoming like GM.
JPB: Oh, I think Apple's a lot *worse* than GM because Apple is still clinging to a mythology that just gets in the way. I mean, if Apple could just kind of settle in and *be* GM, everybody there would be a lot happier.
MK: It lacks the comfort and self-assurance of a mature organization which, no matter how much you might disagree with its values, has a degree of predictability. Younger organizations that are still in the throes of violent organizational psychoses become very unpredictable.
JPB: Apple is like the Chinese Cultural Revolution conducted by people in three-piece suits. Any corporation has a totalitarian quality, but people work for them because it's supposed to be safe, right? You give up your mind but get the benefit of the collective immune system that will protect you against the slings and arrows of individual fortune. So IBM takes care of their employees. They rarely fire anybody. They've got a nice retirement plan... they take care of their employees. Apple exercises much the same kind of totalitarian control over its employees and offers them *none* of the benefits. They have no retirement plan, period.
MK: Instead they offer up the vision that they're doing something to make a difference in the world, which *used* to be true.
M2: So who benefits?
JPB: That's kind of like saying, "What good are mosquitos?" Mosquitos arise because there's room for them in the ecology. Corporations arose because there was an ecological niche that was created by a lot of things, modern telecommunications being one.
M2: So Mitch, how did you end up still thinking for yourself?
MK: I can't help it.

A nasty symmetry set itself up between the old techno-hippies and these young digital skate-boarders

THE ORIGIN OF THE ELECTRONIC FRONTIER FOUNDATION
MK: I read John's account of his visit from Agent Baxter on the

"That's what led us to the whole metaphor of the 'electronic frontier.' All of the good stuff that we know about is sufficiently difficult that only a few pioneers, some outlaws, maybe a few vigilantes, and early settlers, are comfortable.

"Out on the frontier, there aren't established laws or practices," Kapor continued. "We're making it up as we go along. But ultimately we've got to civilize the frontier. We have to allow ordinary folks to come and settle. We need to build the equivalent of railroads, because if we don't take the lead in doing it and it happens by itself, it's probably not going to come out in a way that any of us will really like."

The Electronic Frontier Foundation began when Kapor, after reading an article Barlow had written (on the WELL computer network) about his visit from Agent Baxter, visited him in Wyoming one afternoon. "We realized that this wasn't so much a planned and concerted effort to subvert the Constitution," said Barlow, "as the natural process that takes place whenever there are people who are afraid and ignorant, and when there are issues that are ambiguous regarding Constitutional rights.

"Whenever there's a new medium, there's always a struggle to find out whether the Constitution is going to apply to that medium, whether or not the first amendment will apply. There's now a struggle under way to find out whether free speech can be expressed in bytes and bits. And that's basically what the Electronic Frontier Foundation is about.

"We're looking at a whole range of things dealing with future shock, the anxiety of society at large toward computers, the particular anxiety of society at large toward hackers, and what I like to call the learning curve of Sisyphus— which is what happens when you've got a technology that develops faster than anybody's ability to learn it."

Shortly after the EFF reception in Silicon Valley, R. U. Sirius and I met with Barlow and Kapor to learn more.

- David Gans

An Acid Take on Digital Capitalism

JOHN PERRY BARLOW: On May Day of this year I got a phone call from FBI Agent Baxter down in Rock Springs. I said, "What do you want to talk to me about?" And he said, "Well, I'll tell you when I get there. I've got a stack of papers." And he *did* have a stack of papers.

MONDO 2000: Wait a minute. So the FBI calls you and says we need to see you...?

JPB: Well, yeah. That happens.

M2: And you thought it was neighborly to invite 'em over and hear 'em out?

JPB: Well, I thought it was probably closer to my best interest to do that than to tell him if he came I'd kill him.

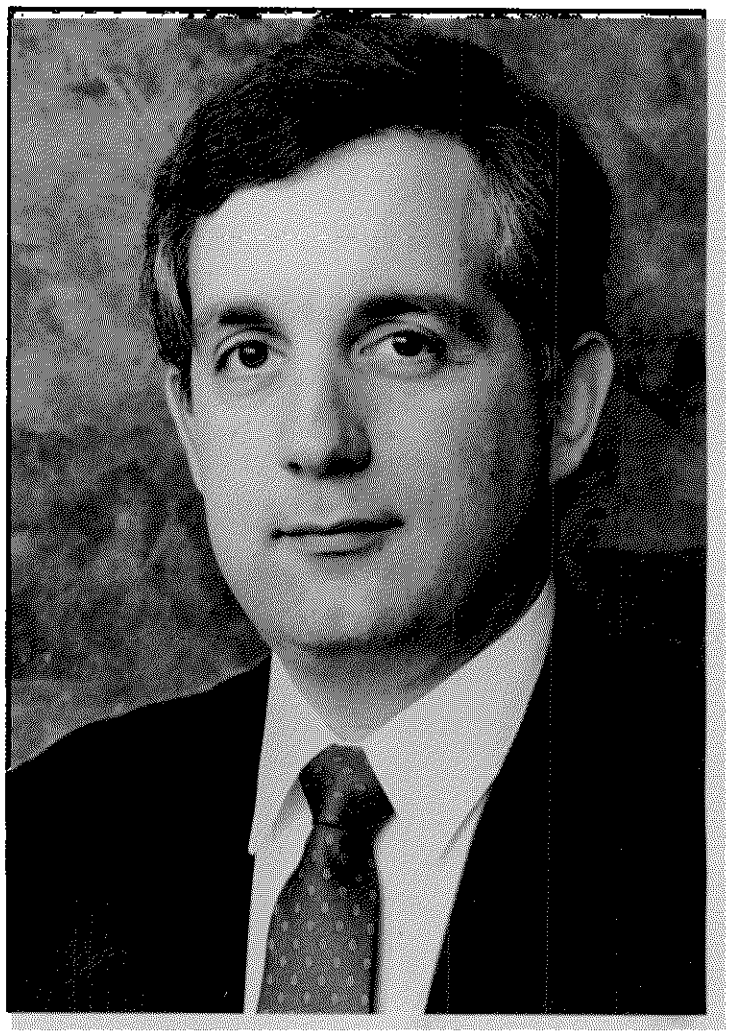
So his stack of papers was about something called the NuPrometheus League and they'd taken a little snippet of Apple's ROM code and had sent it to, among other people, Mitch Kapor. Understand that Apple basically sells ROM code. I mean, they're commonly thought to sell machinery, but what they really sell is the software that's on the ROM chip inside that machinery. That's the holy mojo that makes a Macintosh a Macintosh. So Apple freaked. And they invoked the awesome forces of the FBI which, for reasons having to do with corporate culture, is closely tied in with Apple's security company. There's a revolving-door policy between the FBI and Apple's security contractor.

M2: Mitch, the person or persons who call themselves the NuPrometheus League sent this piece of code out to a bunch of people, including yourself. Why did they do that and what was it?

MITCH KAPOR: I don't have the faintest idea why they sent it to me! [laughter] I just stuck the thing in the drawer, because it was an unlabeled diskette and I was afraid of viruses.

JPB: [laughing] A disk that says "Apple Source Code" on it, it's kind of like, [seductively] "Put me on your computer."

MK: But then the story hit the papers that somebody had actually taken a small, not terribly important piece of the source code for something called 8-bit color QuickDraw and sent it out. So I looked at it again, long enough to determine that it looked like Apple source code. Then I sent it back to Apple and I thought that was the end of it. Several months later I got a call from the FBI. It was actually before John's visit.



Mitch Kapor

M2: Did you guys already know each other?

JPB: Yeah. I'd interviewed Mitch for *MicroTimes*. We became friends in the the first 30 seconds. It was one of those cosmic recognition experiences. Here was somebody else thinking some of the peculiar thoughts that I'd previously thought were mine alone... coming at it from a completely different angle.

MK: We're both interested in dislocations of consciousness because we think that's central to understanding how weird the world is—how everybody's mind has gotten genuinely bent, especially by technology... especially by digital media. John, of course, is in the process of writing a book about this.

We also had a common set of experiences in the 60's involving what I—when I speak to straight business audiences—charitably refer to as recreational chemicals, which contributed to a fundamental outlook.

M2: Ye olde acid heads' league...

JPB: Right! You got it, buster.

Civilizing the Electronic Frontier

An interview with Mitch Kapor & John Barlow of the Electronic Frontier Foundation

by David Gans & R. U. Sirius

Space may be the final frontier, but there's at least one more earthbound arena ripe for socio-political struggle before it's time to start worrying about Martian mineral rights and the exploitation of Betelgeusian guest workers. Electronics.

The United States Constitution and the Bill of Rights were created in the era of hand-set type, before the telegraph, telephone or broadcast media. Each new wave of technology has pushed at the boundaries of liberty and tugged at the coattails of authority by enabling more rapid and comprehensive dissemination of information. There's more communication taking place outside the purview of centralized authority as well as more light shed on the inner workings of government and business. For a long time now, drugs have been seen by the government as the main threat to its control of knowledge and information. Since the 1960s, the particular species of vegetable that I sometimes carry in my pocket could, if found by the wrong person, land me in jail and lose me my property.

Now it's my disk drive.

The advent of personal computers and modems, coupled with the immense penetration of the telephone network, threatens the hegemony of the government/corporate paradigm by empowering millions of individuals. In the 90's, thanks to desktop communication, it is no longer necessary to "publish" "revolutionary" documents in the old sense of the word. Information can be propagated across thousands of miles in all directions in a matter of moments and it can't be stopped short of dismantling the entire telephone system. This genie can never be put back in the bottle. But that hasn't discouraged the Enforcement Community from doing its saurian best to try.

Acting on requests from certain corporations, the FBI and the Secret Service—armed with vaguely worded warrants—have raided businesses and homes of private citizens and seized tremendous numbers of computers and related items, with very few corresponding arrests. The language on the warrants was vague because even in the rare case when the government knows what it's looking for, on the electronic frontier, it probably has no idea what it's looking *at*.

So here I am watching a beautiful July sunset from the deck of a home overlooking Silicon Valley, participating in a good-natured but urgent gathering sponsored by the two founders of the Electronic Frontier Foundation, Mitch Kapor and John Barlow. Their alliance began with an arguably pointless act: someone, probably an employee of Apple computer, "liberated" a relatively minor piece of Macintosh operating code and sent it, over the signature of "NuPrometheus League," to a number of industry figures. Mitch Kapor, founder of Lotus Development Corporation, was one of the lucky recipients. Kapor immediately inferred that the mysterious floppy was nothing more politically significant than an attempt to infect his computer with a virus, and sent it back.

John Barlow, Grateful Dead lyricist and writer about things cyber, didn't receive a floppy disk from NuPrometheus, but because he attended the fifth Hackers Conference in October 1989, he *did* receive a visit from an FBI agent regarding NuPrometheus. Investigating agent Baxter evinced a woefully inadequate grasp of the matter he was investigating.

"He referred to them as the New Prosthesis League," Barlow told the assembly, who howled with laughter. "He was looking for something called 'the ROM Code.' He didn't know what a ROM chip was, he didn't know what code was, he didn't know whether it had been stolen or what exactly had happened to whatever it was.

"And I realized that what we were looking at was a microcosm of a whole set of things that could begin to happen with government and society and computers. And it was just a little pinpoint of future shock that was going to blow up into something big and ugly if we weren't very careful about how it got managed.

"A few days later, I found out that this process was well under way in the Secret Service," Barlow continued. "They had come up with something called Operation Sun Devil and they were breaking into the homes of teenage kids, rousting them up in the middle of the night, coming in with guns, sledgehammers and, I assume, no more knowledge of the situation than Agent Baxter had when he showed up at my home in Pinedale, Wyoming."

"It's simply beyond the reach or grasp of 99.9% of the people today" Kapor added, "given the relative immaturity of the technology and the fact that there hasn't been a concerted effort made from within the industry and the academic research community to make the stuff usable. And if it's not made usable, there's going to be an increasing gulf between the information haves and the have-nots.

Illustration by Eric White

May 1, 1990: John Barlow visited by FBI Special Agent Richard Baxter. Baxter is investigating the NuPrometheus League which he calls the "New Prosthesis League."

Barlow—who is an exquisite writer as well as the Grateful Dead's second poet—writes up his bizarre Alice-Through-the-Looking-Glass experience with the FBI man the following day and posts it on the WELL, a bulletin board run by the *Whole Earth Review,* under the name "Crime and Puzzlement":

"Poor agent Baxter didn't know a ROM chip from a vise-grip when he arrived, so much of our time was spent trying to educate him on the nature of the thing which had been stolen. Or whether "stolen" was the right term for what happened to it.

"You know things have rather jumped the groove when potential suspects must explain to law enforcers the nature of their alleged penetration."

The strangest and most laughable revelation in Barlow's piece is that the FBI had it as a matter of record that John Draper aka Cap'n Crunch, the famous phone phreak mentioned in the first paragraph of this piece, is the CEO of Autodesk. For those unfamiliar with the world of hackers and computer programmers, this would be somewhat akin to them believing that Bart Simpson is the President of Fox, 'cept Draper wasn't even *working* for Autodesk anymore. Remember. This is the Federal Bureau of *Investigation* we're talking about here. A slow 9-year-old with a telephone and 15 minutes to investigate would discover the information to be ludicrously false. This is kind of a scary comment.

May 4, 1990: Robert Morris Jr. sentenced to a $10,000 fine and 400 hours community service for unleashing the Internet virus.

May 9, 1990: The Secret Service and Prosecutors in Phoenix Arizona announce 28 new raids under Operation Sun Devil. In three days, 28 search warrants are executed in 14 cities; 42 computers and 23,000 disks were confiscated. Only four arrests are made. Most of the raids are targeted against credit code abusers and similar minor players. However, confiscations of BBSs contribute to an overall chilling effect on electronic expression and association.

Late Spring 1990: PC software pioneer Mitch Kapor, independent rancher/Grateful Dead songwriter John Barlow, John Gilmore, pioneer at Sun Microsystems, Apple co-founder Steve Wozniak, and others form the Electronic Frontier Foundation: to protect freedom of speech and expression at the leading edge of computer technology and electronic publishing.

July 23, 1990: Neidorf trial begins.

July 27, 1990: Neidorf trial ends. Defense shreds prosecution case and the trial ends with a Southern Bell employee revealing that the allegedly illicit and dangerous $79,000 document was, in fact, available to regular Southern Bell consumers for less than $30. The Government drops the case in exchange for a promise from Neidorf to stay out of trouble for a year. The price of victory for Craig: over $100,000 in legal expenses.

August 1990: Steve Jackson Games still suffering as Secret Service refuses to return all their property, provide a lawful search warrant, or give evidence of any pending indictment or other legal action.

August 1990: CPSR (Computer Professionals for Social Responsibility) file Freedom of Information Act suit in Federal District Court, seeking FBI records on the secret monitoring of computer BBSs (bulletin board systems) across the country.

August 16, 1990: Several more young hackers arrested including "Zod," who was popped for operating a BBS chat system on an Air Force UNIX computer accessed via a University computer system. Unauthorised copies of game software and system source code are found in his computer as well. Case continued to October.

As We Go To Press/Fall 1990: The Secret Service still refuses to return computers or other property confiscated during the year. In many cases, SS also refuses to reveal details of warrants *or* to file charges. Victims remain in legal and personal limbo, their businesses and careers jeopardized or destroyed.

TO BE CONTINUED, WE SUSPECT M

The allegedly illicit and dangerous $79,000 document was available to Southern Bell customers for less than $30

"What's this ?" an SS agent asked upon seeing the dread weapon of the youthful terrorist. "It's a phone machine" Acid Phreak replied

January 15, 1990: AT&T has a spontaneous near-death experience in the form of a nationwide system crash. Somehow a rumor circulates that a coven of hackers had cast the deadly spell, though AT&T denies it. For its own part, AT&T never told the public that their vital calls would go through normally if they simply dialed the five-digit code for any other long distance carrier.

January 22, 1990: Robert Morris convicted of releasing the worm which temporarily shut down Internet.

January 24, 1990: Secret Service agents raid Acid Phreak and Phiber Optik (two of the more controversial participants in the above-mentioned *Harper's Magazine* Conference), holding a gun to the head of Acid Phreak's 12-year-old sister and confiscating all his electronic equipment including CDs and a telephone answering machine. "What's this?" a Secret Service agent asked upon seeing the dread weapon of the youthful terrorist. "It's a phone machine," Acid Phreak replied. "What does it do?" the superstitious savage queried. "It answers phones," Acid Phreak confessed.

Though no charges are filed, these and other individuals are interrogated on suspicion of having caused the AT&T crash and of being key members of Legion of Doom. For the record, AT&T continued to maintain that hackers were not the cause of the crash. The alleged hackers ' conspiracy called the Legion of Doom took its name from the *Superman* movie and was, in fact, a loosely-knit group of friends with about as much formal structure as a glob of cybersocial protoplasm.

February 2, 1990: Secret Service agents raid Len Rose, aka Terminus. Rose, his wife and child, are terrorized at gunpoint, denied food and use of the bathroom. Calls to lawyers are denied, computers and other property are confiscated. Rose is eventually charged as part of the Legion of Doom conspiracy. His alleged crime: having bits of UNIX source code, something as common among professional UNIX consultants as doctors having self-prescribed medicines in their homes.

February 7, 1990: In the by now familiar Gestapo style, the SS raids Robert Riggs ("The Prophet"), Franklin Darden ("The Leftist") and Adam Grant ("The Urville" / "Necron 99"). This time, an indictment charges various federal felonies including fraud and conspiracy involving taking copies of proprietary software and unauthorized entry into the Bell South computer systems and specifically mentioned the Legion of Doom.

Bell South spends several months investigating the case before turning it over to the Secret Service, using the SS primarily as the enforcement arm of a corporate investigation, and spending 1.5 million dollars in the process. Since it's a corporate, rather than government investigation, Freedom of Information laws don't apply, raising an important issue that is sure to come up again in the future.

February 15, 1990: Craig Neidorf, editor of the on-line magazine *Phrack* is raided, charged (among other things) with publishing the Bell South E-9ll document. His computers—in essence the electronic printing presses for his magazine—are confiscated, putting *Phrack* out of business. Bell South claims that the E-9ll document is worth over $79,000.

Late February 1990: Rich Andrews, operator of Jolnet, is visited by Secret Service. Andrews' crime? Just to be on the safe side, he'd informed AT&T officials about the E-911 document which had appeared on his network. As a reward for his good citizenry, his computer equipment is confiscated. No charges are filed. Significantly, the computer also contains the electronic mail of uninvolved Jolnet subscribers, raising substantial privacy issues.

March 1, 1990: SS raids of Steve Jackson Games and its employees. Jackson is the second largest game publisher (after Milton Bradley), has published numerous fantasy-role-playing games, and was about to launch one called *GURPS Cyberpunk*. The SS confiscates computers at Jackson's offices and employees' homes. No charges are ever specified but connections between Steve Jackson's assistant, and *GURPS Cyberpunk* author Lloyd Blankenship, and the Legion of Doom were mentioned. To this date, equipment has not been returned. Jackson's company has lost over $125,000 and is close to bankruptcy.

device for phone phreaking. And back before the digital revolution was taken over by the marketing departments, it was common knowledge that hackers were the backbone of the industry. Hacking is about exploration and access—exploring the limits of systems, finding what you need, whether to satisfy your curiosity or to complete some useful work. Proprietary concerns are not always treated with the utmost respect. Since hackers also tend to be pranksters, they can at times tend to be downright *dis*respectful towards authority. But a revolutionary conspiracy of self-conscious anarchists, this subculture has never been. Not quite.

Cut to 1990. A year that will live in infamy. For some unfathomable reason, agents of the law decided that this is the time to get busy stomping on self-expression. Just briefly: we had the bust of an art gallery in Cincinnati for showing Robert Mapplethorpe's infamous photos, we had police agents entering a music shop in Florida and seizing dangerous CDs, records and cassettes, we had the 2 Live Crew busts, we had Jock Sturges—a reputable photographer—busted and all of his everything seized for daring to process photos of the young nude body, and we had the US Armed Forces invasion of Humboldt County, uprooting a fistful of the killer weed to impress the president of Colombia.

It is in this context that we come upon Operation Sun Devil and the concerted crackdown against young computer hackers by the US Secret Service.

Think of this calendar of events as a kind of scorecard that you can refer back to as you read this section's interviews with such Dramatis personae ***as Craig Neidorf, Steve Jackson, John Barlow, Mitch Kapor, et al.***

Summer 1988: Hackers' Convention 4.0. CBS News shows up with prepared script intending to depict hackers as dangerous criminals. This was particularly bizarre given that *this* Hackers gathering, formed by Stephen Levy (author of the book *Hackers)* and Stewart Brand with the Whole Earth Institute, is frequented primarily by older, comfortable, relatively law-abiding computer fiends. Many of the people who were portrayed as "high in the Santa Cruz mountains plotting the downfall of the computer industry" were actually CEOs in that industry. Many more were, at the very least, major stockholders and well-paid executives in mainline companies. The dangerous-looking longhaired man seen looking at violent computer games while playing with a yoyo by millions of newswatching Americans was none other than Clifford Stoll, National Security Agency collaborator and author of *The Cuckoo's Egg*. The CBS coverage was probably the first inkling for the older 60's-generation hacker set that something might be amiss in their world.

November 1988: The Internet Worm runs wild across many of the nations' computer networks, shutting down an estimated 6,600 computers tied to Internet and causing an estimated loss of 40 to 90 million dollars. The code, written by Robert Morris, was intended to map the net. In the words of John Barlow, "It was going to go around to every node on the net and report back in and tell just how big this sucker is." But, due to faulty code, it winds up reproducing itself at a phenomenal clip, eating up all the cyberspace in its path and closing many systems. Within a day of Morris' arrest, it is revealed that his father, also Robert Morris, is the *chief computer security expert at the National Security Agency.* Those who wish to conjecture about the possible meaning of this may proceed at their own risk.

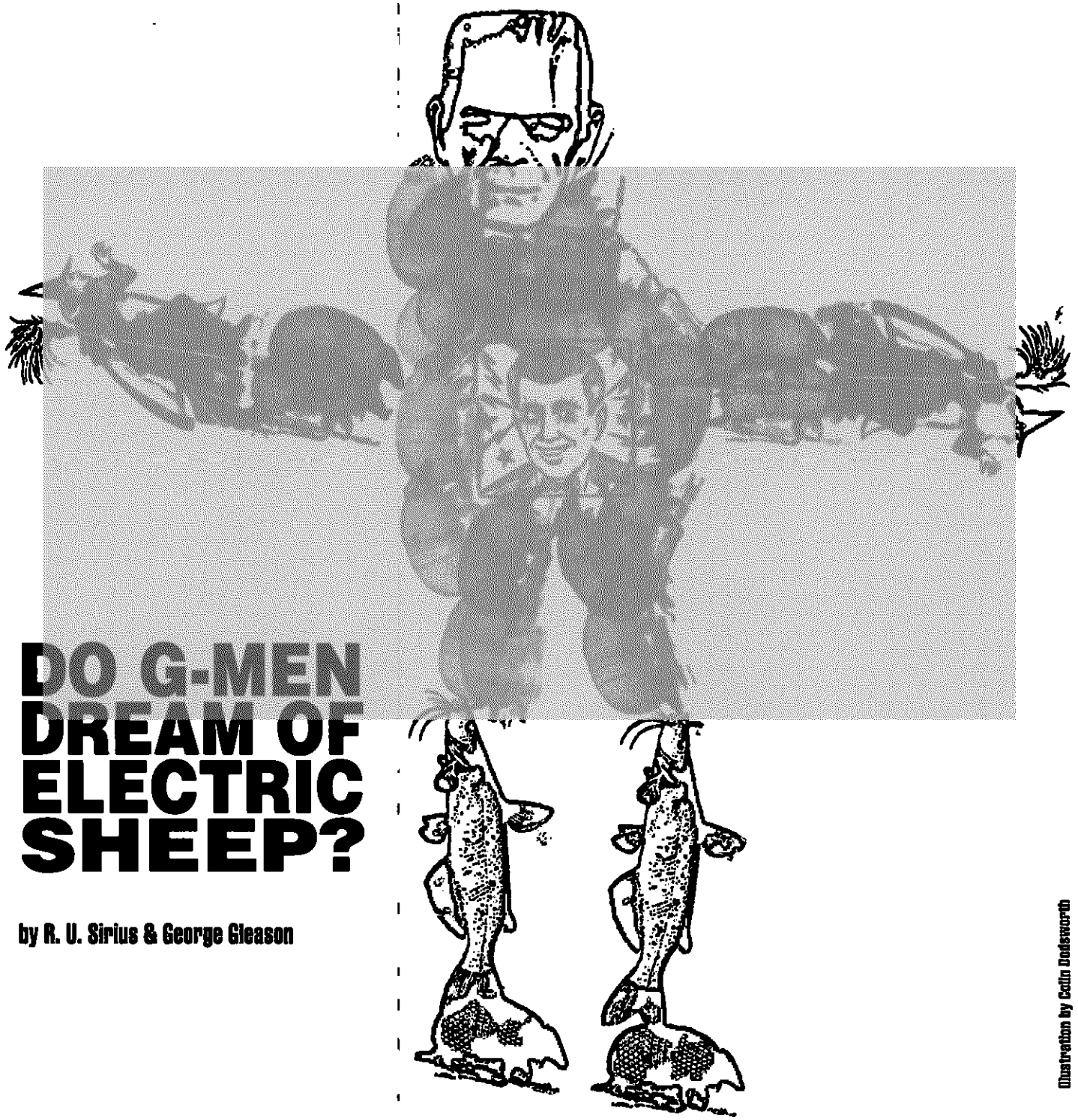
December 1988: Legion of Doom member "The Prophet" downloads a Bell South document on the administration of E-911 systems, and then posts it around bulletin board systems (BBSs) such as Jolnet. It reaches Knight Lightening, aka Craig Neidorf. Knight re-publishes it in his electronic magazine, *Phrack.*

June 1989: A group calling itself NuPrometheus league releases bits and pieces of Apple source code: the software equivalent of Macintosh DNA. NuPrometheus promises more to come. Apple has a proverbial cow.

December 1989: *Harper's Magazine* hosts a virtual hackers' conference on The WELL, a BBS whose members include a number of computer and communications industry pioneers. Hackers and cyberpunks of all stripes attend. The result is published as a cover story.

• *continued on next page*

Many who were portrayed as "high in the Santa Cruz mountains plotting the downfall of the computer industry" were actually CEOs in that industry



DO G-MEN DREAM OF ELECTRIC SHEEP?

by R. U. Sirius & George Gleason

Illustration by Colin Dodsworth

It's no secret that mischievous young computer hackers get into trouble with the law. Occasionally, as in the case of the original legendary phone phreak John Draper aka Cap'n Crunch, they wind up in jail, although for the most part, their cyber-joyriding pranks are merely wrist-slapped. Suspended sentences. Probation. Charges dropped along with promises not to hang with the wrong crowd. Law enforcement quickly learned that it is not in their best interests to lock the hacker—and all that tricky expertise—in with a bunch of hardcore criminals. Indeed, the unmasked hacker may end up working as a security agent—for the phone company, a bank, or even some federal agency. Computer "crime" can be seen as the bush league, training for the Security Industry.

This relatively benign view of phreaking held through the first years of the personal computer industry. After all, Steve Wozniak and Steve Jobs gave birth to the PC partly through funds gathered by selling the "blue box," a

HACKERS & CRACKERS

Illustration by Mark Landman

Academy... I don't know who the hell spoon-feeds you this kind of nonsense. Look, I've had a number of individuals that I've represented under investigation by the Secret Service and the FBI, and *they're* still walking the streets. I don't know who the heck has gone and blown the Secret Service up to this mythological shape and size. It's so silly.

M2: (bewildered) Well, you certainly have an interesting perspective on all this.

AB: Look, you guys have gone out there and you've taken an ant and turned him into Goliath!

M2: Wait... wait... wait. Who's "you guys?" I'm a journalist doing an interview.

AB: I meant the computer industry. I apologize. All I'm saying is, put this in the proper perspective. If you do a numbers game, you're going to find that the Secret Service is a small, criminal investigative agency that is involved in a lot of different areas. Computer communications is only a part of their game. It simply doesn't have the resources to go around doing all the things that it's been given credit for doing. And secondly, the Secret Service investigations, frankly, are not the best around. A pretty good lawyer can usually shoot holes through it.

He Calls it "Industrial Espionage!"

M2: You said in one of our earlier conversations that phone companies and corporations hire individuals to scan BBSs looking for criminal activity.

AB: Sure. They pay private investigators to scan boards. That's investigative work and it's perfectly legal. It's to identify a malevolent hacker *before* he strikes. *Any* force creates a counterforce. That's not bad. That's what makes democracy tick.

M2: Several people within Operation Sun Devil have said that the crackdown has been a positive deterrent.

AB: Of course. I think you're going to find that these cases were designed to scare individuals and make them think twice about engaging in criminal activities.

M2: But then, that same chilling effect has caused lawful BBS operators and users to be fearful and to take excessive security measures in fear that they will be swept up in the dragnet.

AB: Well, if you're obeying the law, the Secret Service isn't going to bother you.

M2: But you're refusing to look at the actual cases! The Jackson case, the Jolnet case... what about the Craig Neidorf/*Phrack* case!? He's being charged with wire fraud in connection with publishing the E911 documents in his electronic journal. What about constitutional issues regarding freedom of the press? *The Post* and *The Times* weren't prosecuted for publishing the Pentagon Papers. Is an electronic journal different from a hardcopy one?

AB: No, I would apply the same standards. But I wouldn't compare the material available on the bulletin boards with *The Times* or *The Post*. Some of the stuff leaves a lot to be desired.

M2: But it should enjoy the same free...

AB: You've got to realize that—and I tell this to a lot of the computer-types I talk to—the public couldn't really give a damn if somebody's computer is seized by the government.

I think this industry needs some techno-ethics. I've seen a lot of people who call themselves hackers, who are—for all practical purposes—criminals. They're not hackers. You know, the hacker thing is just a kind of a veil for them. If you're an industrial spy who breaks into a system and sells the information to a competitor... call it what you want... I call it industrial espionage. I mean, if he came to me, I'd defend him and I'd probably get him off. But that isn't the issue.

M2: But what you're describing isn't hacking. Industrial espionage is abhorrent to most hackers, too.

AB: Well, I don't care about the terms.

M2: But, if you're talking about the establishment of ethics, then you need to establish terminology that can differentiate types of activity, don't you?

AB: Look, hackers need to accept the fact that they operate in a larger society and they're a minority. They need to learn to balance their needs with the needs of society in general. I'd like to run red lights occasionally, but I can't do it 'cause the law says I can't. How would you like it if I got into *your* medical files?

M2: People keep talking about medical files! Is this a big problem that we're not aware of!?

AB: I've come across cases of people getting into other people's medical or financial files for purposes of blackmail. If you want to have access to someone's financial files, it can be done. Absolutely.

He'd Rather Walk

M2: What sort of groups do you lecture to?

AB: Computer professionals, security professionals, executive-types, management-types, supervisors, lawyers, government officials.

M2: In a recent speech, you stated that "Millions of Americans find themselves the victims of computer crimes" and "The public is called upon to pick up the tab for billions of dollars in annual losses... at the hands of computer criminals, hackers, and pranksters." What did you mean by those statements?

AB: I meant that if some half-wit breaks into a government computer and destroys files, the taxpayer has to pay for it. If Uncle Sam pays for it, I pay for it. Think about it.

M2: But where did you get those figures!?

AB: Oh, that's just guesswork. White collar crime runs in excess of a hundred billion dollars. My sympathy goes to the public. I'm not so interested in technophiles who think they have an inherent right to do whatever they feel. I'm concerned for the average Joe Blow American.

M2: Do you think that the media has exaggerated the threat of computer...

AB: I'll tell you what *I* think. I think the media has exaggerated the threat of law enforcement running around and locking people up. And I think the media tends to glamorize hackers. Some of the hackers I've met, I wouldn't even have over for coffee, let alone glamorize. I don't think we would miss hackers very much if they weren't around.

M2: What!? Of course we'd miss hackers! We wouldn't have personal computers without them! We'd probably both be out of jobs!

By the way, are you on any computer networks? Do you ever telecommunicate?

AB: Nah, I've never gotten into computer networks. I'm old-fashioned (laughs).

M2: Do you even *use* a computer?

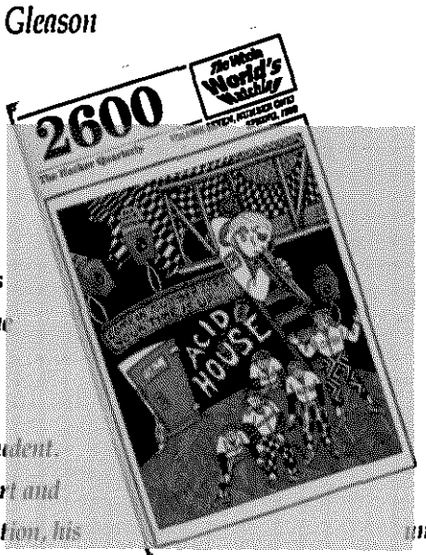
AB: Yes, we have computers in our office. But I often write my books by hand. I'm a believer in labor. I believe in automation, but on occasion, I'd "rather walk," as they say. You know what I mean? M

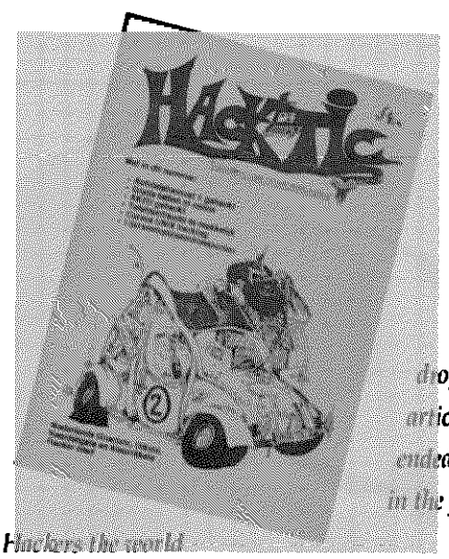
SYNCHRO TECH
RESEARCH FOUNDATION
Presents

Phreaks "n" Hs

An Interview with Hacker Publishers Emmanual Goldstein of 2600 & Rop Gonggrijp of Hack-Tic

by R. U. Sirius & George Gleason





The Emmanual Goldstein of Orwell's 1984 was a legendary author whose forbidden book fuelled the fires of hidden discontent among the thought-criminals of Oceania. The actual real life Goldstein could pass for a University student. With curly hair, printed T-shirt and a look of purposeful concentration, his accent barely hints at his New York origins. He is the editor of 2600, the North American hacker's journal.

Rop Gonggrijp is Goldstein's European counterpart. He is the soft-spoken spokesperson for Hack-Tic, the Dutch hacker's journal whose subtitle contains a word sure to provoke consternation in the hearts of control freaks around the world: "techno-anarchists."

Together they made the trek up the offices of MONDO 2000. With them was a certain "Bill," whose mastery of hardware engineering and other subjects has made him a legend among hackers and phone phreaks on the West Coast. R.U. Sirius rolled the tape and performed a friendly interrogation. I stopped by to drop off another article, and ended by joining in the fun.

Hackers the world over have begun to see themselves as something of a movement. On one level hacking is about exploring the depths and limits of communications and computing technology; on another it's about electronic freedom of speech and unfettered play.

Telecommunications experts of all political stripes are concerned about the lack of coherence in the design of local and global telecommunications. Short-sighted decisions are becoming the rule, with bureaucracy winning out over sound engineering principles. The role of hackers in these issues can be likened to that of ecologists in energy policy; they call for informed public participation and decisions that will be sustainable and fair. Their uncompromising feistiness is important. They show just how fossil and monolithic the old systems are in the face of the new realities of the decentralized global nervous system.

George Gleason.

HACKERS QUESTION EVERYTHING

EMMANUAL GOLDSTEIN: A hacker is someone who asks lots of questions and doesn't believe in following the rules all the time. If somebody says, "Don't look into that anymore, don't ask me any more questions about that," they won't accept that and they'll do it anyway.

MONDO 2000: What about finding answers?

EG: A good hacker will look everywhere to find answers... ask all kinds of people, play with all kinds of machines, try it himself. A hacker defines his own terms.

M2: Do you think there's any revolutionary intent?

EG: Well, you see, you say revolutionary intent these days and it's kind of a turn-off, unfortunately. And anyway I think it's a lot more subtle than that. I think there is some revolutionary intent. Yeah, it's there. It's inside people. But they don't want to say it.

M2: Rop, would you say that the European hacker community is more overtly political?

ROP GONGGRIJP: I tell you there's no such thing as a European hacker community! There's probably more of a difference between Dutch hackers, German hackers, the few British hackers I know, and French hackers—where they won't even call themselves hackers because the French government is so sharp on these things. Every European country has its own mentality.

The German hacker groups I know, like the Chaos Computer Club, are *very* political—concerned about freedom of information, access to information, rules, DDR modernization of the phone system and of the government itself. The Dutch hackers have more in common with most of the American East Coast hackers, I think. It's basically a very playful group that is exploring, finding things out, building things, doing crazy things with technology.

While you can use your hacking abilities to further criminal goals, that doesn't make the criminal acts themselves hacking, and that's unfortunately what the media has mixed up. So it's a great hack to be able to figure out a way to work things so that nobody gets charged for phone calls. I think that's clever. But to simply charge some poor couple in Idaho $1,000 for your phone calls, there's nothing great or particularly clever about that.

M2: What's your feeling about the ATM hack?

EG: I think there's people out there doing it right now. I think if you make the card and you can figure out how to do it, more power to you. You've created something and used your mind. But if you buy the card from somebody and if you just used the card to get money, if you're not figuring anything out, you're just committing a crime. There's no hacking involved. And of course, you don't get that crazy burst of energy from figuring something out... "Ah-hah! *Now* I've got it!" That's what hacking's about! That's very healthy.

Now we're being told that it's wrong to be curious, it's wrong to ask questions. Why do you want to know that? The only reason you'd want to know that is if you wanted to commit a crime. And what does that do to young people today? It makes them very scared, timid. There was a kid who went to our meeting in Los Angeles who was kicked off a Bulletin Board for asking questions about Captain Crunch.

RG: One thing about the ATM hack... the only thing we printed [*Hack-Tik* printed the controversial diagrams that were left out of "ATMs and the Rise of the Hacker Leisure Class" in issue #1 of *MONDO*] was a diagram that shows: what a magnetic stripe is, where the tracks are, where it's PIN [Personal Identification Number] is; and how you read it, how you write to them, and how you copy them. We never told anybody how to figure out PINS. Anybody can figure that out from information in almost any public library. We think people have a right to know what is on those magnetic stripes. We think people have a right to know how things work.

EG: I wouldn't stop there. I'd tell people how you figure out PINS. I'd like to tell that to people. That's a hack. It's a crime when you go out to use the information against somebody.

M2: My analysis is that what we think of as money and value right now is just electronic information and that it can reasonably be manipulated in any way anybody wants to. And right now the people in control manipulate the hell out of it. They're always creating money and there's really no bottom line in value, so finance itself is really basically just a digital battle or game.

EG: I'll tell you this: the more digital the society gets, the more we'll be able to completely change money. We'll be able to change a date on a document. We'll be able to add a figure to a bank balance. We'll be able to change a "no" to a "yes" at some point. How do you trace things like that? If you're a good programmer, there are no fingerprints. At the same time, we're telling people to be careful and be aware. Understand that the facts can be changed and this is how they can be changed. And

That's all we've been talking about since we got here, so you can imagine how much trouble we're in now!

The more digital the society gets, the more we'll be able to completely change money. We'll be able to change a date on a document. We'll be able to add a figure to a bank balance

if we don't tell people, they can be changed anyway.
RG.: There's this panic about hackers being able to access something like TRW... credit records. Everybody that subscribes to TRW can get your credit record. Everybody! *Every* employee at any company that wants to sell you things, people that want to sell you loans, they can *all* get your credit records. A few hackers got access to that information, and the whole nation's upset.
EG: What Rop is saying is true, but I'd say that the media *tries* to get the whole nation upset. But a lot of people are more sophisticated than we give them credit for. I've talked to people of all types who are a lot more outraged that these records are being kept and passed around in the first place.

TELECOMMUNICATIONS

RG: If I tell you about a simple device that works in thus and such manner and allows you to do toll fraud on the phone system here, it's illegal for me to tell you that in California... also, in Germany.
EG: That's all we've been talking about since we got here, so you can imagine how much trouble we're in now!
M2: The cost of covering actual territory by telecommunications is now really minimal. The phone companies want us to keep thinking in terms of territorial, rather than informational landscapes...
RG: You want to know what the rates for calling from Iraq to here are? I understand it's a lot lower than the reverse.

It's important that ordinary people overcome their fear of technology and grasp control—do what the hackers do. If everybody had the knowledge that the hackers do, you wouldn't see such rip-offs.
GEORGE GLEASON: You know, the phone company doesn't do their own tech anymore. If something's wrong, they send for the manufacturer to come and fix it. The phone company engineers feel very bad about this because their work degraded from designing systems and doing telecommunications engineering to just screwing the wires on. It also means that there's really nobody with a global overview of what's going to happen, what the design philosophy is going to be. They just install what they think is profitable at the moment. They buy the cheapest switch possible. But even the phone company doesn't have an idea of what telecommunications should be for society.

Now imagine the equivalent of an AT&T crash happening in a situation like that where nobody in charge really knows how the whole thing works. That's frightening.
M2: How would you build it back up again?
RG: Take two tin cans and a piece of nylon wire and communicate. You can put all of the instructions on the back of a postcard.
M2: Can you draw a diagram of that?
RG: Sure. [laughs]

DARKSIDE HACKING?

M2: Talk about the Galactic Hacker Party. What's that all about?
RG: Well, first of all, it wasn't a large meeting of terrorists planning the downfall of planet Earth. It was very much about issues— political issues and technical discussions. We understand that it was described by some U.S. hackers as a meeting of darkside hackers.
M2: What's that supposed to mean?
EG: Anything the computer industry doesn't like!
RG: The Zero Positive Ball in Amsterdam was a 69-hour-long happening linked with the San Francisco AIDS convention. While it wasn't officially a Galactic Hacker Party event, it was organized by a group of people closely associated with the Galactic Hacker Party. What happened was a whole team of hackers created a worldwide network. There were computer terminals in bookstores in Amsterdam, there was an alternative bookstore, a somewhat more mainstream bookstore, a gay and lesbian bookstore, and the main center itself had 10 terminals. There was this happening going on and people would come in and use that network. It was made simple, so people walked off the streets who'd never touched a computer before in their life and were hooked to the network. People started talking about getting a computer system themselves, buying a modem, coming to the University library to use their terminals. It was getting people into computers. That's what hackers do if you leave them alone. They evolve into people who are involved in building networks, building systems. Exploring is only phase one. Creating is phase two. If you stop people from exploring, if you point guns at them and kick their computers in the back of your car and drive away with it and tell them to never do a thing like that again, they're not gonna create either.
EG: But they *will* remember. M

THE COVERT SPECTRUM

BY JIM HOUGAN

"A bit of transmission has been coming through,
But so disjointed that I cannot be sure
Whether I am to work more closely now with
Artifact, or terminate him . . . "
from Reflections on Espionage
by John Hollander (Atheneum, 1976)

IN THE LATE AUTUMN OF 1987, a pirate broadcaster seized control of the transmission signals of two television stations in Illinois. For nearly two minutes, startled Chicagoans listened to a bizarre diatribe about a local sportscaster, while watching a naked man being spanked with a flyswatter.

Halfway around the world in Teheran, a television audience of shocked fundamentalists stared at their sets in horror, as agents of the CIA-sponsored "Flag of Freedom" organization took control of the Iranian government's own television signal to attack the Ayatollah — and promote the cause of the exiled Baby Shah.

What does it mean when the CIA and a practical joker mount parallel and highly technical covert media operations on separate continents — the one to overthrow a government, and the other to mock a sportscaster?

It's getting a little . . . Videodrome out there.

Since the creation of the Central Intelligence Agency in 1947, covert activity has metastasized within the federal government. Virtually every U.S. agency today is host to one or more secret components whose operations are as invisible as Washington can make them. From the unheard-of Office of Foreign Availability at the Commerce Department to the determinedly anonymous Federal Research Division of the Library of Congress, the American government has spawned a sub rosa bureaucracy whose day-to-day business resembles nothing so much as a conspiracy in (what we're told is) the public interest.

To say that Big Brother is watching is a cliche, of course, but it is also true. And yet, as profound as this development is, its importance is likely to be dwarfed by an even more radical development. Technological change has commercialized the covert intelligence function to the point where its tools and practices are available to anyone who can pay for them — to anyone, in other words, from the neighborhood grocer to the ecological activist, inside trader, serial killer, and political nut. And while the publicly available technology is often somewhat less than state-of-the-art, there are compensations: e.g., the private sector is free from congressional oversight.

★ ★ ★

I'm sitting in a darkened room in front of a shortwave console, headphones clapped to my ears, listening to a woman's voice on the Upper Sideband:

"Sierra foxtrot, sierra foxtrot. Six, one, seven. Three, five, one. Five, four. Dis-information . . . "

I know it won't improve the sound, but I can't help

Washington-based writer Jim Hougan has had three books published: Secret Agenda *(about Watergate);* Spooks *(about corporate use of intelligence agents); and* Decadence: Radical Nostalgia, Narcissism and Decline *(about the seventies). When asked how he would characterize himself, he answered unhesitatingly: "literary thug."* —*Robert Horvitz*

leaning forward instinctively, lowering my head into the pale yellow light from the radio dial, straining to hear. Did she say "dis-information" . . . or "this information?"

"Three, six, four, nine, three." A pause.

"Seven, nine, one, one, two." Another pause.

The voice is sensuous but mechanical, matter-of-fact and utterly mysterious. The message she's sending is as impenetrable as its authors can make it: 54 groups with five numbers in each, directed, we may suppose, to Agent 617 from Sender 351. Or vice versa. It's impossible to tell.

The transmissions are received by agents in the field using ordinary portable shortwave radios. The messages are decoded with the help of "one-time pads" of randomly generated numbers arranged in groups. The code is probably unbreakable, unless, as sometimes happens, the pad itself is captured (quite possibly over the dead body of the agent in question). It's a system in which each group of numbers represents a word or phrase. Thus, "54209 67319 38785" might mean "information required about — security arrangements — at the airport." Then again, it might not.

The woman's voice beats at my ears, hypnotic in its nonsensicality. She and her sisters (and an occasional brother) have been reading numbers into the void on hundreds of shifting channels for decades. They broadcast from almost every part of the world in languages as diverse as Spanish, Russian, German, Chinese, English, Bulgarian, and the old standby Morse Code. Their accents are American or Mandarin, Honduran or Czech. Some of the broadcasts begin with signature-tunes, musical passages that, in effect, cue the agent to get out his pad and pencil. (The Chinese apparently start their broadcasts with four notes played on a marimba, reminding some listeners of Macy's, while the Romanians alert their agents with a passage from "The Meadowlark," played on a piccolo.)

Leaning forward, I tilt my head to the side and, listening intently, hear a barely audible click between each of the numbers. According to covert radio expert Harry Helms*, the woman is a bionic creation — the spooks' counterpart to Directory Assistance. A human may have voiced the numbers originally, but nowadays the transmissions come from a device that strings together brief, prerecorded audio tape-loops in the needed sequence. The station from which she's broadcasting is probably a robot as well: an unstaffed, remotely controlled, windowless bunker surrounded by cyclone fencing, video cameras, barbed wire and hidden alarms.

A mathematics professor tracked a string of numbers transmissions to a facility just like that several years ago. Set amid the farms and forests near Remington, Virginia, about an hour's drive from CIA headquarters

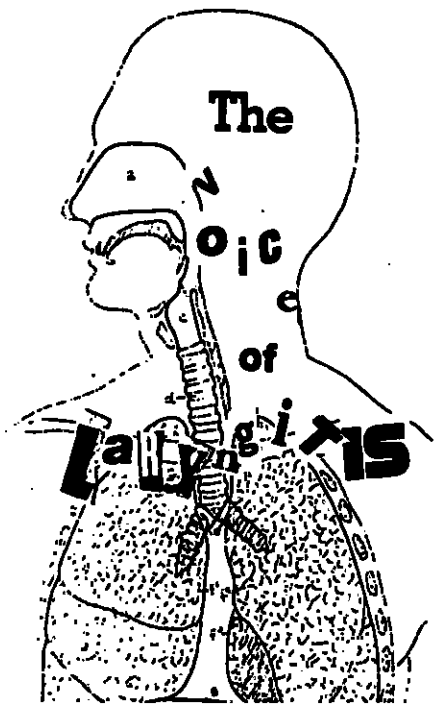


Fig. I-T. *The lucky listener may still have a chance to hear the Voice of Laryngitis, often considered the most creative and professional pirate to operate from North America.*

Pirate Radio Stations

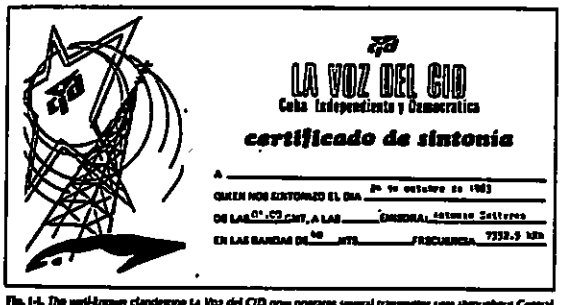


Fig. I-L. *The well-known clandestine La Voz del CID now operates several transmitter sites throughout Central America. But in 1982, they were caught broadcasting from Florida.*

in Langley, the installation bristles with dipole and log-periodic antennas. A sign at the entrance reads:

WARRENTON TRAINING CENTER
NCS
U.S. ARMY
STATION C

Transmissions from the Remington stations (there are several in the area) have been recorded in English, Spanish and Morse Code. While the Pentagon and other government agencies refuse to comment on the facilities, other than to say that their missions are classified, it is thought that at least some of the broadcasts are for training purposes. After all, junior CIA officers need real-time practice in the field.

Where, in fact, it can get very rough.

Indeed, if reports from Nicaragua are believed, the Warrenton "numbers stations" were used to coordinate plots against Sandinista leaders. According to one report, the CIA recruited a Nicaraguan-born femme fatale to assassinate that country's foreign minister in 1982.

* Helms edits *Umbra et Lux*, a monthly newsletter dedicated to unlocking the mysteries of covert radio transmissions.

The woman was allegedly given a Sony shortwave radio capable of picking up the coded broadcasts, a one-time pad concealed in a wooden figurine, secret inks, and an edible notebook. Her instructions were said to be transmitted in four-digit groups at 11 P.M. on 9074 kHz.

Interestingly, there has been no let-up in numbers broadcasting from the Warrenton site, even as a pro-US regime takes charge in Nicaragua and, elsewhere around the world, the Cold War thaws.

" . . . Uno seis ocho dos. Ocho seis zero uno. Nueve tres ocho quatro. Final. Final!"

The Crystal Ship

QSL

Shortwave

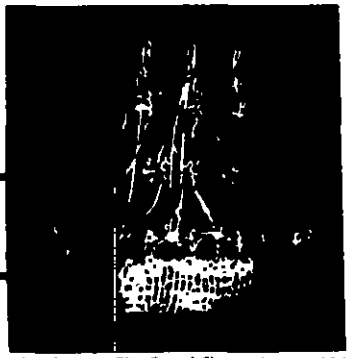


Fig. 8-3. *featuring hard rock political music. The Crystal Ship took a youthful approach to socialism.*

That there is mystery in poetry and poetry in mystery is clear to anyone who's thought about either. John Hollander made the point some years ago with *Reflections on Espionage.* A book-length poem, it was structured as a series of apparently decrypted radio messages from an agent known only as "Cupcake," to his controller, "Image." The verse is knowing — about espionage, about radio, about life.

2/1 (TO IMAGE)
Image, there were funny pings in my headset
During the transmission tonight, echoing
Neither in my head nor in the earphone, but
Somewhere within, it seemed to me, their own sound.
Transmitting the truth is always a problem.
Facts we can encipher, and they then become
Sendable messages: why do not the truths
Climb obediently into disguises,
Learn their lines well and be off? Instead they hang
About and plague us with unvoiced reproaches.
Perhaps these headset pings — I dreamt last night I
Fled someone, and ran into a cave ("This is
A place of broken artifacts" rang in my
Ear as if I had just been so instructed);
Then I was sitting down and heavy pebbles
Were dropping around me at slow intervals
("Broken echoes" my head said). Then I awoke,
Forgetting the dream, the cave, the broken stones.
Tonight the dying sounds inside my headset
Recalled them all. Echoes of truth? Collect them,
Image, fragmentary as they are, like shards
Of mirror, each of them reflecting the whole.

The point about numbers broadcasts is not just that they're an intriguing mystery. It is, rather, that despite being sent out in dozens of languages over hundreds of frequencies for more than forty years, the existence of these stations is entirely unknown to all but a relative few. The average person (if that's not a contradiction in terms) has little idea of the electromagnetic plenum that surrounds him. To stumble upon a "numbers" broadcast is to realize that each of us is living, obliviously but in fact, in an atmosphere of unapprehended secrets.

Not all of these secret broadcasts are in code. "Covert communications" is a catch-all covering an array of transmissions that are, in one way or another, supposed to be secret. This can mean coded texts from known transmitters, or clear voices from hidden sources. Whichever, one can, with readily available equipment, listen to the transmissions of surveillance "bugs," drug smugglers plying the US's boundaries, as well as the Customs agents chasing after them. You can even hear Air Force One.

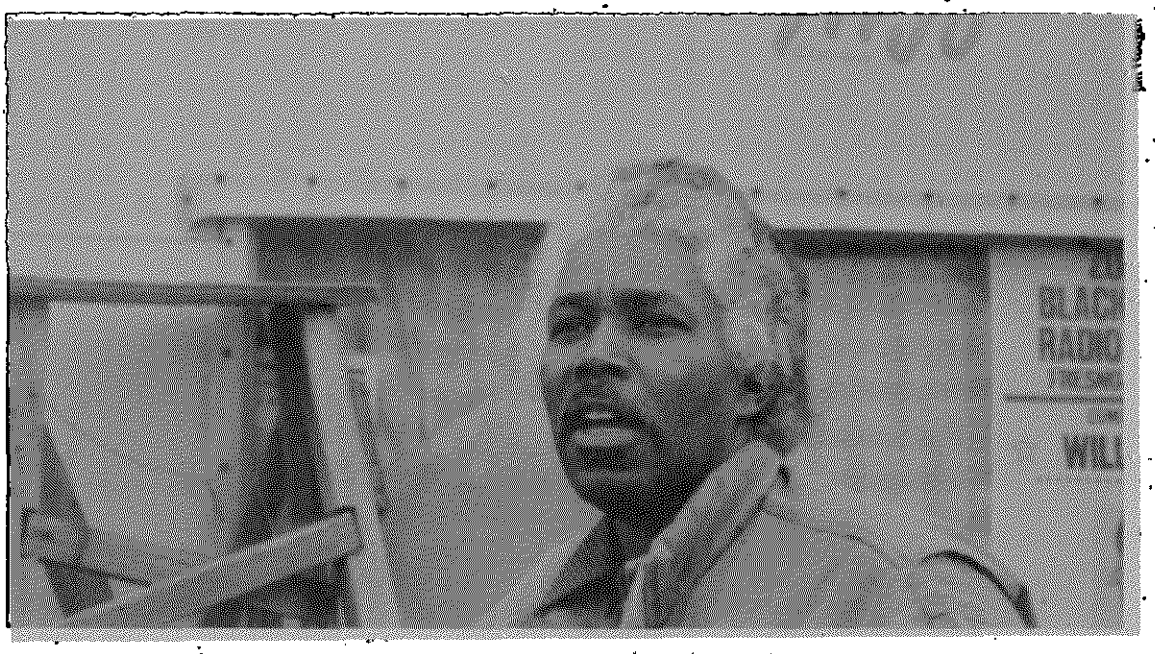
One type of covert communication that definitely wants to be heard is clandestine broadcasting. While such stations go to considerable lengths to keep their locations secret, their messages are meant for all within earshot. Radio Caiman, for example, has been broadcasting a mix of rock and Latin music, interspersed with anti-Castro talk segments, for nearly five years, from a transmitter believed to be just outside Guatemala City. The station's powerful signal, longevity and slick progamming set it apart from other Spanish-language clandestines. In the opinion of many shortwave listeners, Radio Caiman is probably funded and programmed by the CIA, while its less sophisticated counterparts are operated by independent groups.

The number of clandestine broadcasters operating in the world at any given time is anyone's guess — but certainly there are dozens. They have names like "Flag of Freedom Radio" (targeted at Iran), "Radio Truth" (which tells South Africa's side of the apartheid story), and the "Voice of the Broad Masses of Eritrea" (which supports Eritrean independence from Ethiopia).

What many of these stations have in common is exile. In almost every case, their transmitters are located outside the countries to which they're broadcasting. An exception is "Radio Patria Libre," which urges the overthrow of the Colombian government from a location in the mountains northwest of Medellin.

Then there are "pirate" broadcasters whose content is apolitical (in a conventional sense), but whose identities and locations are as carefully guarded as the clandestine stations'. The Crystal Ship. The Voice of Laryngitis. Secret Mountain Laboratory. These are playful and romantic names, conjured up by "kids playing radio." They beam crude casseroles of rock and satire into the void, using homemade or modified ham transmitters.

There are some serious exceptions. Such as the "Voice



Walter Dunn ("The Black Rose") outside his pirate radio station "Zoom Black Magic." The station broadcasts over a 24-mile radius using Radio Shack equipment.

of Tomorrow." An openly neo-Nazi enterprise, the Voice of Tomorrow undoubtedly thinks of itself as a political clandestine. It transmits calmly voiced racial propaganda and rightwing populist analysis aimed at "raising the consciousness" of White America. The Voice is heard, intermittently, on a variety of shortwave frequencies. In contrast to "hobby pirate" stations, its announcers and production style are strikingly professional. VOT's transmitter is thought to be located in Virginia, within a few hours' drive of FCC headquarters.

It is the Federal Communications Commission's responsibility to put pirates stations off the air, and likewise, we assume, domestic clandestines not supported by the US Government. The FCC claims that the Voice of Tomorrow moves their transmitter each time they go on the air, and their broadcasts are only an hour long, making them hard to catch. A spokesman adds, "Judging by the complaints we get, the broadcasts are infrequent." Perhaps. But they also had a hard time busting "La Voz de Alpha-66," a virulently anti-Castro station which broadcast from Miami on the same frequency (6666.6 kHz) three nights a week for most of the Reagan years. Their transmitter was finally confiscated around the time the Voice of America's Radio Marti came on the air.

The FCC's agents had no difficulty finding Walter Dunn, however.

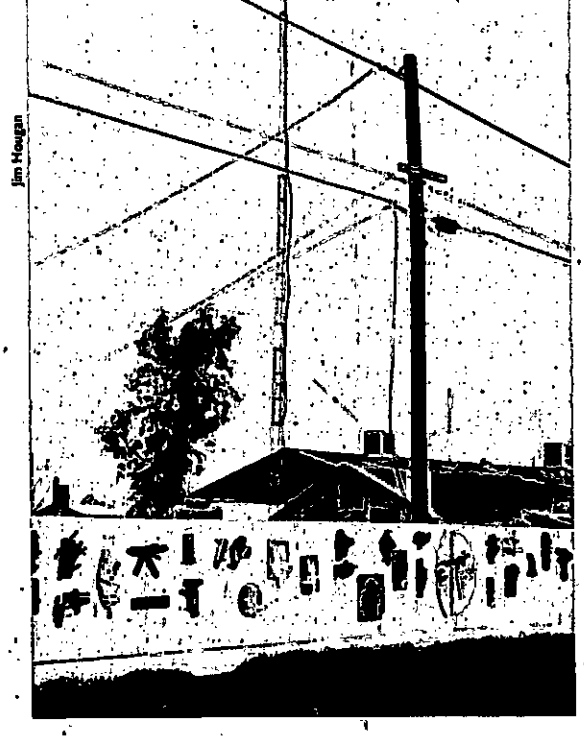
Dunn is a handsome black Californian with graying hair, a mellifluous voice, and a rap that's funny, smooth and pointed, all at once. Transmitting from Fresno, Dunn's "Zoom Black Magic Radio" has been the target of several FCC raids. According to "the Black Rose," as he's also known, six FCC agents showed up at his house some time ago, scaring the wits out of his bedridden mother. Accompanied by police cars and a two-ton flatbed truck, brought to the scene to haul off broadcasting equipment that could actually have been carried away in a bucket, the FCC was determined to put Dunn out of business. And it succeeded.

But only for a few days.

Dunn is a man with a mission, and a belief in his right to broadcast. He's often been heard on 100.5 FM at night, transmitting from a beat-to-death 14-foot Aljo trailer in the "Zoom Compound." The Compound is, in fact, Dunn's backyard and it's easy enough to find: the station's antenna, a 76-foot, leaning tower of Zoom, rises beside Dunn's vegetable garden to provide about 125 watts of "effective power."

Operating on listeners' donations that enable him to rake in as much as $60 per month, Dunn uses Radio Shack equipment to put out a signal for 24 miles in every direction. He's assisted by a phalanx of volunteer DJs and technicians with handles like "Iceberg," "Mellow Yellow," and "Daddy Rich." Together, they play everything from jazz to "thump thump," interspersed by an outrageous mix of "community messages" and Zodiacal hype. The Saturday night that I spent in the trailer, reclining on a couch with my head against the ceiling and my chin on my chest, "Mr. Ebony" (James Gearon) was at the microphone, putting out a smooth stream of good-natured blarney.

"You want to take a ri-iiide in time? Okay — kick back! Two six eight, four three oh eight is the magic number. 'Shark Attack' comin' atcha!" Gearon reaches for a Wes Montgomery album, plucking it expertly from one of the dairy crates that holds the station's



Jim Hougan

"Zoom Black Magic's" antenna, visible behind a fence decorated with sculptures by Walter Dunn's brother, Warren.

records, and begins to quote from a poem that he's written: Love is Man eating the Wisdom Dinner From God through his Woman's Hand. He puts the album on a battered Technics turntable, flips a switch and sits back with a satisfied smile. "Welcome to Slave Quarters Radio," he says, as he turns up the monitor — a cheap portable with a tinny sound.

Sitting in the trailer is a little like being in a submarine made of scraps. J.C. Penney bags cover the windows, making it impossible to see outside. The main source of light inside comes from a yellow heat-lamp. The lamp drives the cold from the air, which is good because the trailer is otherwise unheated. But it fills the space with a thick, almost liquid, light.

I ask Gearon where he's from. "Chicago," he says. "I had a business there: the Master-Blaster Shoeshine Parlor, Valet Service and Dye-Works. On 79th Street. I did okay, ya know, but I got burnt-out. See, all them brothers in the fast lane . . . would come in and want their shoes dyed the same color as their pink pants. Which was okay, but : . . after awhile, I burnt out on shoes. So here I am." Indeed.

The next morning I ask the Black Rose what Zoom Black Magic is all about. "Well, first of all," he said, "we're not filthy lowdown dogs and pedophiles like those other stations. We're one of the thousand points-a-light that Marsa Bush spoke of. What you see here," he continues, "is a Rasta versus Goliath story. I mean, it's pitiful. There's a black community of 100,000 people in the San Joaquin Valley, and there isn't a radio station around with a black personality on the air. We're filling a need," he says, and then hastens to point out that Zoom Black Magic isn't *just* a black station:

"It's a people-station. We cover the spectrum, ethnically. I mean this is your voice, your drum — whatever your color is."

Surveying his radio demesne with the calm gaze of a Texas rancher scanning the horizon for his property line, the Rose is suddenly at a loss for words. "This . . . this . . . this —" Finally, he hits upon the right word, and his expression changes to a scowl. "This is BULLSHIT," he shouts. "In the 20th Century, this is absolute bullshit! But you know what? Some . . . some —" Dunn casts around for the right word and, finding it, smiles: "Some FRUITCAKE — someone like Morton Downey — could take this thing and RUN with it!"

Dunn is a gadfly, not a revolutionary. His attacks on the black "booooj-wah-zee" may be culturally subversive in the San Joaquin Valley, but he's not out to overthrow the government. On the other hand, he is determined to expand his broadcasts to the television spectrum. Indeed, Dunn worked for years as a technician at a television station, and he's already experimented with a pirate signal out in the Fresno area. Zoom Black Video can't be far behind.

For all of the Rose's playfulness and hyperbole, the stakes are enormous. To live in ignorance of the hidden spectrum of airwaves, oblivious not just to its mysteries but to the very fact and fullness of its existence, is to cede control of the medium to people and institutions that do not necessarily have our best interests at heart. Consider, if you will, a recent announcement from the Defense Department under its "Small Business Innovation Research Program." *

It is a solicitation for bids from researchers to explore the use of radio to deliver computer viruses into targeted communications systems and networks.

"The purpose of this research," the solicitation explains, "shall be to investigate potential use of computer viruses to achieve . . . (information) disruption, denial, and deception. . . . Research in effective methods or strategies to remotely introduce such viruses shall also be conducted. Efforts in this area should be focused on RF [radio frequency] atmospheric signal transmission such as performed in tactical military data communications."

According to the Washington Post, the would-be sponsor of this project is — the US Army's "secretive Center for Signals Warfare in Warrenton, Virginia."

A computer virus is just a stanza of code let loose, numerical programming instructions that propagate. Nothing would be more natural for the boys at Warrenton than to want to use clandestine radio to broadcast such viruses.

"Sierra foxtrot! Sierra Foxtrot! Six, one, seven. Nine, five."

Artifact can kiss his ass goodbye. ■

* "Solicitation 90.2 FY-1990 Small Business Innovation Research (SBIR) Program," p. 45: "A90-217 TITLE: Computer Virus Electronic Counter Measure (ECM)."

CLANDESTINE ACCESS

BY ROBERT HORVITZ

FASCINATION WITH covert radio communications has never been greater. Here are paths into this mysterious realm.

Joining the Association Of Clandestine (Radio) Enthusiasts will bring you up to speed quickly. Their monthly bulletin, The ACE, is the single best source of current information about pirate and clandestine radio activity.

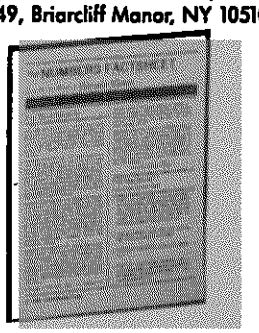
The Ace: Sample issue $1.50. Annual membership: $18 in the US, $19 in Canada/Mexico, $25 elsewhere. From ACE, P. O. Box 11201, Shawnee Mission, KS 66207-0201.

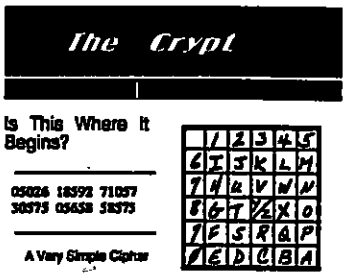
Two ACE columnists, Harry Helms and "Havana Moon," spread their wings wider in Umbra et Lux, a monthly newsletter devoted to "signals intelligence" and covert shortwave communications. Their main interests seem to be studying anomalies in coded message traffic and finding secret transmitter sites.

Umbra et Lux: Sample issue $2. $18/year (12 issues) in the US, $21/year in Canada, $30/year elsewhere, from DX/SWL Press, 10606-8 Camino Ruiz, Suite 174, San Diego, CA 92126.

"Havana Moon" has written a lot about numbers stations. Claiming to be a former spook, this June he started a quarterly newsletter called The Numbers Factsheet. Lists of recently active frequencies and descriptions of unusual intercepts appear each issue.

The Numbers Factsheet: $16/year (4 issues) domestic, $25/year international, from MoonBeam Press, P. O. Box 149, Briarcliff Manor, NY 10510.





—The Numbers Factsheet

Folks with modems might find H Moon's "Los Numeros Online" service worth visiting. In addition to computer files on a wide range of radio subjects (not just clandestines), there are "live online" conferences on Saturday nights, with callers reporting signal catches in real-time for the group to monitor and discuss. Sort of an ethereal hunting party.

Los Numeros Online: Found on the Portal computer communications system in Cupertino, California. $10/month for full access to Portal. Call 408-973-9111 for registration information (9 a.m. — 5 p.m. PST).

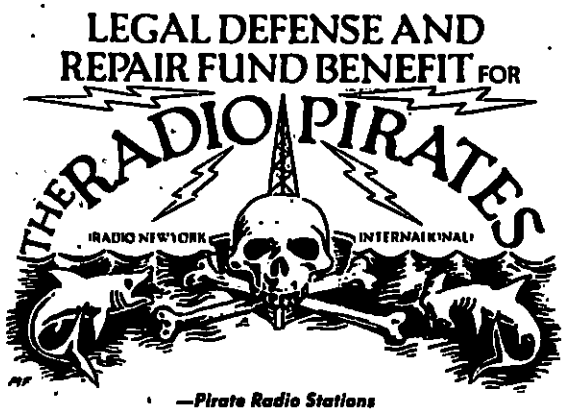
***Electronics & Radio Hobbyist's Newsletter** is for folks interested in broadcasting without a license. That can be done legally, so long as you stay within strict limits on power and antenna size. If done right a low-power AM or FM station can cover a dorm, a city block, even a neighborhood. This newsletter is a forum for all aspects of low-power operation, legal and illegal, with reports from the field and photos of home-made stations sent in by readers, plus editor Ernest Wilson's useful circuit diagrams and tech-tutorials. Wilson's company, Panaxis, also sells high-grade equipment for low-power stations, usually in kit form.*

Electronics & Radio Hobbyist's Newsletter: $24/year (12 issues); trial sub $14/6 issues) from Panaxis Productions, P. O. Box 130, Paradise, CA 95967-0130.

Andy Yoder publishes the biweekly Pirate Pages, where subscribers trade station gossip and lore. He's also the author of Pirate Radio Stations. This book's subtitle, "Tuning in to Underground Broadcasts," is an exaggeration. Most of the stations described are in North America, signing on for a few hours of weekend or holiday fun. Few could be considered radical or dangerous, though they do violate FCC rules. Yoder's fanship both helps and hurts the book, adding anecdotes but losing critical perspective.

The Pirate Pages: Biweekly; $6/12 issues from Andrew Yoder, P.O. Box 109, Blue Ridge Summit, PA 17214.

Pirate Radio Stations: Andy Yoder (1990, 182 pp.). $12.95 postpaid from TAB Books, Blue Ridge Summit, PA 17294-0850; 800/233-1128 (or Whole Earth Access).



—Pirate Radio Stations

For an overview of recent air piracy in North America, see ***The Pirate Radio Directory*** *by George Zeller. The 1990 edition gives brief sketches of more than a hundred stations heard during 1989, mostly in the shortwave band. Illustrated with souvenir cards and letters sent to listeners, there's also general information about when and where to listen, and how to contact the perpetrators.*

The Pirate Radio Directory (1990, 71 pp.): $9.95 postpaid from Tiare Publications, P. O. Box 493, Lake Geneva, WI 53147 (or Whole Earth Access).

World War 2 was the crucible in which modern radio warfare developed. Aileen Clayton's ***The Enemy Is Listening*** *gives a terrific account of that period. The first woman commissioned as a British intelligence officer, she managed some of the teams and stations which monitored German radio transmissions for the codebreakers. She also helped figure out the secret "radio beam navigation" system that let German pilots find British targets at night. The British eventually used this knowledge to misdirect the planes.*

The Enemy Is Listening: Aileen Clayton, 1982. Ballantine Books, Out of Print.

The Puzzle Palace was a breakthrough in public knowledge about the National Security Agency's worldwide eavesdropping network. Big issues, dazzling research, still must reading.

The Puzzle Palace: James Bamford (1983, 656 pp.). $10.95 ($12.45 postpaid) from Penguin USA, 120 Woodbine Street/attn: cash sales, Bergenfield, NJ 07621.

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA). It made "endeavoring" to "intentionally intercept" certain signals a federal crime. Earlier laws set limits on what you can do with signals legally received, and the FCC enforces its transmission rules. It is thus essential to know the law if you tread in this arena. Fortunately, the relevant parts of the United States Code have been gathered in a single volume: ***Compilation Of The Communications Act Of 1934 And Related Provisions Of Law.*** *In addition, some states have laws limiting the mobile-use receivers that tune outside the broadcast bands. Those have been assembled by Frank Terranella in the* ***A.N.A.R.C. Guide To U.S. Monitoring Laws.*** *The FCC's rules governing broadcasting are found in* ***Code of Federal Regulations Title 47, Part 74.*** *The rules governing unlicensed transmissions are in Part 15 of the same title.*

Compilation of the Communications Act of 1934 and Related Provisions of Law: Committee Print 101-I, House Committee on Energy and Commerce (1989, 397 pp.). $12 from Superintendent of Documents, Government Printing Office, Washington, DC 20402-9371; 202/783-3238.

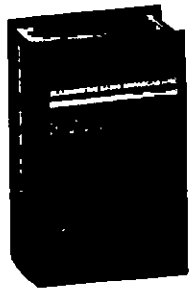
A.N.A.R.C. Guide To U.S. Monitoring Laws (1990, 44 pp.): $7.50 postpaid from ANARC Publications, 1218 Huntington Road, San Marcos, CA 92069.

Code of Federal Regulations, Title 47: Part 0-19 ($18 postpaid) and Part 70-79 ($18 postpaid) from Superintendent of Documents, Government Printing Office, Washington, DC 20402-9371; 202/783-3238.

Clandestine Radio Broadcasting is a comprehensive history of illegal stations that broadcast against particular political regimes. "Underground" fairly describes these. Hundreds of stations are discussed, from all parts of the globe, from the 1930s to the mid-1980s. Only a handful of short-lived TV projects are noted, TV being so much harder to do without getting caught. Details about political context are sometimes ample to a fault here, but the depth of scholarship is welcome, given the speculative hype this subject usually generates.

•

Clandestine stations generally emerge from the darkest shadows of political conflict. They frequently are operated by revolutionary groups or intelligence agencies that are unable or unwilling to leave a documentary record of their activities. And, unlike printed propaganda, no artifact remains. Consequently, a good deal of what has been published about clandestine radio broadcasting is nothing more than educated guesswork. In many cases, the guesswork is not even particularly educated. Because it is usually difficult to pinpoint a station's sponsorship, location, motives, and so on, very few scholars or journalists have taken the risk of writing in depth about clandestine radio broadcasting. Indeed, this is the first book-length interpretative history of the subject.



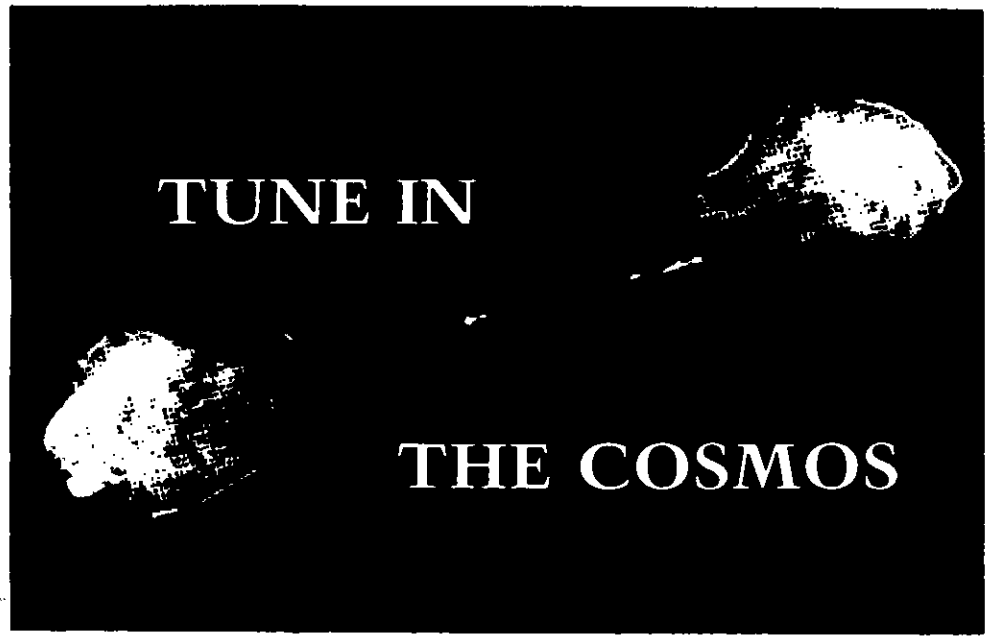
Clandestine Radio Broadcasting (A Study of Revolutionary and Counterrevolutionary Electronic Communication): Lawrence C. Soley and John S. Nichols (1986, 383 pp.). $48.95 ($51.95 postpaid) from Praeger Publishers c/o Greenwood Press, 88 Post Road West, P. O. Box 5007, Westport CT 06881; 203/226-3571.

•

This tactical difference reflects how easily available radio technology is in modern Poland compared to post-World War II Palestine. The Poles can inexpensively procure the parts needed to build transmitters. If a cheaply built transmitter is confiscated by Polish authorities, it can easily be replaced. In Palestine, the situation was different. Parts were neither in ready supply nor inexpensive. Seizure of a transmitter would have been a major loss. That is no longer the case in the Middle East or other parts of the world, since radio components are now easily obtained in most regions. In Chile, for example, guerrillas can afford to blow up a transmitter to make a political point. The growth of radio receiver ownership and the availability of transmitters has led to a growth in the number of operating clandestine stations during the 1970s and 1980s.

•

Numerous pirate stations are operated in the Soviet Union. One report (Helms 1981) estimates there are about 3,000 Soviet pirate broadcasters, most of whom frequently broadcast obscenities and rock music. During a six-day period in 1971, 115 illegal transmissions were monitored by Soviet authorities in less than five hours (Taylor 1972), and most of the transmissions were from radio "hams." Fewer than 1 percent of the offenders who are caught making illegal broadcasts in the Soviet Union receive criminal sentences. Most are fined or receive "social discipline." Jail sentences are reserved for clandestine broadcasters, whose transmissions appear less often than those of pirate broadcasters.



The powerful extragalactic radio source Cygnus A, one of the first to be identified with a galaxy. This radiograph reveals fine filamentary structure in the two radio lobes, separated by about 3 x 10^5 light-years. A giant elliptical galaxy is known to be centered at the small bright spot in the center of the picture. Thin jets connect the central "engine" in the galaxy to the powerful radio lobes.
—The Invisible Universe Revealed

Getting into Amateur Radio Astronomy

BY JEFF LICHTMAN

IT IS ESTIMATED that all the energy which has fallen upon Earth's radio telescopes would not equal the kinetic energy in a single snowflake. Yet radio astronomers have so refined the sensitivity of their equipment that these small powers are not only detected, but also evaluated into information about the Universe which is both illuminating and exciting.

Radio astronomy has been described as the examination of ripples on waves riding upon an ocean of noise. One begins with as large an antenna as can be achieved, to trap as much energy as possible from the desired object. Most discrete radio objects are very weak, so receivers must have low internal noise and very high gain. Happily, the design of such equipment has been made easy with the arrival of very-low-noise amplifiers and receivers using gallium arsenide field effect transistors (GaAsFETs). The large market generated by ham radio operators and television receive-only satellite stations has encouraged manufacturers to invest in this type of research. Mass production of these devices has brought their cost down to within the budget of the average radio astronomy amateur.

Basically, amateur efforts in this discipline fall into two general categories:

1. Indirect methods — for studying solar phenomena, meteor infall and Jupiter noise storms, for example. This is usually done at the low radio frequencies, with relatively narrow-band receivers. It does not involve sharp imaging of the radio noise source. The readout instrument is usually a strip chart recorder or a computer.

2. Imaging radio astronomy — this work makes up the bulk of amateur radio astronomy efforts. It is, by its nature, best practiced at higher frequencies, with broad-band receiving equipment.

The purpose of the Society of Amateur Radio Astronomers (SARA) is to provide sufficient technical information to enable amateurs to do this kind of work. Such information circulates freely within the society and is regularly published in SARA's monthly 24-page journal, *Radio Astronomy*. Additional specific information is available from SARA's technical advisors, many of whom are radio engineers.

You are invited to survey the potential of each radio band, and to evaluate your own potential. Specific design information may be secured from the SARA Journal office, or from SARA's technical advisors.

(The following band descriptions are adapted from the *Radio Astronomy Handbook* by R. M. Sickels, 1986.)

20-100 kHz

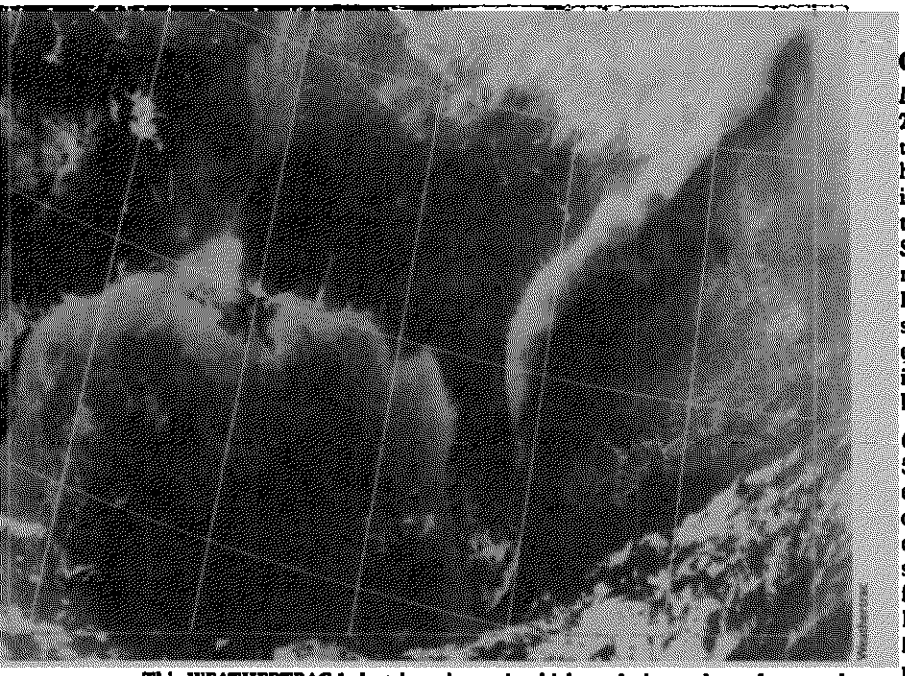
This noisy radio band is useful in observing solar flares. The plan involves simple receivers of very inexpensive design and which are usually home-built. Antennas may be long-wires, loops, and in some instances amplified whip antennas for those who lack the space for more elaborate arrays. The cost of the basic receiver may range from $30 to $60. To this must be added the cost of a strip recorder, which may be bought quite cheaply at some of the ham radio flea markets, but may range from $350 to $700 if purchased new. The observing technique involves the continual monitoring of Earth-produced atmospheric noise (mainly equatorial lightning discharges) for any enhancements due to solar flares. These observations are regularly conducted by a dedicated group loosely affiliated with SARA (the VLF Experimenter's Group), and the data are useful to professional solar observatories and to all others who have an interest in our closest star.

Jeff Lichtman is a founder, and now president, of the Society of Amateur Radio Astronomers (SARA). For more information, and/or help starting a radio astronomy project, contact SARA Membership Services, 247 North Linden Street, Massapequa, NY 11758. —*Robert Horvitz*

- a receiver that can tune the 137 MHz satellite band, with channel bandwidth of 30-50 kHz
- a video detector/demodulator
- an analog-to-digital converter
- a computer interface
- image formatting software
- a computer with a monitor that can display at least 16 gray-tones, with resolution of at least 640 x 480 pixels.

Note that the video detector and a/d converter are often combined on a printed circuit board that fits in a computer's expansion slot.)

Polar satellites move across the sky. Tracking them with a directional antenna requires software to calculate when and where to point the antenna, plus a mechanism for steering it. Much easier is using a nondirectional antenna that can acquire signals from a wider field of view, with no aiming or tracking. The most popular nondirectional design is the "Turnstile-Reflector," easy to build for around $35 (see photo). Plans have been published in several places, including Taggart's *Weather Satellite Handbook*. Vanguard Labs' WEFAXTENNA is a prefab of somewhat similar design, for folks lacking the tinkerer's impulse. "Quadrifilar helix antennas" are also getting popular. Their virtue is that they can gather signals from a broader sky-region without moving. The downside: they cost more ($250-$300).



This WEATHERTRAC Industries printout is a high-resolution, enhanced-gray-scale fax with a grid overlay showing the Gulf and Florida regions taken from a NOAA infrared range.

ADDITIONAL RESOURCES

NOAA/NESDIS publishes a bulletin for "direct users," with status news about US and foreign wesats, upcoming conferences, contacts, NOAA services, etc. Publication schedule is somewhat irregular, contents are very useful. To get on the free mailing list, write to: Mona Smith, E/SP21, NOAA/NESDIS Data Collection & Direct Broadcast Branch, Room 806, World Weather Building, Washington, DC 20233.

The Journal of the Environmental Satellite Amateur Users' Group (JESAUG) focuses on more advanced hardware/software innovation. Outstanding. To get it, you join JESAUG. Jeff Wallach, editor. $30/year (4 issues) in the US, $40/year elsewhere, from the Dallas Remote Imaging Group, P. O. Box 117088, Carrollton, TX 75011-7088.

Satellite Imagery Interpretation For Forecasters — This three-volume set, published in 1985 for NOAA, is now available from the National Weather Association (4400 Stamp Road, Room 404, Temple Hills, MD 20748; 301/899-3784). Cost is $32 for members, $45 for non-members. NWA membership is $20/year.

COMPUTER BULLETIN BOARDS

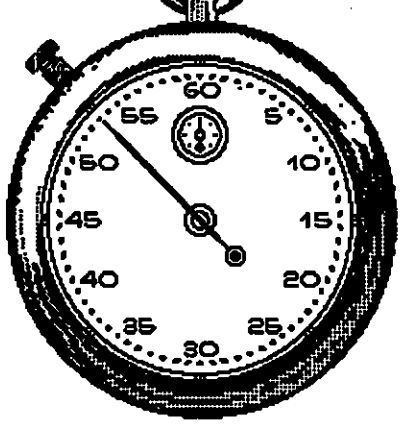
Datalink BBS (Jeff Wallach, sysop; 214/394-7438 in Dallas, Texas): A fantastic resource for anyone interested in ham radio, satellite monitoring or digital image processing. Jointly sponsored by the Dallas Remote Imaging Group, AMSAT North America, and the Environmental Satellite Amateur Users Group. Has current AMSAT and NOAA Bulletins, satellite frequencies, current orbital elements (necessary for tracking), launch information, voluminous picture files, lots of shareware, tutorials, etc.

Celestial RCP/M BBS (T. S. Kelso, sysop; 513/427-0674 in Fairborn, Ohio). Sysop edits and distributes electronic editions of NASA's "Prediction Bulletins" giving current "Keplerian" orbital elements for satellite tracking. Always available here first. Focus is on astronomy and satellites, also carries electronic editions of NOAA WEFAX Bulletin. With recently upgraded BBSware, new features are still being designed and added.

NOAA.DRUSER Electronic Bulletin Board: This free service run by NOAA/NESDIS is moving to a new computer-home on September 30th. The new phone number isn't yet known as we go to press. Assuming it will continue much as it is now, this is where NOAA posts electronic announcements about changes in satellite status, orbital elements, and electronic editions of their "direct user" newsletters. Write to Mona Smith at NESDIS for the new number.

Several wesat equipment vendors also run BBSs, not just to promote their products but to help spread useful information and shareware. See listings above. ■

A One-Minute Course On How To Do T.V.



BY RICHARD FREEMAN

A SHORT TIME BEFORE I DROPPED out of Anthropology, I was regaled with what I now think of as suburban legends. The one I still remember concerned a tribe somewhere that was shown, perhaps on a bedsheet hung from a tree limb, their first motion picture. No one in the tribe knew what to make of the action. Instead, they all followed a chicken that was in one of the scenes. I wonder (not only what movie had a chicken in it but whether this story could possibly be true).

What makes me wonder is my experience producing television programs. I've helped set up a TV station in town for almost no money at all, and I've watched fifth-graders learn to use all the equipment in under 15 minutes — and go on to do their own shows with interviews and trivia contests and music. Either the technology is very simple or we are watching a miracle.

Whenever I teach someone how to use a TV camera, I always feel like apologizing that it wasn't more complicated. That there isn't more to learn and more to say. The only trick is learning that it is this easy. What stops most people, I think, is the idea that TV is terribly technologically complex and expensive . . . whereas all that you need, if you have cable access, is a camcorder and about $500 worth of sound equipment. Anything else is gravy.

First you need to live in a small town with a cable access channel that isn't being used. I assume there are lots of towns like mine — Yellow Springs, Ohio — that have that cable capability but haven't used it yet.

Certainly the equipment needed is simple. For the audio, we use a Radio Shack control board (the under-$100 model works fine) which allows us to plug in three microphones, a cassette deck, and a CD player. Add a small pair of $50 monitor speakers, some wire, and a telephone and you can go on the air as a radio station.

To do just radio (over the TV), all you need to do is plug a connection cord from the board into the tuner that's hooked up to the cable modulator.

The next step is to produce TV. To do this you need a camcorder and a tripod. It too plugs right in.

Kids learn to handle the camcorder in under a minute (all there is to learn is what button to push to zoom in and out). Another five minutes will be enough to show everyone how to work the control board. They already know how to use cassette decks and CD players.

Kids have watched enough television (unlike those poor tribesmen) to know exactly how it's done. Whatever else needs to be taught, they'll teach you.

Our studio is a basement room in the village building. Though most of it still looks like a combination of Castle Dracula and junk storage, one wall has a gray rug hung on it. With a table in front of the rug and a couple of home-made spotlights, we have a set that looks great on TV.

The trick to producing television seems to be to teach the kids how to use all of the equipment as quickly as you can and then, the same night, let them do their shows. When an audience shows up to watch, you can teach them as well. And there is an audience. Our kids get 80 phone calls in a half-hour trivia contest.

I find it particularly funny that I can produce TV and use a computer while I don't know how to drive a car. In 1962 only a few people could do the first two and I felt completely out of things not being able to do the latter. This century is just full of such jokes. ■

The Jolly Roger is hoisted in Leipzig, in front of the building where video artists broadcasted East Germany's first pirate TV station.

Pirate TV in Eastern Europe

BY EVELYN MESSINGER

Evelyn Messinger is a television producer specializing in international news. She is a founding member of Internews, a non-profit consortium of independent video newscasters. Their most recent noteworthy projects have been Space Bridge events — live TV hookups with Moscow citizens and officials. —Kevin Kelly

TELEVISION HAS PLAYED an increasingly significant role in the downfall of Eastern Europe's one-party states. In Poland, underground pirate video transmissions kept Solidarity alive for nearly 10 years. Last fall, East Germans judged the effects of their anti-government demonstrations by watching the coverage they received on West German news programs. In Romania, control of the television station is tantamount to control of the government.

Now another aspect of the newly flexible television medium has come into play. Independent broadcasters using jerry-rigged transmitters and home video equipment have sprung up in Poland, Hungary, Romania and East Germany, intermittently broadcasting programs ranging from rock videos to local news reports. Even in the USSR, unofficial pirate broadcasts have taken place, and are credited with aiding the election of radical candidates to government posts in a number of cities.

In late March, I visited the city of Leipzig to investigate Kanal X, East Germany's first and only pirate TV station. Kanal X is a lever stuck into the ironclad media armor of Europe. The lever is slender and fragile, but with the right amount of pressure it could open a large hole, allowing independent broadcasting into the future of Europe, both East and West.

PIRATE TV

To Americans, pirate TV means the guy whose face appeared illegally on a cable TV channel a few years ago. Acts like this are rare in the US, because they're not necessary. Independent producers and activists here have historically agitated for, and often won, access to the spectrum of channels. There are allowances and avenues for all types of broadcasting. The mighty Network is balanced by the lowly low-power

In Poland, residents bypassed the government's monopoly on TV by installing their own backyard satellite dishes to pick up Europe-wide broadcasts. Programs were taped off the air and duplicated in small-time basement and attic shops on VCR cassettes, then peddled around the country.

station, and virtually all cable systems have some form of public-access programming.

Access to European television, on the other hand, has largely been constrained by government controls. The recent emergence of new technologies in the West has loosened things up somewhat, increasing the number of channels transmitted by satellite, cable and broadcasting. In the face of inevitable change, some countries foresaw the need for independently produced programming and for guaranteeing independent voices some access to the airwaves. In the UK, a new channel (Channel 4) was established in the early eighties. Although commercial, its government-dictated mandate was to have programming which was produced almost entirely by new, small production companies. This single channel became an outlet for all manner of unusual viewpoints, and although Channel 4 has since grown more conservative, the independent companies established by it still flourish, providing a limited counterpart to US diversity.

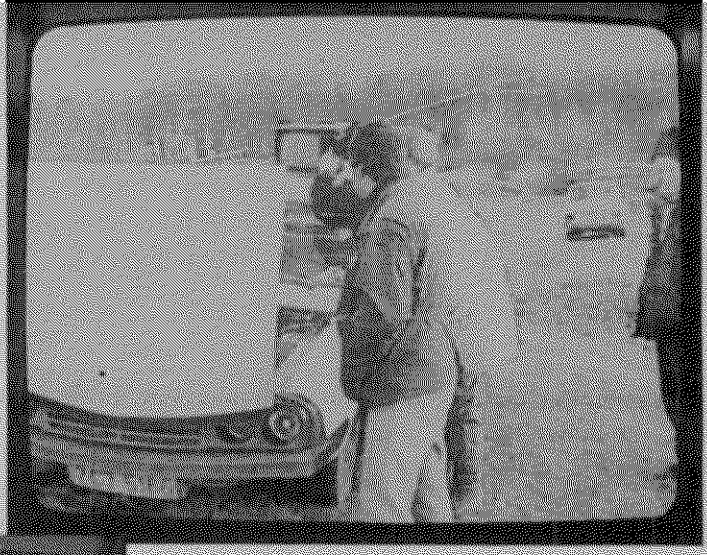
In Italy, a Supreme Court order guaranteed media proliferation as an aspect of free speech in the seventies. Italy has since fostered what is probably the most diverse television landscape in the world. Every sort of television program imaginable exists there, from nude game shows to coverage of community meetings. Inspired by the Italians, France has recently allowed greater access to TV outlets for independent producers, although channel ownership is more tightly controlled than in Italy or the US.

But the proliferation of new cable and satellite outlets in Western Europe has generally been given over to large media conglomerates which are pan-European, and often global, in scope. These include established publishers like the German Springer Group and the Australian-based News Corp. of Rupert Murdoch. These satellite- and cablecasters have helped to shut out small independent voices in favor of endless American re-runs, locally produced Wheel of Fortune clones, and slick rock videos produced by megabuck record companies.

The medium's development in Eastern Europe has taken a different turn. Pirates here are often dedicated idealists broadcasting a message not to the liking of governments in power. Technology is everything in this context. As equipment has gotten cheaper and smaller, the success of clandestine transmissions has improved.

Before the advent of miniaturization, not only could tyrants terrorize with abandon, but they controlled the spin on news reports of their deeds. No one outside of the USSR, for example, knew what Stalin was doing, because there was no way for an activist to videotape the mass graves, let alone transmit the images to the world. Consequently there were few activists, and no repercussions. But as early as the 1960s, TV technology had progressed to a point where it could begin to change things. The earliest example I've found of Eastern European pirate TV is a series of clandestine broadcasts in 1968 in Prague, Czechoslovakia. After Soviet troops took over the city, a remote TV van, designed to transmit signals from soccer matches and the like, was diverted and secretly dismantled. The equipment was set up in a sealed room and anti-government transmissions took place for many months. The Soviet tanks, which could be seen circling the block below the station's secret headquarters, never found the transmitter. Poland's Solidarity movement had a similar system of clandestine broadcasting through the political repression of the eighties, but by this time the necessary

Romanians discovered that they could pick up Western TV by driving their cars to the nearest western border, parking in countryside lanes, and tuning in with a TV plugged into the car's battery. Of course one may have to stand holding the aerial to get a decent picture. And of course, something to drink makes it all even better. What's on? Music videos, soap operas, sports.



equipment could be carried from rooftop to rooftop in a set of suitcases. By the time these repressive governments collapsed (partly from the weight of sins that were no longer hideable), the videos of their undoing could not only be made by anybody with a home video camera, but could be transmitted to local audiences by anybody with a VHS player and a rudimentary understanding of how to do it.

So, today:

• In Lithuania, the much-suffering USSR rebel state, a daring and unusual pirate broadcast took place in autumn 1989. The Moscow city channel is rebroadcast there on UHF channel 22. After it signed off one evening, a "test transmission" was beamed from the Experimental Youth Studio of Siauliai in northern Lithuania. The transmission included a tour of the regional prison and army base, and local celebrity interviews.

• In suburban Moscow, Leningrad, and Kiev, village-sized apartment complexes are equipped with master antennas and complex-wide cable systems. They often have their own "local" channel, broadcasting exclusively to the 20,000 or so residents of the complex.

• In Romania, Free Timosoara Television (FTT) began transmitting with home-built equipment shortly after the uprising that ended Ceausescu's rule. The station is now protected by soldiers who were assigned to the task by the provisional government.

• In Hungary and Poland, a number of small-scale independent broadcasters, born during their respective revolutions, have achieved legitimization in their countries as exceptions to obsolete broadcasting rules.

• And in Leipzig, East Germany, the tiny Kanal X covers local news and rebroadcasts reports from around the world pulled off the Western satellites.

Ironically, these tentative forays into small-scale broadcasting have the potential to enhance the diversity of television all over Europe. But if the Eastern European countries simply adopt Western European patterns, they will inherit a system which is top-heavy with state-run bureaucracies and the increasingly powerful Pan-European commercial broadcasters.

East Germany, which can simply "plug in" to the existing West German television system, will integrate more easily than most. The experience of Kanal X may foreshadow the future of all the new Eastern European broadcasters.

LEIPZIG

The city center of Leipzig, East Germany, is a press of shoppers and their children. Under grey skies and Gothic facades, they crowd around tables heaped with vegetables, tall stacks of West German beer cases, and brightly painted mobile trailers selling french fries or cream-filled waffle sandwiches. The most popular items for sale are West German magazines. At the heart of the largest clusters of people one finds a small cardboard box with two stacks, one of *Der Spiegel* and one of *Stern*, West German equivalents of *Time* and *Newsweek*. They are expensive by East German standards, yet they have been selling so well that many local East German papers, born during the revolution, have been forced out of business.

I get a strange feeling of deja vu in the streets of Leipzig, but I can't place it — certain buildings, and even rooms inside buildings, seem out of place, yet familiar. Finally I realize that the city is dotted with Soviet-style architecture, incongruously grafted onto this European landscape. A "people's restaurant," massive and 1950s-style on one corner; a dimly lit coat room, with hundreds of empty hooks and hangers designed for a colder climate. I marvel that the Russians could have dominated this foreign territory for so long.

In a run-down section of Leipzig stands Democracy

House, the headquarters of the home-grown political parties, rights groups and activist organizations that lead the famous Monday night demonstrations which toppled the government of the city (and the nation). These are the ones who *didn't* leave for the West, the sort of people who would lead a peaceful revolution, and who would now be buzzing around the door of Kanal X.

"ARE YOU INTERESTED IN MAKING TV?"

If you live in Leipzig you might have had your TV antenna tuned southward, to pick up West German signals from Bavaria (East Germans are world-renowned for their expertise with TV antennas). On March 17, 1990, you would have received the first signals of Kanal X. The first show: an East German video artist's work, as rare as the East Germans with access to video gear. Then, a home-made "news" story with street interviews about the upcoming election, then a nightly news report, in English, from CNN.

Perhaps it's more accurate to say that this is what you were supposed to see. Many who watched saw lots of static, faint video signals coming as if from Mars, and that's all. The station was beaming out 8 watts in a tenuous link to the world, obstructed by insufficient power and a tall building next door.

Over the last four months, Kanal X has only been on the air a total of four nights. Although the transmitter has been improved, reception is still marginal. But the effectiveness Kanal X lacks in broadcast power is made up for in the power of its idea to set off deep legal speculation, bureaucratic opposition, heavy media coverage locally and internationally, and even debate in Berlin, where new laws are being considered.

Kanal X began in the mind of West German video artist Ingo Gunther, whose works often suggest bridges between journalism and art. Gunther has sold Earth imagery made by satellites to the world's news organizations (see *WER* #50, p. 62) and to museums in Europe. He has used worldwide news reports as both the content and the form of his sculptures. The Kanal X transmitter, in fact, is officially a sculpture, being displayed in Democracy House.

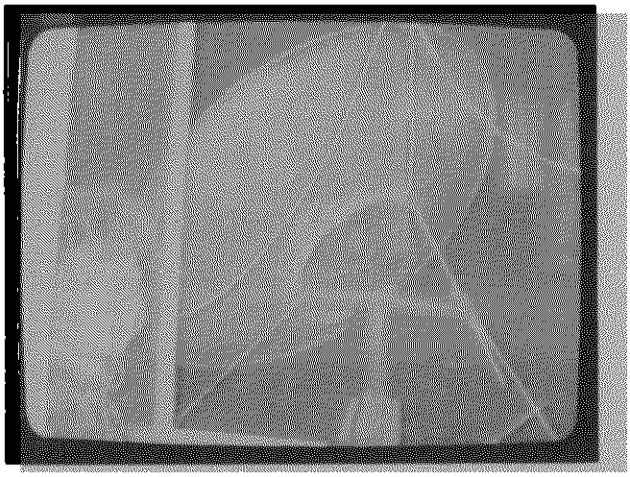
Working with Joerge Seyde of Leipzig's New Forum Party, Gunther enlisted two other West Germans, a professional who installed the transmitter and a video buff who donated his own home equipment. Joerge, who works at the local art museum, took nominal charge of the station. He enlisted his younger brother Thomas and other activists from the various parties located in Democracy House, with the question, "Are you interested in making TV?"

Thomas Seyde, at 33, is the oldest of these young guys (they are almost all males). They have long hair by current Western standards, wear tee-shirts, jeans and denim jackets. They might be heavy-metal aficionados in another world. Only months ago, they began demonstrating in the streets each Monday night. Now, Thomas is the cameraman, and a teen-age Green Party worker conducts interviews, although he's never been on TV before. On the afternoon of March 17, they are frantically editing their first videos for broadcast. At 10 PM that night, Kanal X goes on the air for two hours. It seems to work, although there's no way to know for sure.

Over the next few days, people call in to say they have been watching the station with varying degrees of success. Young people show up, asking if they can work there in their spare time.

On the second night of broadcasting, Joerge receives a visit from a representative of the Leipzig state post office, the PTT. This is the organization officially responsible for East German television reception and transmission. The man informs him that, since Kanal X hasn't a license, it must shut down. Surprisingly, the official rattles off every single program broadcast so far. Everyone is worried about this development, but also a bit proud that somebody got a good signal. After three nights on the air, Ingo and Joerge begin the bewildering process of attempting to gain legitimacy for Kanal X in a country with no laws. The station ceases to broadcast.

During this period, Thomas and the other KXers continue to "make TV." They shoot the opening night of Leipzig's first independent cafe, where young people have fixed their hair into a local approximation of punk. In the crowded cafe, as it appears on the video screen, everyone is smiling. Thomas gets a phone tip alleging that voters in an old-age home were forced to vote for a certain party in the recent election. He begins to check out the story. The KX kids are busy shooting and editing, building a library of stories against the day that they will broadcast again.



A Czechoslovakian woman shows off her homemade epoxy satellite dish, mounted on the balcony of her high-rise apartment building.

Meanwhile in East Berlin, the prestigious, newly formed Media Control Commission is debating the future broadcast landscape of East Germany. Rumblings of Kanal X reach their ears. The press continues to cover the now silent Kanal X, which was always more powerful than its transmitter.

X, LAWS AND VIDEOTAPE

The stacks of expensive West German magazines selling in downtown Leipzig can serve as a metaphor for the possible fate of Eastern European independent TV. When the West German news publications became available, everyone simply stopped buying local papers. Recently, East German Television (the only one) announced that it would soon merge into the West German national broadcasting system, a system with virtually no provision for independent outlets. As West German TV takes over, what will happen to Kanal X?

The signs aren't good. In May, Kanal X returned to the air for one night. By now, the station's story has been featured in East and West German newspapers, on the two West German TV networks and on East German Television's popular Youth Program. The PTT representative again appeared at the door of Kanal X, demanding that the station cease broadcasting instantly. He finally relented, allowing the program to finish, on the promise that it would be the last.

In the quiet streets of Leipzig, one senses the fragility of a lame-duck reality. The Kanal Xers are the people who stood in the streets and brought down the old world. Political entrepreneurs, they are being eased out of the leadership of the new enterprise in favor of cooler heads. In the final analysis, they are too idealistic.

Perhaps this is the fate of a truly successful revolutionary. A less successful one loses the Revolution but becomes a martyr. The spectacularly unsuccessful ones are those that end up in power.

Many Westerners, including a number of US foundations wishing to help enhance democracy, are beginning to pour money and expertise into Eastern European broadcasting. In my telephone polling of these groups, few were concerned that, by allowing mega-stations but not tiny broadcasters, these countries may be simply trading one form of broadcast tyranny for another. In light of the US public-access broadcasting battles of the 1970s, which assured a wide range of options here, are we really ready to tell these small broadcasters to either pack up their hard-won transmitters or begin broadcasting re-runs of Mr. Ed? Ingo Gunther fears that, with their lack of technical training, East Germans will not even be eligible for jobs when the Western media swallows up their broadcasting. As it was with the newspapers and magazines, the locals won't have a chance.

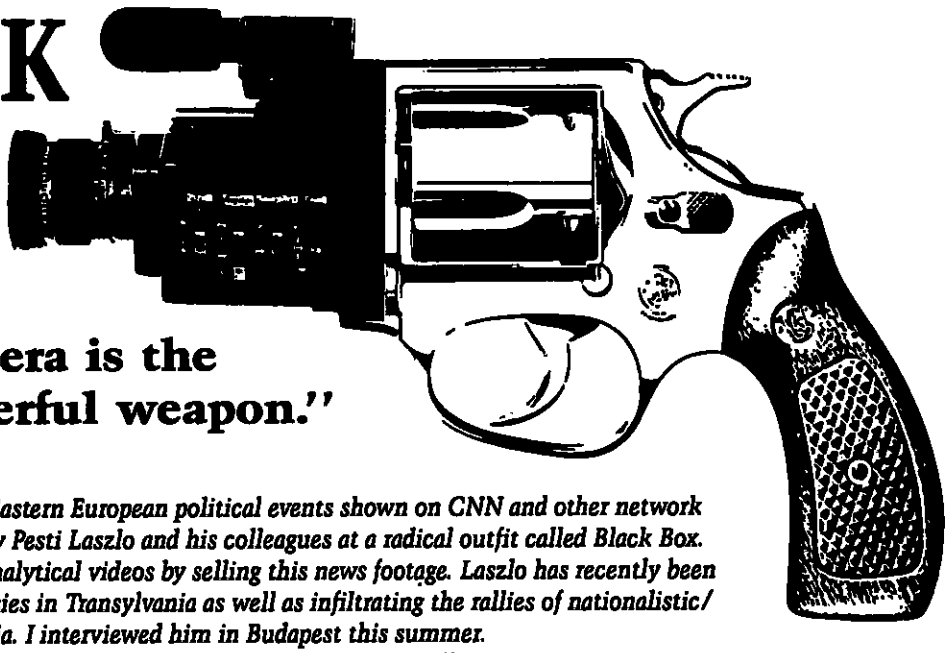
But even if it never broadcasts again, Kanal X could change the future of German television. The fact that small independent stations already exist all over Eastern Europe gives them leverage to become institutionalized in a way that was never considered in Western Europe, and that could buck the ominous trend. Now that they have gained a foothold, these little guys are fighting to have themselves written into new broadcast laws. This is one area where American expertise can really help. But if American supporters assume that rampant commercialism is the same thing as freedom, then this is one battle that those who went to the barricades will surely lose.

Back at Kanal X, two bleary-eyed young men learn to edit videotape. The transmitter sleeps, the satellite dish sits silent. Occasionally someone walks in and asks about the station. Come back next week, they say, maybe then. Thomas begins to fiddle with the camera. Tonight they have an appointment to shoot a squatter community, young people who are inhabiting a derelict building in the older part of Leipzig and making it new.

Thomas picks up the camera, and throws it onto his shoulder. "I'm hot!" he grins, heading for the door. ■

The opening logo of Kanal X, East Germany's underground TV station, which relied on amateurs with no previous video experience to pick up camcorders and make TV.

BLACK BOX



"The camera is the more powerful weapon."

Much of the footage of Eastern European political events shown on CNN and other network news programs is shot by Pesti Laszlo and his colleagues at a radical outfit called Black Box. They subsidize longer analytical videos by selling this news footage. Laszlo has recently been working among the gypsies in Transylvania as well as infiltrating the rallies of nationalistic/fascist groups in Romania. I interviewed him in Budapest this summer.

—Morgan Russell

THERE IS A GREAT and long tradition of illegal political literature, called "samizdat," in Hungary. But visual samizdat is a more recent phenomenon, appearing all over Eastern Europe, as well as in Moscow, Leningrad, and Armenia in the U.S.S.R. at the end of the eighties. In Eastern Europe we call this Second Publicity. This unofficial news circulates side by side with the official news sources, called First Publicity. It includes gossip, what people discuss informally in the street, illegal printed materials and, finally, video documentation.

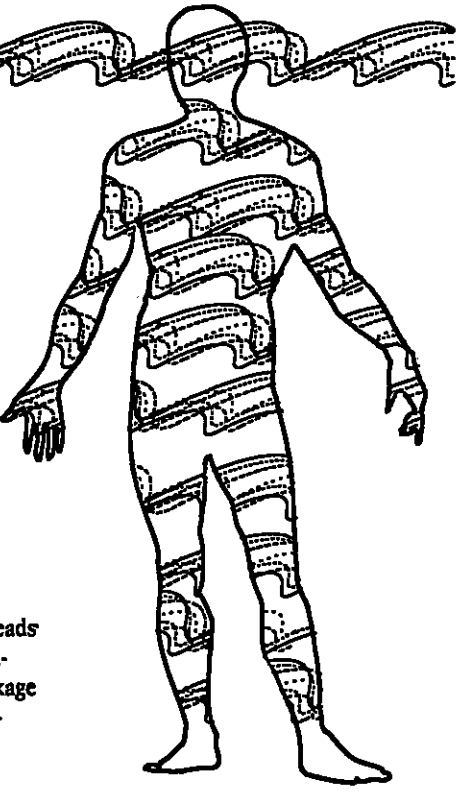
The video medium is more like the printing press than filmmaking is. Publications can be produced in any number, and circulated in the streets under the poorest conditions. Black Box appeared thus, as a video periodical in regular editions. In most cases, we issued two to three hundred copies. Did these cassettes have any effect in a country of ten million? Obviously it could not have had a large-scale influence. Still, it did reach the "alternative intelligentsia," who had a primary role in transforming Hungary during these last two years. This active layer of society was able to obtain information and form its views accordingly.

When the "sweep of history" in Hungary became somewhat calmer last summer, we started to work abroad. We were in Prague well before the changes there, in the GDR, the Soviet Union, in Karabah and in Kosovo. There is no esthetic, sociological, or professional knowledge implied in this activity: rather it requires an ability to run fast when you have to, to realize exactly when you have to keep your mouth shut, and when to change your car's number plate to a new one. It resembles conspiracy or espionage. We have been arrested, imprisoned, beaten up and involved in car chases. We made our films with tear-gas sprays in our hands to defend ourselves.

We have worked with our camera in Romania many times. That revolution was one of the most elevating experiences for us. At that time, we thought a whole nation was able to change during a single day, to transform its views. Since then we've realized that this was only an illusion. Imagine us being in an enclosed city, all roads blocked by tanks, no European journalists allowed. We are there and we witness a massacre starting at 6 PM sharp. My camera sees and records Romanians arriving at the demonstration with axes and pitchforks — a demonstration where there are Hungarian people standing defenseless, without weapons. When the Romanians start with their pitchforks, when our cameras record the first dead people, there is no one else there to record it but the Romanian television. The next day, it shows some of the events and announces that Hungarian people attacked Romanian people. Twenty million Romanian people watch this web of lies on the screen.

But there is something on which the official communications system does not count: the outsider's camera. Our cameras actually become weapons in our hands: we can "shoot" ministers and Prime Ministers. These people will not be able to continue lying. The camera and the gun physically resemble each other, but the camera is the more powerful weapon. If I had had a real machine gun with me there, I could not have caused more harm to my political opponents.

We are on our way back to Romania. Recently, one of our colleagues was killed there after a police "interrogation." The fascist organizations do not allow journalists to visit their events, they break cameras and attack cameramen. They recognize that the camera is a weapon, and that the video marksmen of Eastern Europe, from the Urals to Berlin, from Vilnius to Bucharest, are taking aim. ■



Inhabiting the Electromagnetic Environment

BY ROBERT HORVITZ

IT'S A PUZZLE. On the one hand you have folks sticking their heads in electronic "tuning" fields, as some sort of brain-boost or non-chemical psychedelic, and on the other you have folks afraid of leakage from video monitors, microwave ovens and power lines. Are electromagnetic fields (EMFs) a neat high or a lethal hazard?

Maybe both, maybe neither. Maybe we just don't know.

There's been an upsurge recently in public concern about the invisible fog of electromagnetism we live in. It must concern us because that fog has thickened so much this century, and it permeates our bodies. Every electric motor, appliance and current-carrying wire radiates energy as a byproduct of normal operation. We also use radio to communicate, as in broadcasting, cordless and cellular phones, beepers and CBs. Microwave ovens are popular. So are electric blankets and stoves. Radar is used by police departments, meteorologists, aviators and navies around the world. Metal detectors, remote-controlled toys . . . the list goes on and on.

We can't see these emissions. That used to mean we ignored them. But now that a wide range of biochemical effects has been attributed even to weak EMFs, invisibility feeds fear: we don't know when or how much we're being exposed. Exposure is likely anywhere that electricity flows, and our dependence on things electric grows daily.

There's some consolation in knowing that this wave energy penetrates our bodies precisely because we absorb so little of it: we are nearly transparent to radio. And compared to sunlight, which can sear flesh in a few hours, low-frequency EMFs are "soft." The sun's ultraviolet rays are a much more immediate health threat.

Which partly explains why research on the biological impact of EMFs got off to a slow, faltering start. Another reason is that bioelectricity seems to attract charlatans and quacks like no other subject. That has made funding agencies and serious scientists leery. Plus, some people in high places oppose research whose findings could impede "progress," raise business costs, establish liability, or encourage regulation. Shutting down the Environmental Protection Agency's research program on EMFs in 1986 was one of the Reagan Administration's many low points.

Despite the prevailing skepticism and lack of funding, interest in EMF bioeffects increased during the 1980s, after some curious results were found in lab experiments, and a statistical study showed associations between powerline EMFs and serious illness. Federal inaction in the face of growing public fear led some local governments to impose tight restrictions on EMF sources. As the patchwork of local standards spreads, it's starting to look like the cost of *not* doing the research needed to establish consistent and reasonable safety standards may be higher than doing it right.

A few hints of consensus have started to emerge from the work done so far. With caveats galore (I'm no doctor, we still don't understand the mechanisms, not everyone agrees), this fool rushes in where a lot of other fools have already been mucking around:

- First, don't panic. If you ride by car or bike, live in a major city or a mobile home, you're already facing bigger health risks than EMFs.
- Many bio-effects seem to occur at specific combinations of frequency and power, suggesting that molecular resonance is involved. If that's the case, setting exposure limits across the broad spectrum will be difficult. (To use a plumbing analogy, your pipes may "sing" when water flows through them at a specific rate. Decreasing the flow will stop the singing; but so will *increasing* it. And when the water is at a different temperature, the singing starts and stops at different flow-rates. This kind of nonlinear relationship between "dose" and effect means that at certain frequencies,

a weak EMF might have more impact on a specific chemical reaction than a stronger one does.)

• The orientation of the field, the coherence and shape of the waves, the way they're modulated (AM, FM or pulse), the peak versus average power density — any or all of these may be important variables. They complicate setting exposure limits, too.

• Magnetic fields may be more of a health problem than electrical fields, though they are often found together. TVs and video terminals, small motors (hair-driers, fans and plug-in clocks), fluorescent lights and electric blankets, are typical sources of magnetic fields in the home. Magnetic shielding (as opposed to electrical shielding) is generally impractical. However, the magnetic fields from most appliances fade to below the background level a few feet or yards away.

• The magnetic fields of powerlines have a farther reach. They are more intense where there's an unbalanced load and the voltage is stepped down by a transformer. You can easily check for "hot-spots" in your neighborhood by walking around with a portable radio tuned to a vacant channel at the low end of the AM band. As you near a radiating section, you'll hear a loudening buzz.

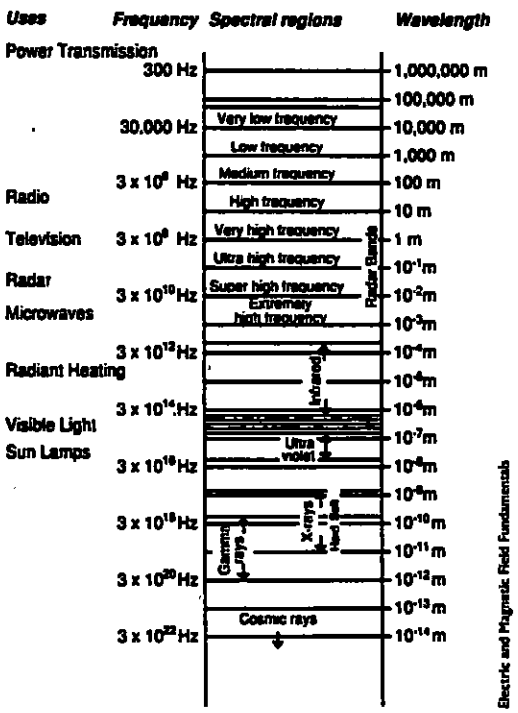
• If you have a microwave oven, have a professional repairman check the seal around the door at least once a year.

• Electric blankets have been singled out as something to avoid because they are meant to be used close to the body for long periods of time. Consider a down comforter instead.

It's important to keep in mind that not all of the recently discovered effects are necessarily harmful. Some may have no health impact at all, and some may ultimately prove beneficial. The real pay-off in EMF bioeffects research may not be just in minimizing risks, but in the development of positive applications. It is already clear that there are therapeutic uses — in bone-healing and pain relief — as well as new imaging techniques which eliminate the need for exploratory surgery. If EMFs can in fact promote or inhibit certain chemical reactions, we may able to harness that ability for desirable ends.

As we learn more about these invisible energies, we may well come to regard our current fears as just part of the shock of seeing with "new eyes." As I. M. Sechenov once wrote:

> It is highly instructive to hear people born blind describe their impressions of the world around them in the first few days following an operation restoring their sight at an adult age. Although such people had already had clear spatial notions concerning all the objects around them . . . the whole field of vision appeared to them to be filled in some solid manner, which seemed in some way to touch their eyes, and they were even afraid to move lest they should stumble upon this or that image. □



NATURAL EMFS

To keep our emissions in perspective, note that the Earth has a very active electromagnetic field. Its churning iron core generates a halo that reaches far beyond the atmosphere. "Ground currents" seep through rock and soil, sometimes causing geomagnetic storms that disrupt power line transmissions. Lightning releases some of the enormous static charges that build up in the atmosphere. Meanwhile, solar flares and sunlight ionize the upper air, producing swirls of charged particles that swathe the Earth. We rarely notice it, but our environment is permanently electrified by the interaction of geomagnetic and solar weather. (See "Sferics," p. 88.)

Natural EMFs buffet us intangibly. Whatever effect they may have, we've had eons to adapt. Human-generated EMFs have only been around for a few generations, and are quite different from natural fields in terms of frequency, waveform, coherence, distribution, etc. We don't yet know what difference these differences make.

The Earth's Electrical Environment is a collection of papers surveying what is known, and not known, about lightning, aurorae, ground currents and the ionosphere, how they interact with each other and with human systems. There's only a few oblique references to bioeffects, but this is the only book I know of that tries to pull together the various aspects of the Electric Earth.

The Earth's Electrical Environment
1986; 263 pp.

$28.95 postpaid from National Academy Press, 2101 Constitution Avenue NW, Washington, DC 20418; 202/334-3313

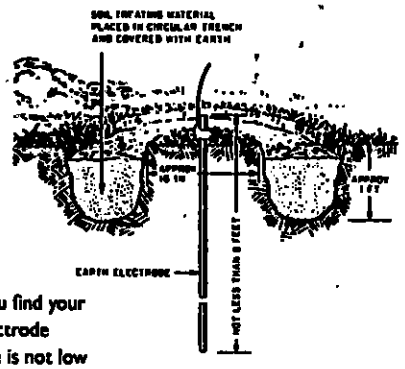
If you have a shortwave radio, you can tune in current solar and geomagnetic weather reports on stations WWV and WWVH. Audible throughout North America and beyond, they're broadcast at 18 minutes past the hour on 5, 10, 15

and 20 MHz. For more detailed current information, if you have a computer and modem, you can call the NOAA Space Environment Services Center's Forecast and Advisory BBS in Boulder, Colorado (303/497-5000 at 1200/300 baud; or 303/497-5042 at 2400 baud).

Good electrical grounding is important for safety (to protect you and your equipment from unwanted current discharges) and for circuit performance (to improve the efficiency of antennas, for instance). Unfortunately, most people's understanding of grounding begins and ends with using an adaptor to plug a three-prong plug into a two-prong socket. *Getting Down to Earth (Manual on Earth-Resistance Testing for the Practical Man)* is a pamphlet which tells in simple, practical terms how to find and establish good ground. Oriented toward large installations, the concepts and rules apply just as well to any scale.

Getting Down to Earth
1982; 48 pp.

$1 from Biddle Instruments, 510 Township Line Road, Blue Bell, PA 19422.



When you find your earth-electrode resistance is not low enough, there are several ways you can improve it:

1. Lengthen the earth electrode in the earth
2. Use multiple rods
3. Treat the soil

Effect of Rod Size: As you might suspect, driving a longer rod deeper into the Earth materially decreases its resistance. In general, doubling the rod length reduces resistance by about 40%.

—*Getting Down to Earth*

MONITORING EQUIPMENT

One of the neatest widgets I've ever seen is the Ambient Power Module, invented by Joe Tate, the Harbormaster of Sausalito. It's essentially an untuned, broadband radio receiver, simple enough to build yourself. Attach a long piece of wire as an antenna (100+ feet, preferably) and a connection to ground, and the Module will draw a small trickle of current right out of the air. (Cross a "cat-whisker" crystal radio with a solar cell, and you have the basic idea.) Output varies with the quality of the antenna, ground, and the energy in your air-space. Typically it's a couple of milliwatts — just enough to run a digital watch or calculator. Not many people will want to put up a 100-foot antenna to drive a calculator. However, you can also use it as a crude measuring device for EMFs (see "Radio Earth," p. 101), by hooking it up to a meter, a strip-chart recorder or a computer (with appropriate interfaces). It won't tell you anything about the frequencies, modulation or where the signals come from, just the cumulative field-strength. Prebuilt units aren't available; instead you can order an illustrated booklet containing easy-to-follow instructions on how to build it yourself. All the parts are cheap and widely available.

The Ambient Power Module
Joseph Tate, 1987; 16 pp.

$5 postpaid from Ambient Research, P.O. Box 153, Sausalito, CA 94966

There's so little agreement about what spectrum bands and features are important to measure, that I won't venture a recommendation of the best model of EMF monitors . . . though I do have a sentimental favorite: Monitor's Model 42B ($350 from Monitor Industries, 6112 Fourmile Canyon, Boulder, CO 80302; 303/442-3773). This is produced by Ed Leeper, who built the magnetic field gauge used by Nancy Wertheimer in her trailblazing study of powerlines and leukemia in Denver (described at the opening of Paul Brodeur's *Currents of Death).* We all owe Ed a great deal for his contribution not just to that project, but to the revolution in attitudes it sparked. *Microwave News* (reviewed below) recently surveyed equipment marketed for the measurement of EMFs in ways relevant to the health issue. The 15 listed units range from sophisticated lab equipment to simple consumer products; in price from $75 (Model 116 from Electric Field Measurements, Box 326, West Stockbridge, MA 01266; 413/637-1929) to $9500 (Model 3D-MFDM, Sydkraft AB, Carl Gustafs Vag 4, S-217 01 Malmo, Sweden). The majority of these devices have been on the market for less than a year; no one has yet done rigorous comparative testing. Since they measure different bands in different ways, they aren't exactly comparable anyway.

ARTIFICIAL EMFS

Research is moving so fast in this field that newsletters are the only way to keep up. *Microwave News* and *VDT News*, both edited by Louis Slesin, are widely acclaimed by all sides as the best sources of reliable and current information. Slesin believes that emissions from computer monitors, and EMFs generally, are a serious health issue. But he's established a reputation as an "honest broker." When a well-done study is published showing no evidence of harm, or refuting a study that found something scary, Slesin reports it just as carefully, and with just as prominent a headline, as reports favoring the other side. As a result, he's been much more effective in changing the attitudes of researchers than more partisan reporters. Almost every study cited in *Currents of Death* was first reported in either *Microwave* or *VDT News.*

As you might have guessed, *VDT News* covers emissions from computer monitors, and worker-health issues related to office equipment in general. *Microwave News* is less accurately titled. It covers the entire radio spectrum, not just microwaves, increasingly focusing on the low end of the spectrum (macrowaves?). *MN* is the more expensive of the two, but it has a lot more news per issue.

Microwave News
$250/year (6 issues); $285/year foreign. 212/517-2800

VDT News
$87/year (6 issues); $97/year foreign. 212/517-2802

Both from P. O. Box 1799, Grand Central Station, New York, NY 10163 ►

Stray fields from electronic devices not only affect flesh, they affect other devices. One McDonald's restaurant had a problem with some of their cash drawers popping open when a policeman keyed up his two-way radio at the drive-thru order window. People living near broadcast towers often hear the broadcasts on their telephone lines. Anyone with a computer and a shortwave radio or scanner knows that computers radiate a *lot* of broadband "hash" (the monitor and printer especially).

Reducing unnecessary emissions, and reducing vulnerability to interference, are complementary ways to limit unwanted interactions. Good design and production engineering can avoid problems before they happen. Shielding may also suppress leakage.

There's a whole industry now devoted to preventing, diagnosing, and solving problems of "electromagnetic compatibility" (EMC). Its leading trade journal, *EMC Technology*, is the place to learn about new detection gear, new shielding materials, and new regulations concerning EMF emissions. The editor has announced plans to increase the mag's emphasis on practical problem-solving.

EMC Technology
Keith Aldrich, publisher/editor

$40/year (7 issues/year) from EMC Technology, 5615 West Cermack Road, Cicero, IL 60650-2290

•

PC card fixes can be as simple as adding a bypass capacitor, series component, (choke, resistor, etc.) or by adding a two or three component network fix. Often such ordinary, inexpensive PC-sized components will eliminate the need for more costly external suppression methods such as shielded cables, metal plates within plastic housings, conductive coatings, metal housings, bulky ferrite or other expensive and inconvenient shielding methods.

—EMC Technology

Electric and Magnetic Fields From 60 Hertz Electric Power is a booklet produced by researchers at Carnegie Mellon University to answer the most frequently asked questions about potential health risks of exposure to electromagnetic fields. Written in layman's language, it recommends "prudent avoidance" of unnecessary exposures, where that can be done without much trouble or expense. It also advises against drastic or costly measures, until we have a better grip on what kinds of exposures pose what kinds of risk. A good introduction to the subject.

Electric and Magnetic Fields from 60 Hertz Electric Power
M. Granger Morgan
1989; 45 pp.

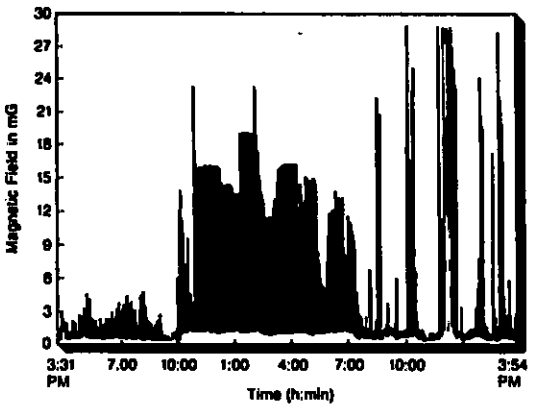
$3 postpaid from Dept. of Engineering and Public Policy, Carnegie Mellon University, Pittsburgh, PA 15213

Given the price and the depth of technical detail (as well as the extensive use of medical jargon), the book *Extremely Low Frequency Electromagnetic Fields: The Question of Cancer* may be best suited for people who are actually interested in doing medical research. The separately authored chapters cover a wider range of topics than the title suggests — from the impact of the microwaves fired at the US Embassy in Moscow, to the influence of light on the pineal gland. But the central focus is the question of whether ELF fields cause cancer.

As a layperson with no medical training, I was a bit surprised to discover that the mysteries of how ELF fields affect living things are still quite secondary to the more basic mysteries of how cells work (singly and together). The answer to the question posed in the book's title won't be found until we understand how cancer in general begins. This book argues that there's good reason to explore all of these mysteries simultaneously.

That's so even though most of the authors in this collection seem to think that based on what we now know, EMFs are not likely to cause cancer. However, they do seem to agree that some EMFs may interfere with biorhythms and the body's ability to suppress cancer once something else initiates it. There may also be other medically significant effects.

Thus, this line of research is worth pursuing for a variety of reasons. It is already providing new clues about how the immune system works, how cells communicate with one another, and how good cells go bad.

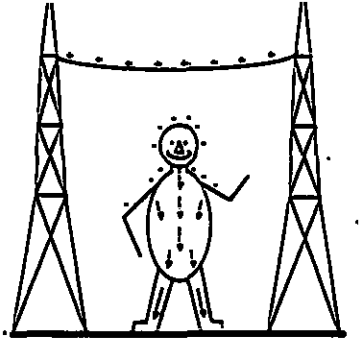


Magnetic-field exposure for an 8-year-old child shows a large increase in field level from electric blanket use at night. "Spikes" during daytime are mostly from exposures received traveling to and from school.
—Extremely Low Frequency Electromagnetic Fields

Extremely Low Frequency Electromagnetic Fields
Bary W. Wilson, et al., Editors
1990; 382 pages

$61 postpaid from Battelle Press, 505 King Avenue, Columbus, OH 43201; 614/424-6393, 800/451-3543

For an overview summary, a background paper published by the US Congress's Office of Technology Assessment is a reasonable place to start. *Biological Effects of Power Frequency Electric and Magnetic Fields* addresses powerline issues, summarizing the research in a relatively accessible, non-alarmist way. Also discusses policy issues, recent regulatory actions, and ongoing research programs. The report closes with pointers to current research, recommendations for future studies, and a bibliography. Reprints are available, and it should be browsable at most Government Document Depositories.



A schematic representation of the surface charges and internal currents that are electrically induced by the charges on an overhead power line in a person under the line whose feet are well-grounded. The total current induced to flow from each foot to ground is about 8 microamps per kV/m of applied field (1 microamp is 1 millionth of an ampere). The density of electrically induced current is the amount of current that passes through a body cross-section perpendicular to the direction of current flow. The current density induced by a 1 kV/m vertical electric field is about 30 nanoamps per square centimeter averaged over the entire volume of the body. One nanoamp is 1 billionth of an ampere.

—Biological Effects of Power Frequency Electric and Magnetic Fields

Biological Effects of Power Frequency Electric and Magnetic Fields
Office of Technology Assessment
1989; 103 pp.
Reprint # NTIS PB89-209985

$23 paper, $8 microfiche from Superintendent of Documents/Government Printing Office, Washington, DC 20402; 202/783-3238

Among recent books on these subjects, *Currents of Death* has certainly attracted the most attention. Author Paul Brodeur gives a pretty good overview of material originally published in Slesin's newsletters. But he differs sharply from Slesin in taking any skepticism about even the flakiest claims of injury from EMFs as proof that the doubter must be part of a massive conspiracy hatched by the US military, the electric utilities and the computer manufacturers, who want to wreak a Holocaust on the public and cover up their evil plan. For Brodeur, there's no such thing as a different interpretation of ambiguous data. There are no errors in the research of the pro-harm camp, fatal errors in every study from the no-harm camp. Reasonable people don't disagree: you're either pro-Life or pro-Death.

This is nonsense. It does a real disservice to the complexity of the scientific issues, and to the honest researchers in both camps trying to figure them out. The breakthroughs in understanding which are likely to emerge from this controversy are probably still cloaked in unresolved questions that Brodeur would dismiss as lame excuses for reactionary caution. If you read this book, make sure you read the OTA paper for some sort of balance.

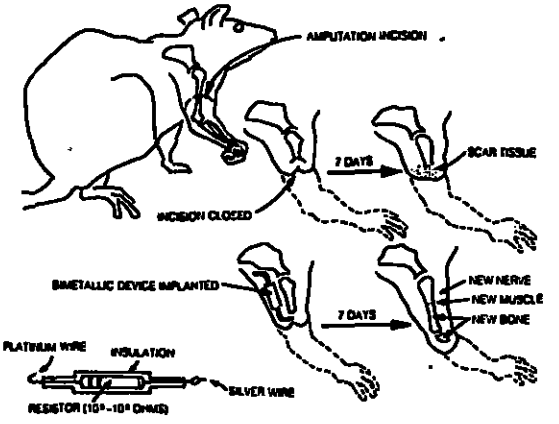
Currents of Death
(Power Lines, Computer Terminals, and the Attempt to Cover Up Their Threat to your Health)
Paul Brodeur, 1989; 333 pp.

$19.95 postpaid from Simon & Schuster, 1230 Avenue of the Americas, New York, NY 10020; 212/698-7541 (or Whole Earth Access)

Robert Becker is one of the pioneers of modern bioelectrical research. Now retired, he was an orthopedic surgeon who devoted most of his life to the study of bone-healing and "currents of injury" — weak electrical flows in the body that seem to stimulate tissue repair. *The Body Electric* (with co-author Gary Selden) presents a radical new theory of bioelectricity, based on Albert Szent-Gyorgyi's hunch that parts of the body are capable of acting as semiconductors (see *WER* #50, p. 55). When tissues with different electronic properties meet in the salty fluid of the body, a sort of diode is formed.

By analogy with solid-state semiconductors, where tiny changes in chemical composition drastically alter the electrical response, one must ask: could tiny changes in body chemistry radically alter the body's electrical fields? Could changes in the electrical fields impinging on the body cause subtle changes in body chemistry?

For a long time, Becker's primary interest was regeneration. There are some mind-blowing passages in the book describing what so-called lower animals can do (regrow hearts, cure induced cancer). Becker sees bioelectricity as a possible key to unlock the regenerative powers he believes still reside in our genes. The ideas in this book are powerful. The vistas it opened will keep medical researchers busy for decades.



Direct-current limb regeneration. *—The Body Electric*

Becker's *Cross-Currents* is newer and written at a less technical level. As the subtitle suggests, it explores the "perils of electropollution" and the "promise of electromedicine." Covering some of the same material as *The Body Electric* and *Currents of Death*, but in a friendlier tone, there are numerous comments on alternative medicine, holistic thinking, natural healing. His explanation of how acupuncture actually works is the best I've read. At the end, Becker gives some helpful low-cost suggestions on ways to minimize risk and exposure to EMFs.

The Body Electric
(Electromagnetism and the Foundation of Life)
Robert O. Becker, M.D., and Gary Selden, 1987; 448 pp.

$10.45 ($11.95 postpaid) from Wilmor Warehouse, 39 Plymouth Street, Fairfield, NJ 07006; 800/843-9389 (or Whole Earth Access)

Cross-Currents
(The Perils of Electropollution, the Promise of Electromedicine)
Robert O. Becker, M.D., 1990; 336 pp.

$19.95 postpaid from Jeremy P. Tarcher, Inc., 5858 Wilshire Boulevard, Los Angeles, CA 90036; 213/935-9980 (or Whole Earth Access) ■

The Real Honest True

BY

LORENZO W. MILAM

We are fighting over the basket and the fruits have fallen into the ditch . . .

—Vivekananda

I REMEMBER WHEN SATELLITES WERE EXOTIC. There were only a few of them, and we would go outside at dusk to watch them rising and setting like so many mini-moons. Now there are thousands of them. Thirty years ago, a political summit meeting could be destroyed because of a "spy plane," the U-2. Satellites have by their proliferation rendered moot the political fear of military eyes and ears.

McLuhan said that information is always liberating. At my favorite bar in Tijuana, The Reno, they watch soccer from Brazil, bullfights from Madrid, the local version of "60 Minutes" from Mexico City, and — from all over — the ever-more-anachronistic wars between Israelis, Arabs, Irish, Pakistanis, Indians, Chinese, Ethiopians, and Afghanis who have yet to hear the message of the thousand setting moons.

★ ★ ★

Those of us who have a lingering love of radio listen to the Canadian Broadcasting System audio services on the ANIK D satellite (transponders 16, 18, 20, 22 and 24). I prefer 24, because I can watch the Canadian Parliamentary Sessions on television with the audio turned to the subcarrier carrying classical programming. There too is the exquisite programming of the CBC French Service (on transponders 20 and 24). At nine PM, a lady who sounds like a Gallic *Passionara* comes on and plays the dances from *Terpsichore*, or the *Dichterliebe*. Or she will move through time and space to present the music of Java, or French pre-WWII cabaret music, or music of India — all the while speaking in a low throaty voice, as if she is telling us a very funny and very dirty joke.

In the old days, CBC's signal could only reach the northern tier of states. It is no accident that our strongest public radio comes out of Minnesota, Michigan, New York and Wisconsin. The CBC was helping to build the model, starting fifty years ago, and we didn't even have to pay for it. Thus one of the early lessons that communications belong to all of us, no matter for whom it is created.

Now, with satellite, the CBC is a gently falling, non-acidic rain of radio wit, drifting down onto the entire Western Hemisphere. Because of age and training and heritage and history, they always sound more sophisticated, wise, knowing and funny than the dull bulbs in our own Public Broadcast System. Anyone with a $995 satellite system — and amplifier and speakers — can hear one of the great radio services of the world.

★ ★ ★

Thirty-five years ago we went into community radio because there was no good broadcasting in the United States. Broadcasting in the United States was not regionalized and free but centralized and commercial. The audience paid a tax to be entertained; the taxes were, and are, called "advertising." Advertising increases the price of products like Excedrin, Froot Loops and most soap products by forty percent.

Some claim that radio died when they decided that the American spectrum could be sold like real estate. That's but part of it. The real problem was that there was no countervailing force to the power of commercial broadcasting until 1940. Typically, the change was technological rather than political: the FCC established "reserved" frequencies for FM and television.

Because of the growth of television, FM was moribund until the early sixties, so strange stations like KPFA, WBAI, KPFK and KRAB had time to prosper — or at least stabilize. They showed that radio could be good, and cheap, and demanding of the listener. They were committed to bias of programs but non-bias of the frequency. This is called Freedom of Speech. KRAB safely nested a member of the John Birch Society on alternative Friday night commentaries with the local leader of the Socialist Workers Party. "Cap" Weinberger, the recent Secretary of Defense, was one of the regular commentators on [the progressive FM network] Pacifica — as were several Marxists.

It wasn't until later that what we were doing came to be called "community" radio. Before that it wasn't community. The early KPFA and KPFK and WBAI and KRAB were stations

Lorenzo Milam's The Radio Papers *(1986) contains the most beautiful, passionate writing about radio published in the English language. It's in the form of short essays originally composed for the program guides of FM stations he had a hand in starting ($11.45 postpaid from Mho & Mho Works, Box 33135, San Diego, CA 92103).*

Despite the confession that follows, Lorenzo didn't kill Real Radio: his vision still inspires. —Robert Horvitz

Deregulation of Broadcasting

for the elite — those who wanted vigorous discussion, strong commentaries, shit-kicking interviews, and rich and controversial musical programming. Later these stations and their followers devolved into lecture halls for social and political minorities.

The final nail in the coffin of Real Radio was put into place by — of all people — me. Jeremy Lansman and I filed RM-2493 ["The Petition Against God"] with the Federal Communications Commission in 1974. We asked the Commission to stop issuing licenses for non-commercial FM stations until they determined whether religious propaganda was a bona fide use of the channels set aside for educational purposes. Because of the controversial, didactic nature of the document [written in the style of H. L. Mencken and G. B. Shaw, my heroes] it generated an enormous response. The FCC has received over 30,000,000 pieces of mail on the subject, and the letters and cards are still coming in at the rate of 1,000,000 a year.

It was soon apparent that the government was trapped into giving religious broadcasters something to assuage their fear. [In a participatory democracy, it is impolitic to stonewall paranoia too long.] The government turned over to the religious broadcasters what they considered to be the least valuable resource in the spectrum, the "non-commercial" portion of the FM band. The tragedy of this loss can be heard today in almost every community in America, where oleaginous voices tell us of their bleak god and how much money he needs for his perpetuation.

It is the brilliant theme of Greek drama that we create what we seek to avoid. Oedipus' father wanted to avoid the prophecy of his own death — so he made it happen. Oedipus wanted to know the truth, so he had to go blind in order to see it. I wanted to protect the frailest portion of the radio spectrum, and thus was able to help destroy it.

★ ★ ★

Jeremy Lansman brought community radio to the middle west in 1968, with the infamous [and still much lamented] KDNA in St. Louis. He went on to assist in the births of other stations and is now manager of KYES, TV channel 5 in Anchorage. According to Jeremy, FM and TV could and should be deregulated. He is here talking of true broadcast deregulation, not the ersatz deregulation proclaimed by the Reagan administration several years ago.

This True Deregulation is The Italian Solution. "It is an inverted order when compared to our own," he says. "It grew out of the fact that in the 1970s the Italian Supreme Court found regulation of local broadcasting by the national government to be unconstitutional."

Instead of chaos — which is what everyone thought would happen — there was a new order, far more simple and perfect and porous than the old system of government fiat. Anyone is permitted to buy and operate a broadcast transmitter. You go to your local equivalent of Radio Shack and buy an FM or television transmitter and you are on the air.

There are literally thousands of FM stations now, run by anyone who wants to transmit. Lansman said that it was in Rome he heard his first Hare Krishna station: it was the only one broadcasting chants 24 hours a day.

There are a few super stations, but their cost-effectiveness is very low. "Those who chose high power have to pay a high power bill," he says. A 100,000-watt station might cost $10,000 to $20,000 a month in electricity, whereas a five-watt station can be operated for less than $25.

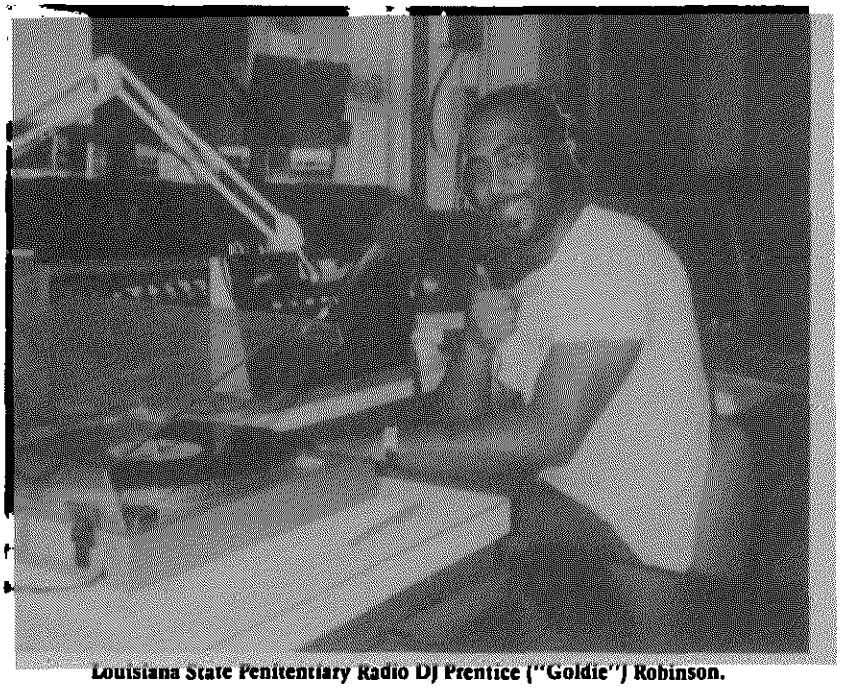
"It is a matter of physics and Adam Smith, and both might be higher powers than the FCC," he says. Italian stations can take risks and more easily tolerate competition because the owners haven't had to invest millions of lira just getting permission to go on the air.

"Since it always pays a broadcaster to go to the channel that is the least occupied, the power bill, the height of your antenna, your location, and your programming become your only limiting factors. It's the ultimate deregulation — restricted only by signal intensity, not the politics of oligopoly." ■

True Deregulation is The Italian Solution — anyone is permitted to buy and operate a broadcast transmitter. You go to your local equivalent of Radio Shack and buy an FM or television transmitter and you are on the air.

JAILHOUSE RADIO

BY DAVID ISAY



Louisiana State Penitentiary Radio DJ Prentice ("Goldie") Robinson.

"THIS IS KLSP, 91.7 FM, you're listening to the very best of radio programming with the Reverend A. J. This is the incarceration station . . . right here . . . Angola, Louisiana . . .

"This is goin' out to the guys in the cellblock area. And lookee here: hang tough, guys, it won't be long. I know how it is sometimes." *[BB King comes up under deejay's voice.]*

"Thrill is gone
The thrill has gone away . . . "

Out of the small studio in the one-story brick control center building of the Louisiana State Penitentiary at Angola, KLSP broadcasts from noon until midnight, seven days a week. It's a bare-bones operation. There's an ancient mixing board, a cheap reel-to-reel machine, two turntables, and a couple of shelves worth of albums. But to the 5,000 inmates who make up its listening audience, KLSP is more than just a radio station.

"Not too many things in Angola can bring these guys happiness." Inmate Andrew Joseph, also known as "the Reverend A.J.," has been one of KLSP's deejays for the past three years. He's serving a life sentence for murder:

"The radio station is really very important to them. They can write in for a request. They can ask for the kind of records they want, so they feel like that they are part of something."

[BB King ends.] A.J. on the air *[heavy reverb:]*

"This is K . . . L . . . S . . . P . . . with goldies . . .

"Yeah, what you all say. Now, you know what we gonna do right now? We gonna check on out of Hotel Loneliness and Hotel Happiness. Brook Benton, from days gone by. Let's roll!

[Record:] "I'm checkin' out . . . "

A. J.: "I'm gonna check out of this old prison one day, y'all: watch it."

[Record:] . . . of Hotel Loneliness. Left my broken heart . . .

A. J.: "Left mine. I'm gonna leave it behind in Angola when I go!"

[Record:] "Ya ya ya ya ya ya."

A. J.: "What y'all say about it over at the Mental Health Unit, my friends?"

KLSP went on the air four years ago, when local church groups donated second-hand radio equipment to the prison, and the FCC gave it a license to broadcast. The station's hundred-watt antenna sits directly behind Death Row, and has a range of about 30 miles. But because the prison is tucked away in remote Louisiana, its listening audience is confined to inmates, many of whom have radios in their cells and dormitories — inmates who literally pay for the station with their own blood. Each time a prisoner sells a pint of blood plasma to a pharmaceutical company for research, KLSP gets a small donation. It adds up to cover the station's entire $5000 a year budget.

"Here the primary listening music is blues." Program director Mitchell Mallette, "The Ragin' Cajun," is serving a mandatory 35-year sentence for armed robbery. He won't be leaving Angola until December 5, 2012.

Mallette: "We have a saying, if I can remember it, somebody told me one time, you can't really heal until you hurt. And the blues have a way of helping you get through those hard times, you know."

Ragin' Cajun on the air: "Going out to all the cellblocks. Also, Camp JCCR, and Death Row . . . "

The three inmates who run KLSP pride themselves on the station's diversity. There's a little something for everyone — from the "Prisoner Poetry" segments to the rabbi who comes on once a week for the single Jewish inmate at the penitentiary. There are legal advice shows, and two 15-minute news breaks a day.

Mallette, reading the news: "An inmate at the Louisiana Correctional Institute for Women in St. Gabriel died Friday on the way to Earl K.

It's only fitting that we have one piece in this section that arrived by radio. This is a transcript of David Isay's sound-portrait of KLSP, the only prison radio station licensed by the FCC, and probably the only station anywhere supported entirely by blood donations. Aired on National Public Radio's "All Things Considered" program, 26 May 1990. —*Robert Horvitz*

Longheart Memorial Hospital, a prison spokesman said. Shirley Johnson Shawlet, 53, was pronounced dead at . . . "

But the core of KLSP has been, and probably always will be, its music. Most of the station's albums have been donated by former prisoners. The collection is limited. It doesn't even include the music of those who spent time incarcerated here at Angola, like the blues great Leadbelly, country rocker Freddie Fender, and Charles Neville of the Neville Brothers. All of the records at KLSP are worn. Many skip from being requested through the prison mail several times a day.

KLSP's Reverend A.J.: "They like old-fashioned music. Even the old gospel. When they request gospel, they don't request the contemporary sounds. They get the oldest, the Mahalia Jackson type stuff, the Inez Andrews, way-back stuff, and this is what makes them identify. They can go back and say, well I remember when I used to go to church with mama. This is what they did in church, so right here at KLSP we bring them back to the times when they were free. And that's a great asset to being in an institution."

A. J. on the air: "Talkin about some precious memories. All of us have some of them, don't we? Let's go back, and see what they're talkin about." *[Scratchy gospel music fades up]*

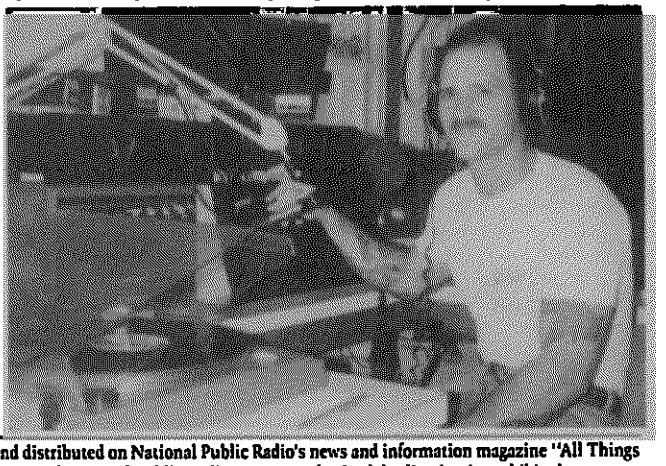
"Precious memories . . .
how they linger."

There's a decidedly glum sound to KLSP. Much of its music revolves around a handful of themes: loneliness, despair, memories, escape. The tone is appropriate. More than half of the 5,000 inmates at Angola are serving sentences of such length that they will probably die here. A similar fate awaits two of the station's three disk jockeys. But as they continually remind their audience, and themselves, there's always hope. Taped up on the station's wall, next to posters of Marvin Gaye and Smokey Robinson, is the gold seal of the former station manager: his pardon from the Governor, his ticket home.

So no matter how bleak the future may seem here, every day KLSP will keep broadcasting the sounds of freedom to its captive audience.

Ragin' Cajun on the air: "When the storms of life are raging, and things seem dark, even in the noonday hour, just remember that God is standing by. The Dynamic Soul-Stirrers . . . "

[Gospel music fades up.] ■



KLSP DJ Mitch ("Ragin' Cajun") Mallette

North American Free Radio Directory

FREE RADIO is made by people who believe in broadcasting without the hassle of licensing, following rules, etc.

They use mail drops, which are just mailboxes that intermediate between free-radio operators and people trying to contact them. They protect the identities and locations of the people behind the stations. If stations gave out their real addresses they'd be busted right away. Some mail drops have a dozen stations listed: they serve several different broadcasting stations.

I think this directory is good a) for allowing people to get in *real* contact, not just fantasize about what they *imagine* free or pirate stations should be, and b) to show the extent of the scene now in North America.

Do not expect a mail drop to pay for your reply: enclose adequate postage (three mint first-class stamps) for forwarding and reply.

These are the known mailing addresses of active and planned North American Free Radio stations, compiled by John T. Arthur in *The Ace* (p. 110), June 1990. Known medium-wave (AM) and FM frequencies are given. —*Robert Horvitz*

Free Radio One: 3434 N. Pacific Highway, Medford, OR 97501.

WTNU: 4431 Lehigh Road/Suite 196, College Park, MD 20740.

Radio Newyork International: Monticello, ME 04760.

United World Radio, Voice of Free Long Island: TAGAR, Room 256, Union Building, Stony Brook, NY 11794.

WJDI (1620 kHz.): P. O. Box 142, Cottekill, NY 12419.

Voice of Tomorrow (1616 kHz & shortwave): P. O. Box 314, Clakamas, OR 97015.

East Coast Pirate Radio, Secret Society Radio, Tube Radio, Voice of Bono, Voice of Greece, Voice of Revolutionary Plainville: P. O. Box 6527, Baltimore, MD 21219.

Hope Radio, Howdy Doody Radio, KRUD, Midnight Radio, One More Voice From America Radio, Radio Chesapeake Bay International, Radio Comedy Club International, Radio Flatulence, RFM, Radio Mexico, Society of Industrialized Music, Voice of the Epileptic Catfish, Voice of Monotony: P. O. Box 109, Blue Ridge Summit, PA 17214.

Black Box Radio, Pirate Radio New England (1616 kHz and shortwave), **Radio Angeline, Radio Espirito, Radio Lymph Node International, Radio Ohm, The Crooked Man, UA Express, WBNY, WBST** (666 kHz & shortwave), **WWW:** P. O. Box 40554, Washington, DC 20016.

Action Radio, KFAT, KMUD, KNBS, KQRP, KROK, KXVN (830 kHz & 92.7 MHz), **Plan 9*, Radio Contraband, Radio EXP, Radio Garbanzo, Radio Free Mumbo-Jumbo, Radio North Coast International, Radio USA, Secret Mountain Laboratory Ltd., Toynbee Radio*, Voice of Aphrodite*, Voice of Bob, Voice of Fubar, Voice of the Golden Eagle, Voice of Kentucky Fried Rodents, Voice of Lester, Voice of Laryngitis, Voice of the Rainbow, 75-WKUE, WQTU** (1620 kHz & shortwave), **WYMN, X-Ray Radio*, Zeppelin Radio Worldwide:** P. O. Box 452, Wellsville, NY 14895.

* Existence questionable. ■

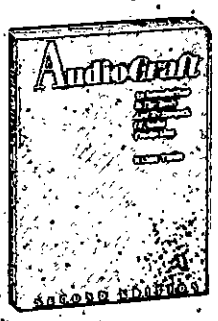
Making Radio

These days, it's getting easier and easier to get started in video . . . several hundred bucks and anyone can be a filmmaker or documentary producer. With that obvious attraction, I think people with stories to tell are picking up cameras and overlooking the audio arts. I think that's a mistake. Radio (and prerecorded cassettes) still provide a vivid, inexpensive, direct medium for fiction, fact, prose and poetry. Cameras are more obtrusive and more cumbersome than microphones, and the difference between special effects for video and radio is the difference between a gaggle of wizards from LucasFilm slaving at computers, or your doing something like playing the sound of your old lawnmower backwards. Also, no other medium matches radio's penetration. No one can watch a documentary while driving to work, biking, or taking a shower, but they can listen to one. In fact, there's an old cliche in radio that goes, "The only difference between radio and TV is that on radio the pictures are better." These two books can help bring your audio pictures into sharper focus.

AudioCraft is an entry-level primer on the nuts and bolts of audio production. The book starts out with the most basic basics, such as the difference between mono and stereo, and it eventually covers topics like reverb and producing live concerts. Author Randy Thom spent years in public radio (before going off and becoming one of those LucasFilm wizards, and picking up an Oscar for his sound work on The Right Stuff to boot), and he's gathered together straightforward explanations of what all those gadgets in the control room do. AudioCraft's widely used as a textbook at schools and community stations, and it's an excellent place to start.

Much of what's best about radio, particularly radio journalism, happens at National Public Radio. Several years back, some of NPR's top reporters, producers, editors and engineers collaborated on Telling the Story, a book and accompanying set of audio cassettes that explain how NPR does what it does. The book and cassettes can be purchased, and used, separately, but there's a synergistic effect to using them both. You can read, for example, about the principles of tape editing, then listen as NPR's top editor takes a rambling, disjointed interview and makes it coherent and interesting. Or hear the individual components of an "All Things Considered" feature, and then go into the studio and listen to it being put together. Telling the Story also covers areas of journalism that fall outside the realm of AudioCraft, issues like reporting styles, writing for the ear, and copyright and libel law.

—Chris Spurgeon



AudioCraft
Randy Thom, Editor
1989; 202 pp.

$30 ($35 postpaid) from NFCB, 666 11th Street NW/Suite 805, Washington, DC 20001; 202/393-2355

Telling the Story
Larry Josephson, Editor
1983; 228 pp.

$17.95 ($19.95 postpaid) from Kendall/Hunt Publishing Co., 2460 Kerper Boulevard/P. O. Box 539, Dubuque, IA 52004-0539; 319/588-1451

•

Many artists in a variety of fields, visual as well as aural, have said that music is the most powerfully emotive of all the arts. Remember that any sound placed in an appropriate context can be musical in the most basic sense, and inherit that magical power. *—AudioCraft*

•

I ask myself: can I bring all the people I interviewed for this story into this studio and read this script and play this tape right in front of them without shame, and when I finish, can I look them in the eye (all of them) and defend everything I have just said?

If I can, I go in and record.

—Telling the Story

•

Before leaving on an assignment, have a few interviews set up. Work the phone hard before you leave, and even harder after you get there. Ask everyone you interview who else you should talk to. If the story is controversial, ask them who their most worthy opponents are and then go do those interviews. Talk to officials and professionals and shop clerks and parking lot attendants. Know what you must cover and cover those subjects with a number of interviews. It is better to have too many than too few choices back at your editing station, better to be in a position to use only your very best interviews in the finished piece. But remember, if you just go out to fill in the blanks of a story you have already done in your mind, you won't have the story — *not the real story.*

—Telling the Story

Miking Techniques:
(Above) ***Try miking from this angle,*** **close to the mouth, with the microphone off-axis relative to the mouth.**
(Below) ***But not this angle*** **— this position is the most likely to accentuate plosive pops and other breath noises.**
—Telling the Story

•

Let's say that we have just taped an interview. There may be several reasons why you, as the producer of the piece, will want to eliminate or rearrange some of the words or ideas expressed in the interview.

► The people interviewed may have said something they now wish removed from the recording.

► There may be words which FCC regulations say you cannot broadcast.

► The ideas expressed in the interview may be more easily understood if their sequence is changed (rearranged in time).

► The length of the interview may exceed the length of time allocated to its broadcast.

► There may be an excessive number of pauses, stammers, mispronounced words, etc. (This is not to say that all "imperfections" in recorded dialogue should be removed, as often they are an important part of the interview.) *—AudioCraft*

BACKSCATTER

Echoes from readers back to *Whole Earth Review* (27 Gate Five Road, Sausalito, California 94965)
We pay $15 for every letter we publish.

Caution: guard burro

RE: ("Guard Donkeys" *WER* #67, p. 40) A few words of caution. Some friends of ours had a wild burro they adopted from the BLM. After years of a domesticated life we borrowed her to see if she could live with and guard our medium size flock of Polypay cross sheep on our farm in the Willamette Valley in Oregon.

BaBa our ram was with the flock of sheep. Rams are quite territorial among the ewes and take aggressive stances towards any interloper; including humans, dogs, cats and burros! Humans get out of the way, cats climb up or run away, dogs go for the kill and burros lash out with their front feet. After about two weeks of cautious coexistence, BaBa was cold cocked, staggered off and for weeks, despite a major indentation and infection in his forehead, recovered.

When using a burro, and I assume the same goes for a donkey, as a guard for sheep requires the proper management of the flock. When the ram is with the flock I would keep the burro out and vice versa. Many farmers keep their rams with the flock for about two months to breed, others keep the ram in longer to catch the yearling ewes who sometimes won't "take" until later in the season. Some with small flocks keep the ram in year round except prior to and during lambing to avoid any potential physical insults to the ewe which could cause death to the fetus or premature lambs.

When the burro is put in with the grazing ewes and lambs during and after lambing, when the ram is penned up, one still has to be careful. Many ram lambs start displaying aggressive characteristics after one month and could invite those lashing out front feet!

Tremaine Arkley
Independence, Oregon

Hemp, not trees

Enjoyed Antler's eight poems in issue #66, especially "Marijuana Saved My Life." Just as Antler's Mayflower ancestor was saved by a hemp rope, George Bush's life may have been saved by hemp too: parachutes in World War II were often made of hemp, and Bush used one when he bailed out of his fighter plane. However, I don't think our president will admit, at this time, to the importance of hemp as a commercial crop, a crop that deserves to be re-utilized.

I've been stunned since reading about marijuana's benefits over the past year. I'd known about its medicinal importance to glaucoma and chemotherapy patients, and the uses of its fibers: e.g., rope and clothing. But, I never knew marijuana is an excellent source of the following: methanol; food — its seed follows only soybeans in protein content; and paper — in fact, the cheapest form on the planet.

However, our costly "War on Drugs" continues to fight this beneficial plant, and its users. Perhaps readers heard about the DEA's "Operation Green Merchant": that sought to close stores stocking grow lights and equipment (a trend observed in *WER* #54). The DEA confiscated these outlets' mailing lists, and often followed-up on growers with warrantless searches.

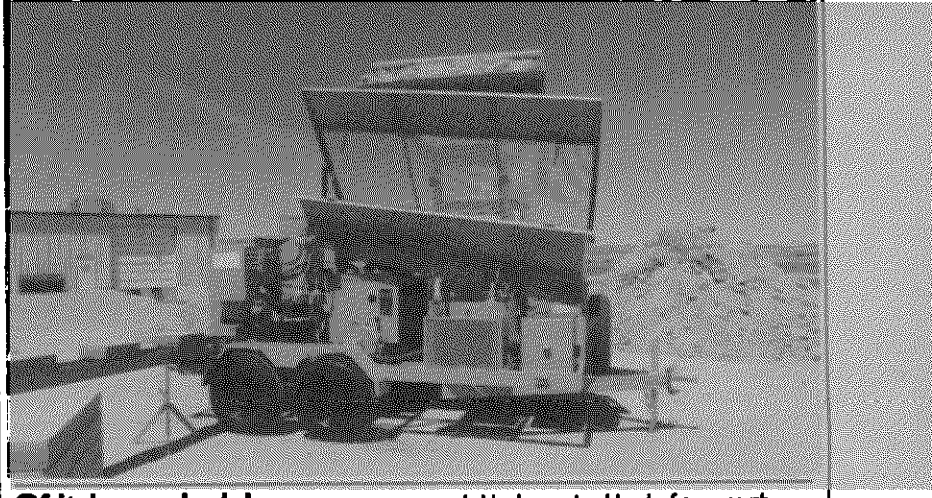
Despite these reactionary times — including calls for recriminalization — there are still signs of hope. Many prominent individuals are advocating legalization. A Kentucky man, Gatewood Galbraith, is running for governor of his state in '91 on a pro-hemp platform: re-introducing its commercial uses, and loosening the noose on his state's smokers. I urge readers to financially support the campaigns of politicians like Galbraith, the Oregon Marijuana Initiative, or the National Organization for the Reform of Marijuana Laws (NORML).

Hopefully, *Whole Earth Review* will one day be printed on hemp paper (rather than worrying about affording costly, re-cycled wood pulp), just as the first two drafts of our Declaration of Independence were printed on hemp.

Worried about the "War on Drugs" destroying personal liberties? Concerned about "Helping Nature Heal"? This is an excellent issue to focus on in the 1990s. Trees, one of our greatest resources, need not be destroyed when a simpler solution abounds.

Gregory Daurer
Denver, Colorado

P.S. An excerpt from Jack Herer's book *The Emperor Wears No Clothes* supplied many of the facts on marijuana cited in this letter. The book is scheduled to be re-issued this year, and I wholeheartedly recommend a review on it.



Of itches and adobe

What does *WER* do? The question would make a good koan.

Let's see. In a phrase, for this reader you provide . . . the scratch, the itch.

If I have an itch, you invariably scratch it. If I don't have one, if I'm floating along fat, dumb, and complaisant, you provide the swift kick that starts me thinking again. Our society is shedding its skin, and *WER* is one of the few magazines trying to understand what the new skin will/should/could look like.

As for your second question, my current resource love is this machine. On May 12-13, it made 7000 pressed-earth adobes (like those rolling along the conveyor) out of which I am building a house. The blocks are adobe sized (10x14x4) and are often called adobes, but they are really rammed earth blocks: a nice blend of two earth building technologies. Advantages: Easier (and cheaper) to transport machine than adobes. Can construct "adobe" buildings in areas far removed from New Mexico or Arizona. (Like Soviet Armenia, where one of these machines went after the quake.) Rammed earth blocks are 3x stronger than traditional sun baked adobes. Can (often, not always) use dirt on site; mine came from septic trenches and excavation. Blocks are very uniform, which means you can use a thin mortar joint. Then there are the standard earth building advantages: solar mass, fewer clearcuts, visually and acoustically nice dwellings . . . If you want more details, give me a call.

James R. Udall
0189 118 Rd.
Carbondale, CO 81623
303/963-2029

Corrections/Issue 68

Aerial Press (p. 16) has a new phone number: 408/462-0188.

The manufacturers of Pango Plunger (p. 62) have asked that customers add $3 postage & handling to the $24.95 list price.

To order The Hardwood Floor Refinisher's Handbook *(p. 67), write to Jim Schmitt, 4653 Columbus Avenue S., Minneapolis, MN 55407.*

UNCLASSIFIEDS

The UNCLASSIFIEDS are a reader-to-reader service available to *WER* subscribers only. They're designed to provide a cheap communications network for *WER* readers and mild financial assistance to the magazine.

UNCLASSIFIEDS are a great way to reach, survey, educate, link up with fellow *Whole Earth Review* readers. Send us your words, ideas, product descriptions, thoughts, messages . . .

TO ADVERTISE:

- **You must be a current subscriber.** Please send a current mailing label (or copy) from the cover of *WER* when you send in your ad copy. You may become a subscriber when you place your ad. *WER* subscription rates are $20/year ($24/year foreign and Canada). Please add this amount to your payment if you are not currently a subscriber. Order forms for subscriptions are at the back of the magazine.
- **Rates are $1 a word.** You count them and send us payment with copy. We will not bill. Payment must accompany the ad and be in U.S. funds drawn on a U.S. bank.
- **The first few words in your ad will be in capital letters.** We cannot do any other words in capitals.
- **To run a repeat ad:** Multiply your ad payment times the number of issues in which you want the ad to run. Send in that amount and we will print the same ad that many times. If you decide to repeat your ad after it has run, or if you wish to make a change in the copy, you must submit the ad again.
- **Deadline** is September 28 for the Winter '90 issue, January 7 for the Spring '91 issue, March 30 for the Summer '91 issue, and June 27 for the Fall '91 issue. Sorry, we will not take ads over the phone. Ads received after deadline will be held for the following issue.
- **We print ads in the order received.** "UNCLASSIFIEDS" means "no categories."
- **Mail ad and payment** (made out to *Whole Earth Review*) to: Susan Rosberg, WER UNCLASSIFIEDS, 27 Gate Five Road, Sausalito, CA 94965.

TAI HEI SHAKUHACHI are being used by teachers of traditional music in Japan & the USA and by professional musicians throughout the world. The unique precision-cast bore method is an innovation which enables me to make high-quality instruments for a very low price. 75-page catalog/sourcebook includes instruments, books, study guides and the most comprehensive listing of recorded bamboo flute music anywhere. $3 (Refundable with order). Monty H. Levenson, P. O. Box 294-A, Willits, CA 95490.

THE LAND NEWSLETTER — buying, selling and sharing land with respect. Special opportunities, upcoming events. $10/year. POB 849-w Glen Ellen CA 95442

LIVING FREE newsletter. Forum for debate among freedom-seekers, homesteaders, survivalists, libertarians, anarchists, outlaws. Lively, unique. $8.00 for 6 issues, sample $1.00. Box 29-WER, Hiler Branch, Buffalo, NY 14223.

WHATEVER YOU'RE LOOKING FOR I can find. Free brochure. Design Research, Dept W, POB 1503, Bangor, Maine, 04401

"THANKS FOR AN ENTERTAINING AND important work. . . . I felt I had lived with you." —Timothy Leary. *The Long Watch* $13.45 ppd. Call or write for free brochure. Spiraling Books, 12431 Camilla St., Whittier, CA 90601, (213) 692-2198.

BOOKS ON NONVIOLENCE, Anabaptism, Quakers, early Christianity, simple lifestyle, and communal living. Many of these books are discounted — up to 50% off in our free catalog. Seekers Catalog, Rt. 19, Box 890E, Tyler, TX 75706.

NEED EXTRA CASH? Self-employment guide describes over 200 companies that need your help! Call 24 hrs. for details. (417) 868-1331

GROUP MARRIAGE: Learn the latest. Send $7.95 for new book (plus $1.50 postage). Quarterly newsletter $9/yr. PEP, Box 5247-WE, Eugene, OR 97405.

THE WELL (Whole Earth 'Lectronic Link): If you have a computer and modem you can be part of a unique community of people that meets online. The Well is divided into conferences that discuss just about anything you can think of. Mind, work, sexuality, Grateful Dead, and parenting are just a few. The rates are $8/month plus $3/hour for online time. Call 415/332-6106 for online sign-up, or 415/332-4335 to talk with a human being.

NATURIST FAMILY VIDEOS/magazines, $2.00, S.A.S.E.; NATPLUS-WER, Box 9296, Newark, DE 19714-9296

FLY AGARIC MUSHROOMS. Amanita Muscaria. Wasson said it was Soma. Allegro said it was Jesus. 30 dried grams red var. muscaria grade A: $60.00. Grade B: $50.00. Red/orange var. flavivolvata grade B: $40.00. Other variations and grades available. J.L.F. P. O. Box 184-W, Elizabethtown, IN 47232 (812-379-2508).

GOLDEN THREADS. Contact publication for Lesbians over 50 (and younger). World-wide. Sample mailed discreetly, $5 (US $). OR send SASE for free information. Box 3177, Burlington, VT 05401-0031.

STINKY FEET? Simple home procedure eliminates and prevents reoccuring foot odor. No powders or charcoal pads. Guaranteed to work. For info pac send $5.00 cheque or M/O & SAE to Clear The Air, Box 1435 Stn. B, London Ontario Canada N6A 5M2

HOME BUSINESS POSSIBILITY — Picturesque retail building, comfortable house, and practical barn, all surrounded by forest service land, in a rural Oregon coast highway tourist area. We've sold/made toys here for 15 years. For brochure call (503) 753-3593.

DIDJERIDU — American crafted didjeridu. Play this powerful aboriginal wind-instrument yourself. Instructional cassette included. $85. Fred Tietjen 26 Allen St., San Francisco, CA. 94109 415-474-6979.

FOLKHEALING, SHAMANISM/HALLUCINogens, fascinating articles/books/ethnobotanical shirts/exotic teas. Send SASE or $1/info. Rosetta P. O. Box 4611 Dept. W Berkeley CA 94704-0611.

ADVERTISING WORKS when you reach the audience that needs your products or services. We specialize in placing ads for healthy, enlightening products in several progressive national magazines. They run the gamut from *Yoga Journal* to *Mother Jones* emphasizing environmental issues, spiritual practices, and holistic health education. Our services are free, but alas, not the ads. GPR, 2054 University Ave. Ste. 302-R, Berkeley, CA 94704. (415) 548-1680.

WORLDWIDE ENGLISH NEWSPAPERS and Magazine-of-Month Club. 65 countries! Sampler 3/$2.98. Free brochure. Multinewspapers, Box DE-WS, Dana Point, California 92629.

GNOSIS MAGAZINE #17 (The Journal of Western Inner Traditions' Fall '90 issue) due out in October. Theme: Sex & Spirituality. Issues #1-16 available. Edited by Jay Kinney. Back issues: $5 each. Subscriptions: $15/4 issues ($20 for Canadian & foreign subs). Checks drawn on U.S. banks or Int. M.O.s to: Dept. W, The Lumen Foundation, P. O. Box 14217, San Francisco, CA 94114.

FREE NEWSLETTER. Grow delicious backyard wild mushrooms. Inexpensive cultures/spores/supplies. SASE. Kingdom, POBX 611, Centrehall, PA 16828.

NEW LEAF CATALOG OF BOOKS for growth and change. One of the most comprehensive catalogs of New Age related books available! Over 14,000 titles in more than 600 categories including: A.I.D.S., Aging, Animal Rights, Astrology, Creativity, Crystals, Dreams, The Environment, Gardening & Farming, Parenting & Family, Reincarnation & Karma, Self-Help, Sexuality, Spiritual Development, UFOs, Yoga & Young Readers etc. Send $10 (refundable with 1st order) for your copy of this giant catalog. We've got the books you want to read! Oak Tree Enterprises, 2040 Polk Street, Suite 259, San Francisco, CA. 94109

DATABASE OF HEALING SYSTEMS, ("From Africa to Zen") helping to connect person with path. Looking for colleagues. Write: Personal Information Stream Management, P. O. Box 7182-WER, Berkeley, CA 94707

JOIN THE MUSIC SOCIETY. Bringing intelligent music to intelligent people. Details: 15 Goldberry Square Room 11, Scarborough ON, M1C-3H6, Canada

---

REDUCE YOUR RISK from radiation emissions from computors. "Bodyshield" apron shields the wearer and reduces the electromagnetic waves that penetrate the body. Free brochure or send $35.00 ppd. to Safe Shields 139 8th St. Pacific Grove, CA. 93950.

FOR LIVING . . . BUY into a small, 8 acre, land trust community in N.E. Pa, Endless Mtns. from our home lets make a difference, ecologically, politically socially, creatively, spiritually. Business potential, guest program & non profit center, now latent, waiting for you. Info: Jann Rucquoi 108 Breeze Ave, #C, Venice, Ca. 90291 for Rabbity Hill Farm.

Pirate Radio • Stopping Junk Mail • Eco-cars

The FBI vs. Teenage Outlaws on the Electronic Frontier

$6 ($6.[illegible] Canadian) No. 68 Fall 1990

WHOLE EARTH REVIEW

ACCESS TO TO[illegible]

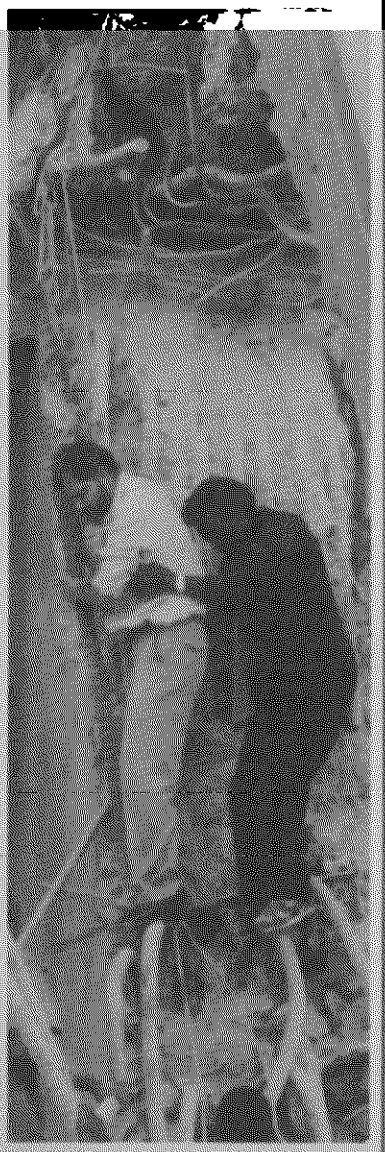
EARTHQUAKE LESSONS

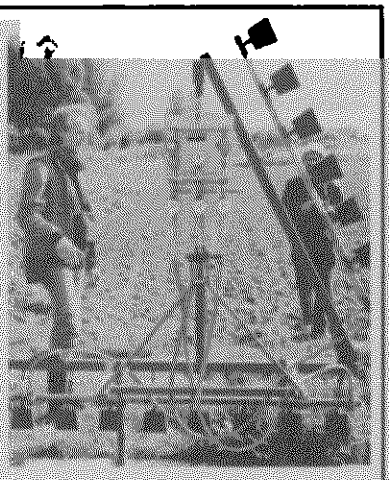
The Crucial Difference of Volunteers

Page 2

WHOLE EARTH REVIEW

Number 68 FEATURES Fall 1990



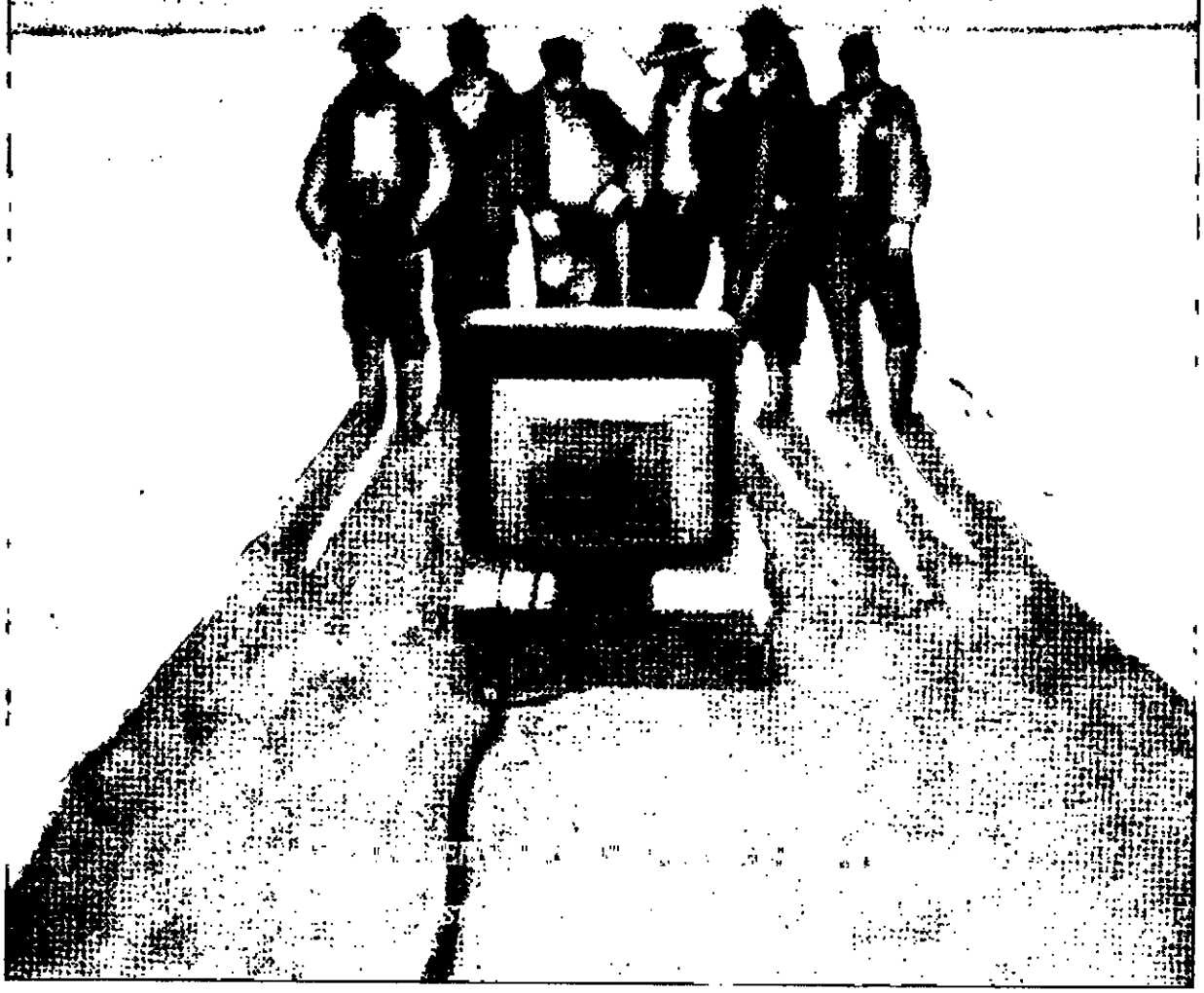


Whole Earth Review ☐ Issue No. 68 ☐ September 5, 1990 (ISSN 0749-5056) (USPS 077-150). Published quarterly by POINT, a California nonprofit corporation. Editorial office: 27 Gate Five Road, Sausalito, CA 94965; (415)332-1716. Subscriptions $20 per year; single copies $5. Inquire for first class and international air rates. Second-class postage paid at Sausalito, California, and at additional mailing offices. Claims for missing issues will not be honored later than six months after publication. Back issues are available on microfilm and as xerographic reprints from University Microfilms International, Serials Bid Coordinator, 300 Zeeb Road, Ann Arbor, MI 48106. Whole Earth Review is indexed by Access: The Supplementary Index to Periodicals, Alternative Press Index, Magazine Index, Consumers Index, Humanities Index, and Book Review Index.

POSTMASTER: Send address changes to Whole Earth Review, P. O. Box 38, Sausalito, CA 94966.

Crime And Puzzlement

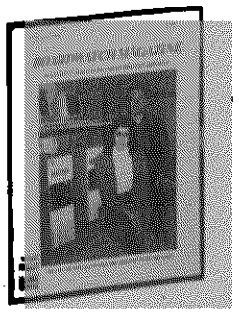
In advance of the law on the Electronic Frontier



Boardwatch Magazine

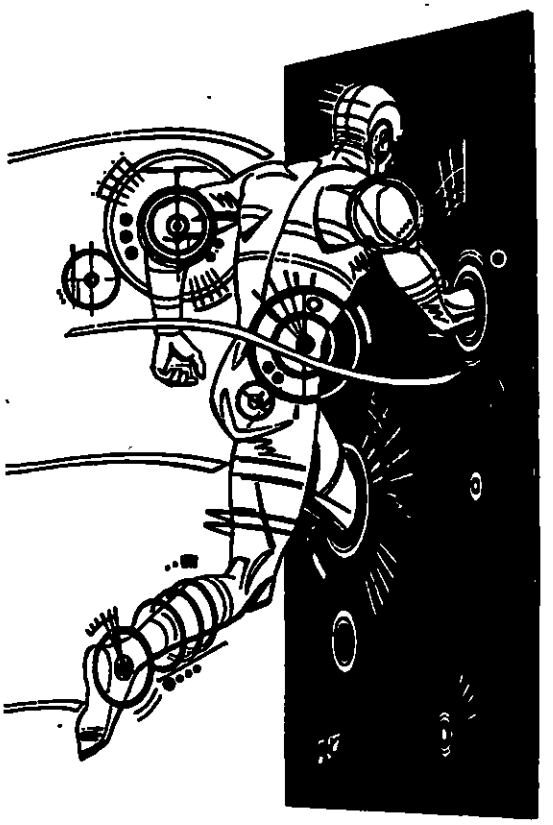
A down-home magazine that covers the down-home side of the online information world of electronic community BBSs and computer teleconferences. Contains news about relevant issues and products and lots of capsule reviews of all these small online outfits, usually run out of homes, that have proliferated all over the country. Boardwatch is valuable because you'd probably never find out about all of these systems from the slick computer/telecomm mags, and it shows you that this is a real movement of grassroots communication that can make a difference in getting people together.

—John Coate



Boardwatch Magazine
Jack Rickard, Editor

$28/year
(12 issues) from Boardwatch, 5970 S. Vivian Street, Littleton, CO 80127; 303/973-6038



•

First BBS in USSR — Tallinn Estonia

. . . With the help of some Finnish friends in Helsinki, a small PCBoard system went into operation in Tallinn (pronounced TAH-LEEN), the capitol of the Republic of Estonia in the USSR. . . .

The board is titled *Eesti BBS #1*. Although somewhat of a group effort, the sysop, or at least the one operating the system and moderating the message areas seems to be one Lembit Pirn of Tallinn. The principal raison d'etre for the system is to support a type of Estonian Association of Small Businesses. It appears they hope to offer some form of trade opportunities to local businesses.

•

We've seen enough announcements for FAX/MODEM/VOICE switches to paper the office here. They all promise to allow you to handle voice, data, and fax calls on a single telephone line — saving the expense of individual dedicated lines. This is a great idea — except in the real world, it just doesn't work.

The trouble is that nearly all of these switches are kludgy and most work under the assumption that the caller at the other end has at least some graduate work in Electronic Engineering.

•

Most electronic mail networks these days can send your message to any telex machine on the globe. All of them operate on a store-and-forward basis under which you upload or key in your message, key in the telex address, and sign off. The system then handles any protocol conversions to get the message into the proper shape for its destination network and begins dialing the target machine. . . .

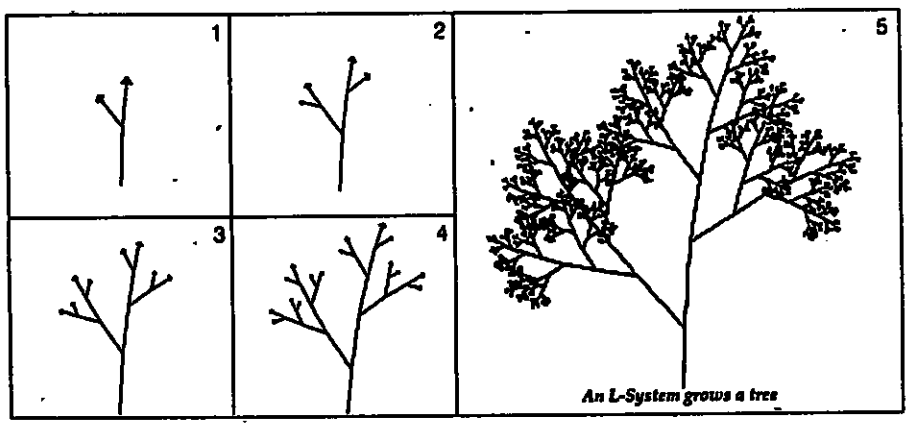
It is important to point out that the telex/e-mail network operates in both directions. Not only can you send to any machine on the net, you can receive messages from any machine as well. These appear in your electronic mail as normal e-mail messages.

Algorithm

Commercial computer software has gotten so slick and sophisticated that doing your own programming has come to sound as foolish as doing your own surgery. This newsletter by A. K. Dewdney, host of Scientific American's former column on computer recreations, is a refuge for old-time "personal programming," a forum for digital do-it-yourselfers creating their own versions of things. I like Dewdney's newsletter because even though I have hypocritically refused to learn programming, the territories he covers — "new cellular automata, cunning fractals, evolving systems, numerical magic, amazing patterns, experiments both real and imaginary" — are ones that I'm trekking in, places unknown and weird enough that they are ideal for amateurs. I feel welcomed by this publication.

—Kevin Kelly

[Suggested by Michael Strasmich]



An L-System grows a tree

Algorithm
A. K. Dewdney, Editor

$30/year
(6 issues); sample $5 from Algorithm, P. O. Box 29237, Westmount Postal Outlet, 785 Wonderland Road, London, Ontario, Canada N6K 1M6

Desperados of the DataSphere

So me and my sidekick Howard, we was sitting out in front of the 40 Rod Saloon one evening when he all of a sudden says, "Lookee here. What do you reckon?" I look up and there's these two strangers riding into town. They're young and got kind of a restless, bored way about 'em. A person don't need both eyes to see they mean trouble . . . Well, that wasn't quite how it went. Actually, Howard and I were floating blind as cave fish in the electronic barrens of the WELL, so the whole incident passed as words on a display screen:

Howard: Interesting couple of newusers just signed on. One calls himself acid and the other's optik.

Barlow: Hmmm. What are their real names?

Howard: Check their finger files.

And so I typed !finger acid. Several seconds later the WELL's Sequent computer sent the following message to my Macintosh in Wyoming:

Login name: acid *In real life:* Acid Phreak

By this, I knew that the WELL had a new resident and that his corporeal analog was supposedly called Acid Phreak. Typing !finger optik yielded results of similar insufficiency, including the claim that someone, somewhere in the real world, was walking around calling himself Phiber Optik. I doubted it.

However, associating these sparse data with the knowledge that the WELL was about to host a conference on computers and security rendered the conclusion that I had made my first sighting of genuine computer crackers. As the arrival of an outlaw was a major event to the settlements of the Old West, so was the appearance of crackers cause for stir on the WELL.

The WELL (Whole Earth 'Lectronic Link) is an example of the latest thing in frontier villages, the computer bulletin board. In this kind of small town, Main Street is a central minicomputer to which (in the case of the WELL) as many as 64 microcomputers may be connected at one time by phone lines and little blinking boxes called modems.

In this silent world, all conversation is typed. To enter it, one forsakes both body and place and becomes a thing of words alone. You can see what your neighbors are saying (or recently said), but not what either they or their physical surroundings look like. Town meetings are continuous and discussions rage on everything from sexual kinks to depreciation schedules.

There are thousands of these nodes in the United States, ranging from PC-clone hamlets of a few users to mainframe metros like CompuServe, with its 550,000 subscribers. They are used by corporations to transmit memoranda and spreadsheets, universities to disseminate research, and a multitude of factions, from apiarists to Zoroastrians, for purposes unique to each.

Whether by one telephonic tendril or millions, they are all connected to one another. Collectively, they form what their inhabitants call the Net. It extends across that immense region of electron states, microwaves, magnetic fields, light pulses and thought which sci-fi writer William Gibson named Cyberspace.

Cyberspace, in its present condition, has a lot in common with the 19th Century West. It is vast, unmapped, culturally and legally ambiguous, verbally terse (unless you happen to be a court stenographer), hard to get around in, and up for grabs. Large institutions already claim to own the place, but most of the actual natives are solitary and independent, sometimes to the point of sociopathy. It is, of course, a perfect breeding ground for both outlaws and new ideas about liberty. ►

Some teenagers, being kids, get into mischief. Maybe even break the law. Nothing new there. What's new here is that some teenagers are caught red-handed but nobody can define what it is that they were doing wrong. They are out beyond the law. Wyoming resident John Barlow, a teenager at heart, is a retired cattle rancher, a lyricist for the Grateful Dead, a former Republican candidate for Wyoming State Senate, and an online correspondent on the WELL. He describes himself as a "hippie mystic and professional techno-crank" and is working on a book for Viking called Everything We Know Is Wrong.

—Kevin Kelly

Recognizing this, *Harper's Magazine* decided in December 1989 to hold one of its periodic Forums on the complex of issues surrounding computers, information, privacy, and electronic intrusion or "cracking." Appropriately, they convened their conference in Cyberspace, using the WELL as the "site."

Harper's invited an odd lot of about 40 participants. These included: Clifford Stoll, whose book *The Cuckoo's Egg* (see *WER #67*, p. 31) details his cunning efforts to nab a German cracker. John Draper or "Cap'n Crunch," the granddaddy of crackers whose blue boxes got Apple founders Wozniak and Jobs into consumer electronics. Stewart Brand and Kevin Kelly of Whole Earth fame. Steven Levy, who wrote the seminal *Hackers*. A retired Air Force colonel named Dave Hughes. Lee Felsenstein, who designed the Osborne computer and was once called the "Robespierre of computing." A UNIX wizard and former hacker named Jeff Poskanzer. There was also a score of aging techno-hippies, the crackers, and me.

What I was doing there was not precisely clear since I've spent most of my working years either pushing cows or song-mongering, but I at least brought to the situation a vivid knowledge of actual cow-towns, having lived in or around one most of my life.

That and a kind of innocence about both the technology and morality of Cyberspace which was soon to pass into the confusion of knowledge.

At first, I was inclined toward sympathy with Acid 'n' Optik as well as their colleagues, Adelaide, Knight Lightning, Taran King, and Emmanuel. I've always been more comfortable with outlaws than Republicans, despite having more certain credentials in the latter camp.

But as the *Harper's* Forum mushroomed into a boomtown of ASCII text (the participants typing 110,000 words in 10 days), I began to wonder. These kids were fractious, vulgar, immature, amoral, insulting, and too damned good at their work.

Worse, they inducted a number of former kids like myself into Middle Age. The long-feared day had finally come when some gunsel would yank my beard and call me, too accurately, an old fart.

Under ideal circumstances, the blind gropings of bulletin-board discourse force a kind of Noh drama stylization on human commerce. Intemperate responses, or "flames" as they are called, are common even among conference participants who understand one another, which, it became immediately clear, the cyberpunks and techno-hippies did not.

My own initial enthusiasm for the crackers wilted under a steady barrage of typed testosterone. I quickly remembered I didn't know much about who they were, what they did, or how they did it. I also remembered stories about crackers working in league with the Mob, ripping off credit-card numbers and getting paid for them in (stolen) computer equipment.

And I remembered Kevin Mitnik. Mitnik, now 25, who recently served federal time for a variety of computer- and telephone-related crimes. Prior to incarceration, Mitnik was, by all accounts, a dangerous guy with a computer. He disrupted phone company operations and arbitrarily disconnected the phones of celebrities. Like the kid in *War Games*, he broke into the North American Defense Command computer in Colorado Springs.

Unlike the kid in *War Games*, he reputedly made a practice of destroying and altering data, including the credit information of his probation officer and other enemies. Digital Equipment claimed that his depredations cost them more than $4 million in computer downtime and file rebuilding. Eventually, he was turned in by a friend who, after careful observation, had decided he was "a menace to society."

His spectre began to hang over the conference. After several days of strained diplomacy, the discussion settled into a moral debate on the ethics of security and went critical.

The techno-hippies were of the unanimous opinion that, in Dylan's words, one "must be honest to live outside the law." But these young strangers apparently lived by no code save those with which they unlocked forbidden regions of the Net.

They appeared to think that improperly secured systems deserved to be violated and, by extension, that unlocked houses ought to be robbed. This latter built particular heat in me since I refuse, on philosophical grounds, to lock my house.

Civility broke down. We began to see exchanges like:

Dave Hughes: Clifford Stoll said a wise thing that no one has commented on. That networks are built on trust. If they aren't, they should be.

Acid Phreak: Yeah. Sure. And we should use the "honor system" as a first line of security against hack attempts.

Jef Poskanzer: This guy down the street from me sometimes leaves his back door unlocked. I told him about it once, but he still does it. If I had the chance to do it over, I would go in the back door, shoot him, and take all his money and consumer electronics. It's the only way to get through to him.

Acid Phreak: Jef Poskanker (Puss? Canker? yechh) Anyway, now when did you first start having these delusions where computer hacking was even *remotely* similar to murder?

Presented with such a terrifying amalgam of raw youth and apparent power, we fluttered like a flock of indignant Babbitts around the Status Quo, defending it heartily. One former hacker howled to the *Harper's* editor in charge of the forum. "Do you or do you not have names and addresses for these criminals?" Though they had committed no obvious crimes, he was ready to call the police.

They finally got to me with:

Acid: Whoever said they'd leave the door open to their house . . . where do you live? (the address) Leave it to me in mail if you like.

I had never encountered anyone so apparently unworthy

of my trust as these little nihilists. They had me questioning a basic tenet, namely that the greatest security lies in vulnerability. I decided it was time to put that principle to the test . . .

Barlow: Acid. My house is at 372 North Franklin Street in Pinedale, Wyoming. If you're heading north on Franklin, you go about two blocks off the main drag before you run into hay meadow on the left. I've got the last house before the field. The computer is always on . . . And is that really what you mean? Are you merely just the kind of little sneak that goes around looking for easy places to violate? You disappoint me, pal. For all your James Dean-On-Silicon rhetoric, you're not a cyberpunk. You're just a punk.

Acid Phreak: Mr. Barlow: Thank you for posting all I need to get your credit information and a whole lot more! Now, who is to blame? ME for getting it or YOU for being such an Idiot?! I think this should just about sum things up.

Barlow: Acid, if you've got a lesson to teach me, I hope it's not that it's idiotic to trust one's fellow man. Life on those terms would be endless and brutal. I'd try to tell you something about conscience, but I'd sound like Father O'Flannigan trying to reform the punk that's about to gutshoot him. For no more reason than to watch him die.

But actually, if you take it upon yourself to destroy my credit, you might do me a favor. I've been looking for something to put the brakes on my burgeoning materialism.

I spent a day wondering whether I was dealing with another Kevin Mitnik before the other shoe dropped:

Barlow: . . . With crackers like acid and optik, the issue is less intelligence than alienation. Trade their modems for skateboards and only a slight conceptual shift would occur.

Optik: You have some pair of balls comparing my talent with that of a skateboarder. Hmmm . . . This was indeed boring, but nonetheless:

At which point he downloaded my credit history.

Optik had hacked the core of TRW, an institution which has made my business (and yours) their business, extracting from it an abbreviated (and incorrect) version of my personal financial life. With this came the implication that he and Acid could and would revise it to my disadvantage if I didn't back off.

I have since learned that while getting someone's TRW file is fairly trivial, changing it is not. But at that time, my assessment of the crackers' black skills was one of superstitious awe. They were digital brujos about to zombify my economic soul.

To a middle-class American, one's credit rating has become nearly identical to his freedom. It now appeared that I was dealing with someone who had both the means and desire to hoodoo mine, leaving me trapped in a life of wrinkled bills and money-order queues. Never again would I call the Sharper Image on a whim.

I've been in redneck bars wearing shoulder-length curls, police custody while on acid, and Harlem after midnight, but no one has ever put the spook in me quite as Phiber Optik did at that moment. I realized that we had problems which exceeded the human conductivity of the WELL's bandwidth. If someone were about to paralyze me with a spell, I wanted a more visceral sense of him than could fit through a modem.

I e-mailed him asking him to give me a phone call. I told him I wouldn't insult his skills by giving him my phone number and, with the assurance conveyed by that challenge, I settled back and waited for the phone to ring. Which, directly, it did.

They were digital brujos out to zombify my economic soul.

In this conversation and the others that followed I encountered an intelligent, civilized, and surprisingly principled kid of 18 who sounded, and continues to sound, as though there's little harm in him to man or data. His cracking impulses seemed purely exploratory, and I've begun to wonder if we wouldn't also regard spelunkers as desperate criminals if AT&T owned all the caves.

The terrifying poses which Optik and Acid had been striking on screen were a media-amplified example of a human adaptation I'd seen before: One becomes as he is beheld. They were simply living up to what they thought we, and, more particularly, the editors of *Harper's*, expected of them. Like the televised tears of disaster victims, their snarls adapted easily to mass distribution.

Months later, *Harper's* took Optik, Acid and me to dinner at a Manhattan restaurant which, though very fancy,

was appropriately Chinese. Acid and Optik, as material beings, were well-scrubbed and fashionably clad. They looked to be dangerous as ducks. But, as *Harper's* and the rest of the media have discovered to their delight, the boys had developed distinctly showier personae for their rambles through the howling wilderness of Cyberspace. Glittering with spikes of binary chrome, they strode past the klieg lights and into the digital distance. There they would be outlaws. It was only a matter of time before they started to believe themselves as bad as they sounded. And no time at all before everyone else did.

In this, they were like another kid named Billy, many of whose feral deeds in the pre-civilized West were encouraged by the same dime novelist who chronicled them. And like Tom Horn, they seemed to have some doubt as to which side of the law they were on. Acid even expressed an ambition to work for the government someday, nabbing "terrorists and code abusers."

There is also a frontier ambiguity to the "crimes" the crackers commit. They are not exactly stealing VCRs. Copying a text file from TRW doesn't deprive its owner of anything except informational exclusivity. (Though it may be said that information has monetary value only in proportion to its containment.)

There was no question that they were making unauthorized use of data channels. The night I met them, they left our restaurant table and disappeared into the phone booth for a long time. I didn't see them marshalling quarters before they went.

And, as I became less their adversary and more their scoutmaster, I began to get "conference calls" in which six or eight of them would crack pay phones all over New York and simultaneously land on my line in Wyoming. These deft maneuvers made me think of sky-diving stunts where large groups convene geometrically in free fall. In this case, the risk was largely legal.

Their other favorite risky business is the time-honored adolescent sport of trespassing. They insist on going where they don't belong. But then teen-age boys have been proceeding uninvited since the dawn of human puberty. It seems hard-wired. The only innovation is in the new form of the forbidden zone and the means of getting in it.

In fact, like Kevin Mitnik, I broke into NORAD when I was 17. A friend and I left a nearby "woodsie" (as rustic adolescent drunks were called in Colorado) and tried to get inside the Cheyenne Mountain. The chrome-helmeted Air Force MPs held us for about two hours before letting us go. They weren't much older than us and knew exactly our level of national security threat. Had we come cloaked in electronic mystery, their alert status certainly would have been higher.

Whence arises much of the anxiety. Everything is so ill-defined. How can you guess what lies in their hearts when you can't see their eyes? How can one be sure that, unlike Mitnik, they won't cross the line from trespassing into another adolescent pastime, vandalism? And how can you be sure they pose no threat when you don't know what a threat might be?

And for the crackers some thrill is derived from the metamorphic vagueness of the laws themselves. On the Net, their effects are unpredictable. One never knows when they'll bite.

This is because most of the statutes invoked against the crackers were designed in a very different world from the one they explore. For example, can unauthorized electronic access be regarded as the ethical equivalent of old-fashioned trespass? Like open range, the property boundaries of Cyberspace are hard to stake and harder still to defend.

Is transmission through an otherwise unused data channel really theft? Is the trackless passage of a mind through TRW's mainframe the same as the passage of a pickup through my Back 40? What is a place if Cyberspace is everywhere? What are data and what is free speech? How does one treat property which has no physical form and can be infinitely reproduced? Is a computer the same as a printing press? Can the history of my business affairs properly belong to someone else? Can anyone morally claim to own knowledge itself?

If such questions are hard to answer precisely, there are those who are ready to try. Based on their experience in the Virtual World, they were about as qualified to enforce its mores as I am to write the Law of the Sea. But if they lacked technical sophistication, they brought to this task their usual conviction. And, of course, badges and guns.

Operation Sun Devil

Recently, we have witnessed an alarming number of young people who, for a variety of sociological and psychological reasons, have become attached to their

computers and are exploiting their potential in a criminal manner. Often, a progression of criminal activity occurs which involves telecommunications fraud (free long-distance phone calls), unauthorized access to other computers (whether for profit, fascination, ego, or the intellectual challenge), credit card fraud (cash advances and unauthorized purchases of goods), and then moves on to other destructive activities like computer viruses. . . .

Our experience shows that many computer hacker suspects are no longer misguided teenagers mischievously playing games with their computers in their bedrooms. Some are now high-tech computer operators using computers to engage in unlawful conduct.

—Excerpts from a statement by Garry M. Jenkins, Asst. Director, U. S. Secret Service

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

—Amendment IV, United States Constitution

On January 24, 1990, a platoon of Secret Service agents entered the apartment which Acid Phreak shares with his mother and 12-year-old sister. The latter was the only person home when they burst through the door with guns drawn. They managed to hold her at bay for about half an hour until their quarry happened home.

By then, they were nearly done packing up Acid's worldly goods, including his computer, his notes (both paper and magnetic), books, and such dubiously dangerous tools as a telephone answering machine, a ghetto blaster and his complete collection of audio tapes. One agent asked him to define the real purpose of the answering machine and was frankly skeptical when told that it answered the phone. The audio tapes seemed to contain nothing but music, but who knew what dark data Acid might have encoded between the notes . . .

When Acid's mother returned from work, she found her apartment a scene of apprehended criminality. She asked what, exactly, her son had done to deserve all this attention and was told that, among other things, he had caused the AT&T system crash several days earlier. (Previously AT&T had taken full responsibility.) Thus, the agent explained, her darling boy was thought to have caused over a billion dollars in damage to the economy of the United States.

This accusation was never turned into a formal charge. Indeed, no charge of any sort of was filed against Mr. Phreak then and, although the Secret Service maintained resolute possession of his hardware, software, and data, no charge had been charged four months later.

Across town, similar scenes were being played out at the homes of Phiber Optik and another colleague code-named Scorpion. Again, equipment, notes, disks both hard and soft, and personal effects were confiscated. Again no charges were filed.

Thus began the visible phase of Operation Sun Devil, a two-year Secret Service investigation which involved 150 federal agents, numerous local and state law enforcement agencies and the combined security resources of PacBell, AT&T, Bellcore, Bell South MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West and American Express.

The focus of this impressive institutional array was the Legion of Doom, a group which never had any formal membership list but was thought by the members with whom I spoke to number less than 20, nearly all of them in their teens or early twenties.

I asked Acid why they'd chosen such a threatening name. "You wouldn't want a fairy kind of thing like Legion of Flower Pickers or something. But the media ate it up too. Probing the Legion of Doom like it was a gang or something, when really it was just a bunch of geeks behind terminals."

Sometime in December 1988, a 21-year-old Atlanta-area Legion of Doomster named The Prophet cracked a Bell South computer and downloaded a three-page text file which outlined, in bureaucratese of surpassing opacity, the administrative procedures and responsibilities for marketing, servicing, upgrading, and billing for Bell South's 911 system.

A dense thicket of acronyms, the document was filled with passages like:

In accordance with the basic SSC/MAC strategy for provisioning, the SSC/MAC will be Overall Control Office (OCO) for all Notes to PSAP circuits (official services) and any other services for this customer. Training must be scheduled for all SSC/MAC involved personnel during the pre-service stage of the project.

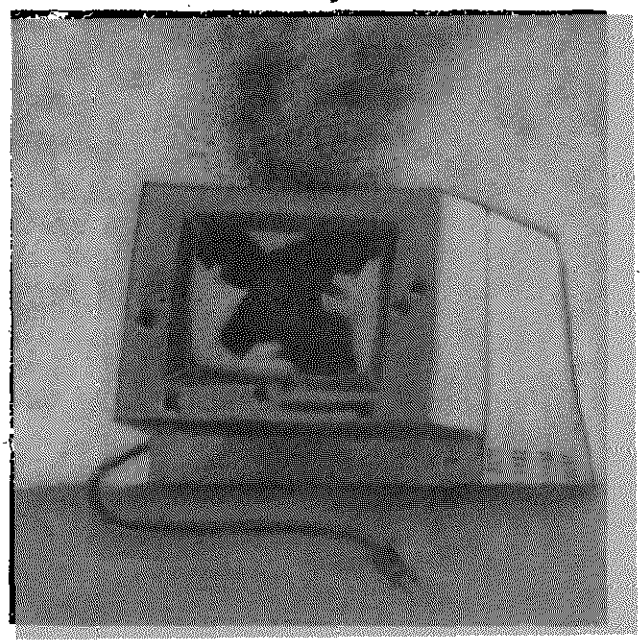
And other such.

At some risk, I too have a copy of this document. To read the whole thing straight through without entering coma requires either a machine or a human who has too much practice thinking like one. Anyone who can understand it fully and fluidly has altered his consciousness beyond the ability to ever again read Blake, Whitman, or Tolstoy. It is, quite simply, the worst writing I have ever tried to read.

Since the document contains little of interest to anyone who is not a student of advanced organizational sclerosis — that is, no access codes, trade secrets, or proprietary information — I assume The Prophet only copied this file as a kind of hunting trophy. He had been to the heart of the forest and had returned with this coonskin to nail to the barn door.

Furthermore, he was proud of his accomplishment, and since such trophies are infinitely replicable, he wasn't content to nail it to his door alone. Among the places he copied it was a UNIX bulletin board (rather like the WELL) in Lockport, Illinois, called Jolnet.

Like the many others whose equipment and data were taken by the Secret Service subsequently, he wasn't charged with anything. Nor is he likely to be. They have already inflicted on him the worst punishment a nerd can suffer: data death.



It was downloaded from there by a 20-year-old hacker and pre-law student (whom I had met in the *Harper's* Forum) who called himself Knight Lightning. Though not a member of the Legion of Doom, Knight Lightning and a friend, Taran King, also published from St. Louis and his fraternity house at the University of Missouri a worldwide hacker's magazine called *Phrack*. (From phone phreak and hack.)

Phrack was an unusual publication in that it was entirely virtual. The only time its articles hit paper was when one of its subscribers decided to print out a hard copy. Otherwise, its editions existed in Cyberspace and took no physical form.

When Knight Lightning got hold of the Bell South document, he thought it would amuse his readers and reproduced it in the next issue of *Phrack*. He had little reason to think that he was doing something illegal. There is nothing in it to indicate that it contains proprietary or even sensitive information. Indeed, it closely resembles telco reference documents which have long been publicly available.

However, Rich Andrews, the systems operator who oversaw the operation of Jolnet, thought there might be something funny about the document when he first ran across it in his system. To be on the safe side, he forwarded a copy of it to AT&T officials. He was subsequently contacted by the authorities, and he cooperated with them fully. He would regret that later.

On the basis of the foregoing, a grand jury in Lockport was persuaded by the Secret Service in early February to hand down a seven-count indictment against The Prophet and Knight Lightning, charging them, among other things, with interstate transfer of stolen property worth more than $5,000. When The Prophet and two of his Georgia colleagues were arrested on February 7, 1990, the Atlanta papers reported they faced 40 years in prison and a $2 million fine. Knight Lightning was arrested on February 15.

The property in question was the aforementioned blot on the history of prose whose full title was "A Bell South Standard Practice (BSP) 660-225-104SV-Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers, March, 1988."

And not only was this item worth more than $5,000, it was worth, according to the indictment and Bell South, precisely $79,449. And not a penny less. We will probably never know how this figure was reached or by whom, though I like to imagine an appraisal team consisting of Franz Kafka, Joseph Heller, and Thomas Pynchon . . .

In addition to charging Knight Lightning with crimes for which he could go to jail for 30 years and be fined $122,000, they seized his publication, *Phrack*, along with all related equipment, software and data, including his list of subscribers, many of whom would soon lose their computers and data for the crime of appearing on it.

I talked to Emmanuel Goldstein, the editor of *2600*, another hacker publication which has been known to publish purloined documents. If they could shut down *Phrack*, couldn't they as easily shut down *2600*?

He said, "I've got one advantage. I come out on paper and the Constitution knows how to deal with paper."

In fact, nearly all publications are now electronic at some point in their creation. In a modern newspaper, stories written at the scene are typed to screens and then sent by modem to a central computer. This computer composes the layout in electronic type and the entire product is transmitted electronically to the presses. There, finally, the bytes become ink.

Phrack merely omitted the last step in a long line of virtual events. However, that omission, and its insignificant circulation, left it vulnerable to seizure based on content. If the 911 document had been the Pentagon Papers (another proprietary document) and *Phrack* the *New York Times*, a completion of the analogy would have

seen the government stopping publication of the *Times* and seizing its every material possession, from notepads to presses.

Not that anyone in the newspaper business seemed particularly worried about such implications. They, and the rest of the media who bothered to report Knight Lightning's arrest, were too obsessed by what they portrayed as actual disruptions of emergency service and with marveling at the sociopathy of it. One report expressed relief that no one appeared to have died as a result of the "intrusions."

Meanwhile, in Baltimore, the 911 dragnet snared Leonard Rose, aka Terminus. A professional computer consultant who specialized in UNIX, Rose got a visit from the government early in February. The G-men forcibly detained his wife and children for six hours while they interrogated Rose about the 911 document and ransacked his system.

Rose had no knowledge of the 911 matter. Indeed, his only connection had been occasional contact with Knight Lightning over several years . . . and admitted membership in the Legion of Doom. However, when searching his hard disk for 911 evidence, they found something else. Like many UNIX consultants, Rose did have some UNIX source code in his possession. Furthermore, there was evidence that he had transmitted some of it to Jolnet and left it there for another consultant.

UNIX is a ubiquitous operating system, and though its main virtue is its openness to amendment at the source level, it is nevertheless the property of AT&T. What had been widely distributed within businesses and universities for years was suddenly, in Rose's hands, a felonious possession.

Finally, the Secret Service rewarded the good citizenship of Rich Andrews by confiscating the computer where Jolnet had dwelt, along with all the e-mail, read and unread, which his subscribers had left there. Like the many others whose equipment and data were taken by the Secret Service subsequently, he wasn't charged with anything. Nor is he likely to be. They have already inflicted on him the worst punishment a nerd can suffer: data death.

Andrews was baffled. "I'm the one that found it, I'm the one that turned it in. . . . And I'm the one that's suffering," he said.

One wonders what will happen when they find such documents on the hard disks of CompuServe, the largest commercial network system. Maybe I'll just upload my copy of Bell South Standard Practice (BSP) 660-225-104SV and see . . .

In any case, association with stolen data is all the guilt you need. It's quite as if the government could seize your house simply because a guest left a stolen VCR in an upstairs bedroom closet. Or confiscate all the mail in a post office upon finding a stolen package there. The first concept of modern jurisprudence to have arrived in Cyberspace seems to have been Zero Tolerance.

RICH ANDREWS was not the last to learn about the Secret Service's debonair new attitude toward the Fourth Amendment's protection against unreasonable seizure.

Early on March 1, 1990, the offices of a role-playing game publisher in Austin, Texas, called Steve Jackson Games were visited by agents of the United States Secret Service. They ransacked the premises, broke into several locked filing cabinets (damaging them irreparably in the process) and eventually left carrying three computers, two laser printers, several hard disks, and many boxes of paper and floppy disks.

Later in the day, callers to the Illuminati BBS (which Steve Jackson Games operated to keep in touch with role-players around the country) encountered the following message:

"So far we have not received a clear explanation of what the Secret Service was looking for, what they expected to find, or much of anything else. We are fairly certain that Steve Jackson Games is not the target of whatever investigation is being conducted; in any case, we have done nothing illegal and have nothing whatsoever to hide. However, the equipment that was seized is apparently considered to be evidence in whatever they're investigating, so we aren't likely to get it back any time soon. It could be a month, it could be never."

It's been three months as I write this, and not only has nothing been returned to them, but, according to Steve Jackson, the Secret Service will no longer take his calls. He figures that, in the months since the raid, his little company has lost an estimated $125,000. With such a fiscal hemorrhage, he can't afford a lawyer to take after the Secret Service. Both the state and national offices of the ACLU told him to "run along" when he solicited their help.

He tried to go to the press. As in most other cases, they were unwilling to raise the alarm. Jackson theorized, "The conservative press is taking the attitude that the suppression of evil hackers is a good thing and that anyone who happens to be put out of business in the meantime . . . well, that's just their tough luck."

In fact, *Newsweek* did run a story about the event, portraying it from Jackson's perspective, but they were almost alone in dealing with it.

What had he done to deserve this nightmare? Role-playing games, of which Dungeons and Dragons is the most famous, have been accused of creating obsessive involvement in their nerdy young players, but no one before had found it necessary to prevent their publication. It seems that Steve Jackson had hired the wrong writer. The managing editor of *Steve Jackson Games* is a former cracker, known by his fellows in the Legion of Doom as The Mentor. At the time of the raid, he and the rest of *Jackson* staff had been working for over a year on a game called GURPS Cyberpunk, High-Tech Low-Life Role-Playing.*

At the time of the Secret Service raids, the game resid-

* $18.95 postpaid from Box 18957, Austin, TX 78760.

ed entirely on the hard disks they confiscated. Indeed, it was their target. They told Jackson that, based on its author's background, they had reason to believe it was a "handbook on computer crime." It was therefore inappropriate for publication, First Amendment or no First Amendment.

I got a copy of the game from the trunk of The Mentor's car in an Austin parking lot. Like the Bell South document, it seemed pretty innocuous to me, if a little inscrutable. Borrowing its flavor from the works of William Gibson and Austin sci-fi author Bruce Sterling, it is filled with silicon brain implants, holodecks, and gauss guns.

It is, as the cover copy puts it, "a fusion of the dystopian visions of George Orwell and Timothy Leary." Actually, without the gizmos, it describes a future kind of like the present its publisher is experiencing at the hands of the Secret Service.

An unbelievably Byzantine world resides within its 120 large pages of small print. (These role-players must be some kind of idiots savants . . .) Indeed, it's a thing of such complexity that I can't swear there's no criminal information in there, but then I can't swear that Grateful Dead records don't have satanic messages if played backwards. Anything's possible, especially inside something as remarkable as Cyberpunk.

The most remarkable thing about Cyberpunk is the fact that it was printed at all. After much negotiation, Jackson was able to get the Secret Service to let him have some of his data back. However, they told him that he would be limited to an hour and a half with only one of his three computers. Also, according to Jackson, "They insisted that all the copies be made by a Secret Service agent who was a two-finger typist. So we didn't get much."

In the end, Jackson and his staff had to reconstruct most of the game from neural rather than magnetic memory. They did have a few very old backups, and they retrieved some scraps which had been passed around to game testers. They also had the determination of the enraged.

Despite government efforts to impose censorship by prior restraint, Cyberpunk is now on the market. Presumably, advertising it as "The game that was seized by the U.S. Secret Service" will invigorate sales. But Steve Jackson Games, the heretofore prosperous publisher of more than a hundred role-playing games, has been forced to lay off more than half of its employees and may well be mortally wounded.

Any employer who has heard this tale will think hard before he hires a computer cracker. Which may be, of course, among the effects the Secret Service desires.

ON MAY 8, 1990, Operation Sun Devil, heretofore an apparently random and nameless trickle of Secret Service actions, swept down on the Legion of Doom and its ilk like a bureaucratic tsunami. On that day, the Secret Service served 27 search warrants in 14 cities from Plano, Texas, to New York, New York. The law had come to Cyberspace. When the day was over, transit through the wide-open spaces of the Virtual World would be a lot trickier.

In a press release following the sweep, the Secret Service boasted having shut down numerous computer bulletin boards, confiscated 40 computers, and seized 23,000 disks. They noted in their statement that "the conceivable criminal violations of this operation have serious implications for the health and welfare of all individuals, corporations, and United States Government agencies relying on computers and telephones to communicate."

It was unclear from their statement whether "this operation" meant the Legion of Doom or Operation Sun Devil. There was room to interpret it either way.

Because the deliciously ironic truth is that, aside from the three-page Bell South document, the hackers had neither removed nor damaged anyone's data. Operation Sun Devil, on the other hand, had "serious implications" for a number of folks who relied on "computers and telephones to communicate." They lost the equivalent of about 5.4 million pages of information. Not to mention a few computers and telephones.

And the welfare of the individuals behind those figures was surely in jeopardy. Like the story of the single mother and computer consultant in Baltimore whose sole means of supporting herself and her 18-year-old son was stripped away early one morning. Secret Service agents broke down her door with sledgehammers, entered with guns drawn, and seized all her computer equipment. Apparently her son had also been using it . . .

Or the father in New York who opened the door at 6:00 a.m. and found a shotgun at his nose. A dozen agents entered. While one of them kept the man's wife in a choke-hold, the rest made ready to shoot and entered the bedroom of their sleeping 14-year-old. Before leaving, they confiscated every piece of electronic equipment in the house, including all the telephones.

It was enough to suggest that the insurance companies should start writing policies against capricious governmental seizure of circuitry.

In fairness, one can imagine the government's problem. This is all pretty magical stuff to them. If I were trying to terminate the operations of a witch coven, I'd probably seize everything in sight. How would I tell the ordinary household brooms from the getaway vehicles?

But as I heard more and more about the vile injustices being heaped on my young pals in the Legion of Doom, not to mention the unfortunate folks nearby, the less I was inclined toward such temperate thoughts as these. I drifted back into a sixties-style sense of the government, thinking it a thing of monolithic and evil efficiency and adopting an up-against-the-wall willingness to spit words like "pig" or "fascist" into my descriptions.

In doing so, I endowed the Secret Service with a clarity of intent which no agency of government will ever pos-

sess. Despite almost every experience I've ever had with federal authority, I keep imagining its competence.

For some reason, it was easier to invest the Keystone Kapers of Operation Sun Devil with malign purpose rather than confront their absurdity straight-on. There is, after all, a twisted kind of comfort in political paranoia. It provides one such a sense of orderliness to think that the government is neither crazy nor stupid and that its plots, though wicked, are succinct.

I was about to have an experience which would restore both my natural sense of unreality and my unwillingness to demean the motives of others. I was about to see first-hand the disorientation of the law in the featureless vastness of Cyberspace.

In Search of NuPrometheus

"I pity the poor immigrant . . . "
—Bob Dylan

SOMETIME LAST JUNE, an angry hacker got hold of a chunk of the highly secret source code which drives the Apple Macintosh. He then distributed it to a variety of addresses, claiming responsibility for this act of information terrorism in the name of the NuPrometheus League.

Apple freaked. NuPrometheus had stolen, if not the Apple crown jewels, at least a stone from them. Worse, NuPrometheus had then given this prize away. Repeatedly.

All Apple really has to offer the world is the software which lies encoded in silicon on the ROM chip of every Macintosh. This set of instructions is the cyber-DNA which makes a Macintosh a Macintosh.

Worse, much of the magic in this code was put there by people who not only do not work for Apple any longer, but might only do so again if encouraged with cattle prods. Apple's attitude toward its ROM code is a little like that of a rich kid toward his inheritance. Not actually knowing how to create wealth himself, he guards what he has with hysterical fervor.

Time passed, and I forgot about the incident. But one recent May morning, I learned that others had not. The tireless search for the spectral heart of NuPrometheus finally reached Pinedale, Wyoming, where I was the object of a two-hour interview by Special Agent Richard Baxter, Jr., of the Federal Bureau of Investigation.

Poor Agent Baxter didn't know a ROM chip from a Vise-Grip when he arrived, so much of that time was spent trying to educate him on the nature of the thing which had been stolen. Or whether "stolen" was the right term for what had happened to it.

You know things have rather jumped the groove when potential suspects must explain to law enforcers the nature of their alleged perpetrations.

I wouldn't swear Agent Baxter ever got it quite right. After I showed him some actual source code, gave a demonstration of e-mail in action, and downloaded a file from the WELL, he took to rubbing his face with both hands, peering up over his finger tips and saying, "It sure is something, isn't it" Or, "Whooo-ee."

Poor Agent Baxter didn't know a ROM chip from a Vise-Grip when he arrived, so much of our time was spent trying to educate him on the nature of the thing which had been stolen. Or whether "stolen" was the right term for what had happened to it.

Or "my eight-year-old knows more about these things than I do." He didn't say this with a father's pride so much as an immigrant's fear of a strange new land into which he will be forcibly moved and in which his own child is a native. He looked across my keyboard into Cyberspace and didn't like what he saw.

We could have made it harder for one another, but I think we each sensed that the other occupied a world which was as bizarre and nonsensical as it could be. We did our mutual best to suppress immune response at the border.

You'd have thought his world might have been a little more recognizable to me. Not so, it turns out. Because in his world, I found several unfamiliar features, including these:

1. The Hacker's Conference is an underground organization of computer outlaws with likely connections to, and almost certainly sympathy with, the NuPrometheus League. (Or as Agent Baxter repeatedly put it, the "New Prosthesis League.")

2. John Draper, the aforementioned Cap'n Crunch, in addition to being a known member of the Hacker's Conference, is also CEO and president of Autodesk, Inc. This is of particular concern to the FBI because Autodesk has many top-secret contracts with the government to supply Star Wars graphics imaging and "hyperspace" technology. Worse, Draper is thought to have Soviet contacts.

He wasn't making this up. He had lengthy documents from the San Francisco office to prove it. And in which Autodesk's address was certainly correct.

On the other hand, I know John Draper. While, as I say, he may have once distinguished himself as a cracker during the Pleistocene, he is not now, never has been, and never will be CEO of Autodesk. He did work there for a while last year, but he was let go long before he got in a position to take over.

Nor is Autodesk, in my experience with it, the Star Wars skunk works which Agent Baxter's documents indicated. One could hang out there a long time without ever seeing any gold braid.

Their primary product is something called AutoCAD, by far the most popular computer-aided design software but generally lacking in lethal potential. They do have a small development program in Cyberspace, which is what they call Virtual Reality. (This, I assume is the "hyperspace" to which Agent Baxter's documents referred.)

However, Autodesk had reduced its Cyberspace program to a couple of programmers. I imagined Randy Walser and Carl Tollander toiling away in the dark and lonely service of their country. Didn't work. Then I tried to describe Virtual Reality to Agent Baxter, but that didn't work either. In fact, he tilted. I took several runs at it, but I could tell I was violating our border agreements. These seemed to include a requirement that neither of us try to drag the other across into his conceptual zone.

I fared a little better on the Hacker's Conference. Hardly a conspiracy, the Hacker's Conference is an annual convention originated in 1984 by the Point Foundation and the editors of *Whole Earth Review*. Each year it invites about a hundred of the most gifted and accomplished of digital creators. Indeed, they are the very people who have conducted the personal computer revolution. Agent Baxter looked at my list of Hacker's Conference attendees and read their bios. "These are the people who actually design this stuff, aren't they?" He was incredulous. Their corporate addresses didn't fit his model of outlaws at all well.

Why had he come all the way to Pinedale to investigate a crime he didn't understand which had taken place (sort of) in five different places, none of which was within 500 miles?

Well, it seems Apple has told the FBI that they can expect little cooperation from Hackers in and around the Silicon Valley, owing to virulent anti-Apple sentiment there. They claim this is due to the Hacker belief that software should be free combined with festering resentment of Apple's commercial success. They advised the FBI to question only those Hackers who were as far as possible from the twisted heart of the subculture.

They did have their eye on some local people though. These included a couple of former Apple employees, Grady Ward and Walter Horat, Chuck Farnham (who has made a living out of harassing Apple), Glenn Tenney (the purported leader of the Hackers), and, of course, the purported CEO of Autodesk.

Other folks Agent Baxter asked me about included Mitch Kapor, who wrote Lotus 1-2-3 and was known to have received some of this mysterious source code. Or whatever. But I had also met Mitch Kapor, both on the WELL and in person. A less likely computer terrorist would be hard to come by.

Actually, the question of the source code was another area where worlds but shadow-boxed. Although Agent Baxter didn't know source code from Tuesday, he did know that Apple Computer had told his agency that what had been stolen and disseminated was the complete recipe for a Macintosh computer. The distribution of this secret formula might result in the creation of millions of Macintoshes not made by Apple. And, of course, the ruination of Apple Computer.

In my world, NuPrometheus (whoever they, or more likely, he might be) had distributed a small portion of the code which related specifically to Color QuickDraw. QuickDraw is Apple's name for the software which controls the Mac's on-screen graphics. But this was another detail which Agent Baxter could not capture. For all he knew, you could grow Macintoshes from floppy disks.

I explained to him that Apple was alleging something like the ability to assemble an entire human being from the recipe for a foot, but even he knew the analogy was inexact. And trying to get him to accept the idea that a corporation could go mad with suspicion was quite futile. He had a far different perception of the emotional reliability of institutions.

When he finally left, we were both dazzled and disturbed. I spent some time thinking about Lewis Carroll and tried to return to writing about the legal persecution of the Legion of Doom. But my heart wasn't in it. I found myself suddenly too much in sympathy with Agent Baxter and his struggling colleagues from Operation Sun Devil to get back into a proper sort of pig-bashing mode.

Given what had happened to other innocent bystanders like Steve Jackson, I gave some thought to getting scared. But this was Kafka in a clown suit. It wasn't precisely frightening. I also took some comfort in a phrase once applied to the administration of Frederick the Great: "Despotism tempered by incompetence."

Of course, incompetence is a double-edged banana. While we may know this new territory better than the authorities, they have us literally out-gunned. One should pause before making well-armed paranoids feel foolish, no matter how foolish they seem.

The Fear of White Noise

"Neurosis is the inability to tolerate ambiguity."
—Sigmund Freud, appearing to me in a dream

I'M A MEMBER of that half of the human race which is inclined to divide the human race into two kinds of people. My dividing line runs between the people who crave certainty and the people who trust chance.

You can draw this one a number of ways, of course, like Control vs. Serendipity, Order vs. Chaos, Hard Answers vs. Silly Questions, or Newton, Descartes & Aquinas vs. Heisenberg, Mandelbrot & the Dalai Lama. Etc.

Large organizations and their drones huddle on one end of my scale, busily trying to impose predictable homogeneity on messy circumstance. On the other end, freelancers and ne'er-do-wells cavort about, getting by on luck if they get by at all.

However you cast these poles, it comes down to the difference between those who see life as a struggle against cosmic peril and human infamy and those who believe, without any hard evidence, that the universe is actually on our side. Fear vs. Faith.

I am of the latter group. Along with Gandhi and Rebecca of Sunnybrook Farm, I believe that other human beings will quite consistently merit my trust if I'm not doing something which scares them or makes them feel bad about themselves. In other words, the best defense is a good way to get hurt.

In spite of the fact that this system works very reliably for me and my kind, I find we are increasingly in the minority. More and more of our neighbors live in armed compounds. Alarms blare continuously. Potentially happy people give their lives over to the corporate state as though the world were so dangerous outside its veil of collective immunity that they have no choice.

I have a number of theories as to why this is happening. One has to do with the opening of Cyberspace. As a result of this development, humanity is now undergoing the most profound transformation of its history. Coming into the Virtual World, we inhabit Information. Indeed, we become Information. Thought is embodied and the Flesh is made Word. It's weird as hell.

Beginning with the invention of the telegraph and extending through television into Virtual Reality, we have been, for over a century, experiencing a terrifying erosion in our sense of both body and place. As we begin to realize the enormity of what is happening to us, all but the most courageous have gotten scared.

And everyone, regardless of his psychic resilience, feels this overwhelming sense of strangeness. The world, once so certain and tangible and legally precise, has become an infinite layering of opinions, perceptions, litigation, camera-angles, data, white noise, and, most of all, ambiguities. Those of us who are of the fearful persuasion do not like ambiguities.

Indeed, if one were a little jumpy to start with, he may now be fairly humming with nameless dread. Since no one likes his dread to be nameless, the first order of business is to find it some names.

For a long time here in the United States, Communism provided a kind of catch-all bogeyman. Marx; Stalin and Mao summoned forth such a spectre that, to many Americans, annihilation of all life was preferable to the human portion's becoming Communist. But as Big Red wizened and lost his teeth, we began to cast about for a replacement.

Finding none of sufficient individual horror, we have draped a number of objects with the old black bunting which once shrouded the Kremlin. Our current spooks are terrorists, child abductors, AIDS, and the underclass. I would say drugs, but anyone who thinks that the War

on Drugs is not actually the War on the Underclass hasn't been paying close enough attention.

There are a couple of problems with these Four Horsemen. For one thing, they aren't actually very dangerous. For example, only seven Americans died in worldwide terrorist attacks in 1987. Fewer than 10 (out of about 70 million) children are abducted by strangers in the U.S. each year. Your chances of getting AIDS if you are neither gay nor a hemophiliac nor a junkie are considerably less than your chances of getting killed by lightning while golfing. The underclass is dangerous, of course, but only, with very few exceptions, if you are a member of it.

The other problem with these perils is that they are all physical. If we are entering into a world in which no one has a body, physical threats begin to lose their sting.

And now I come to the point of this screed: The perfect bogeyman for Modern Times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He understands the value of things you can't conceptualize long enough to cash in on. He is the one-eyed man in the Country of the Blind.

In a world where you and your wealth consist of nothing but beeps and boops of micro-voltage, he can steal all your assets in nanoseconds and then make you disappear.

He can even reach back out of his haunted mists and kill you physically. Among the justifications for Operation Sun Devil was this chilling tidbit:

"Hackers had the ability to access and review the files of hospital patients. Furthermore, they *could have* added, deleted, or altered vital patient information, *possibly* causing life-threatening situations." [Emphasis added.]

Perhaps the most frightening thing about the Cyberpunk is the danger he presents to The Institution, whether corporate or governmental. If you are frightened you have almost certainly taken shelter by now in one of these collective organisms, so the very last thing you want is something which can endanger your heretofore unassailable hive.

And make no mistake, crackers will become to bureaucratic bodies what viruses presently are to human bodies. Thus, Operation Sun Devil can be seen as the first of many waves of organizational immune response to this new antigen. Agent Baxter was a T-cell. Fortunately, he didn't know that himself and I was very careful not to show him my own antigenic tendencies.

I think that herein lies the way out of what might otherwise become an Armageddon between the control freaks and the neo-hip. Those who are comfortable with these disorienting changes must do everything in our power to convey that comfort to others. In other words, we must share our sense of hope and opportunity with those who feel that in Cyberspace they will be obsolete eunuchs for sure.

It's a tall order. But, my silicon brothers, our self-interest is strong. If we come on as witches, they will burn us. If we volunteer to guide them gently into its new lands, the Virtual World might be a more amiable place for all of us than this one has been. Of course, we may also have to fight.

DEFINING THE CONCEPTUAL and legal map of Cyberspace before the ambiguophobes do it for us (with punitive over-precision) is going to require some effort. We can't expect the Constitution to take care of itself. Indeed, the precedent for mitigating the constitutional protection of a new medium has already been established. Consider what happened to radio in the early part of this century.

Under the pretext of allocating limited bandwidth, the government established an early right of censorship over broadcast content which still seems directly unconstitutional to me. Except that it stuck. And now, owing to a large body of case law, looks to go on sticking.

New media, like any chaotic system, are highly sensitive to initial conditions. Today's heuristical answers of the moment become tomorrow's permanent institutions of both law and expectation. Thus, they bear examination with that destiny in mind.

Earlier in this article, I asked a number of tough questions relating to the nature of property, privacy, and speech in the digital domain. Questions like: "What are data and what is free speech?" or "How does one treat property which has no physical form and can be infinitely reproduced?" or "Is a computer the same as a printing press?" The events of Operation Sun Devil were nothing less than an effort to provide answers to these questions. Answers which would greatly enhance governmental ability to silence the future's opinionated nerds.

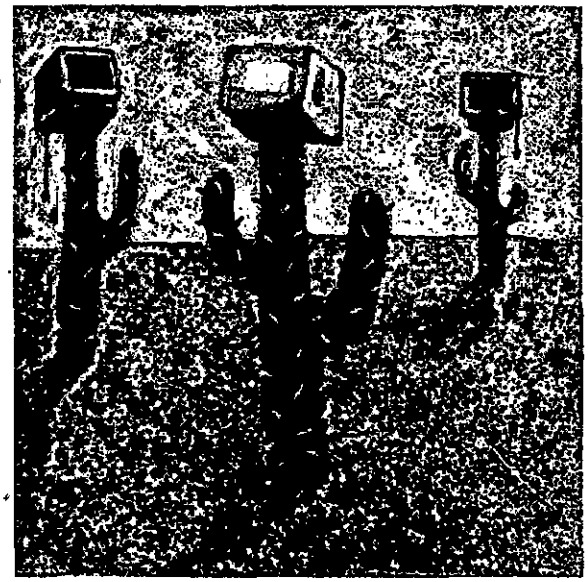
In overreaching as extravagantly as they did, the Secret Service may actually have done a service for those of us who love liberty. They have provided us with a devil. And devils, among their other galvanizing virtues, are just great for clarifying the issues and putting iron in your spine. In the presence of a devil, it's always easier to figure out where you stand.

While I previously had felt no stake in the obscure conundra of free telecommunication, I was, thanks to Operation Sun Devil, suddenly able to plot a trajectory from the current plight of the Legion of Doom to an eventual constraint on opinions much dearer to me. I remembered Martin Neimoeller, who said: "In Germany they came first for the Communists, and I didn't speak up because I wasn't a Communist. Then they came for the Jews, and I didn't speak up because I wasn't a Jew. They came for the trade unionists, and I didn't speak up because I wasn't a trade unionist. Then they came for the Catholics, and I didn't speak up because I was a Protestant. Then they came for me, and by that time no one was left to speak up."

I decided it was time for me to speak up.

The evening of my visit from Agent Baxter, I wrote an

The perfect bogeyman for Modern Times is the Cyberpunk! He is so smart he makes you feel even more stupid than you usually do. He knows this complex country in which you're perpetually lost. He is the one-eyed man in the Country of the Blind.



account of it which I placed on the WELL. Several days later, Mitch Kapor literally dropped by for a chat.

Also a WELL denizen, Kapor had read about Agent Baxter and had begun to meditate on the inappropriateness of leaving our civil liberties to be defined by the technologically benighted. A man who places great emphasis on face-to-face contact, he wanted to discuss this issue with me in person. He had been flying his Canadair bizjet to a meeting in California when he realized his route took him directly over Pinedale.

We talked for a couple of hours in my office while a spring snowstorm swirled outside. When I recounted for him what I had learned about Operation Sun Devil, he decided it was time for him to speak up too.

He called a few days later with the phone number of a civil libertarian named Harvey Silverglate, who, as evidence of his conviction that everyone deserves due process, is currently defending Leona Helmsley. Mitch asked me to tell Harvey what I knew, with the inference that he would help support the costs which are liable to arise whenever you tell a lawyer anything.

I found Harvey in New York at the offices of that city's most distinguished constitutional law firm, Rabinowitz, Boudin, Standard, Krinsky, and Lieberman. These are the folks who made it possible for the *New York Times* to print the Pentagon Papers. (Not to dwell on the unwilling notoriety which partner Leonard Boudin achieved back in 1970 when his Weathergirl daughter blew up the family home . . .)

In the conference call which followed, I could almost hear the skeletal click as their jaws dropped. The next day, Eric Lieberman and Terry Gross of Rabinowitz, Boudin met with Acid Phreak, Phiber Optik, and Scorpion.

The maddening trouble with writing this account is that *Whole Earth Review*, unlike, say, *Phrack*, doesn't publish instantaneously. Events are boiling up at such a frothy pace that anything I say about current occurrences surely will not obtain by the time you read this. The road from here is certain to fork many times. The printed version of this will seem downright quaint before it's dry.

But as of today (in early June of 1990), Mitch and I are legally constituting the Electronic Frontiers Foundation,* a two (or possibly three)-man organization which will raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace.

Already, on the strength of preliminary stories about our efforts in the *Washington Post* and the *New York Times*, Mitch has received an offer from Steve Wozniak to match whatever funds he dedicates to this effort. (As well as a fair amount of abuse from the more institutionalized precincts of the computer industry.)

The Electronic Frontiers Foundation will fund, conduct, and support legal efforts to demonstrate that the Secret Service has exercised prior restraint on publications, limited free speech, conducted improper seizure of equipment and data, used undue force, and generally conducted itself in a fashion which is arbitrary, oppressive, and unconstitutional.

In addition, we will work with the Computer Professionals for Social Responsibility and other organizations to convey to both the public and the policy-makers metaphors which will illuminate the more general stake in liberating Cyberspace.

Not everyone will agree. Crackers are, after all, generally beyond public sympathy. Actions on their behalf are not going to be popular no matter who else might benefit from them in the long run.

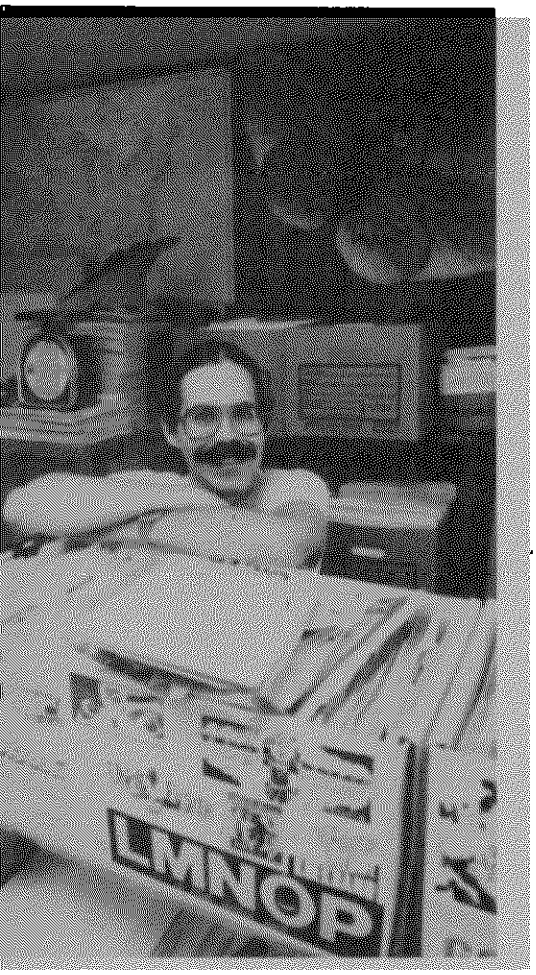
Nevertheless, in the litigations and political debates which are certain to follow, we will endeavor to assure that their electronic speech is protected as certainly as any opinions which are printed or, for that matter, screamed. We will make an effort to clarify issues surrounding the distribution of intellectual property. And we will help to create for America a future which is as blessed by the Bill of Rights as its past has been. ■

* 1 Cambridge Center, Cambridge, MA 02142.

ZINES

WHERE THE ACTION IS: THE VERY SMALL PRESS IN AMERICA

BY MIKE GUNDERLOY



Mike Gunderloy, the Grand Cataloguer of the underground press in America, stands behind his awesome collection of paper narrowcasting. His own zine, Factsheet Five *(6 Arizona Ave., Rensselaer, NY 12144-4502; $6/year) tracks the flow of thousands of personal publishers, made possible by the copy machine.*

—Kevin Kelly

I KNOW A PLACE where you can find out about the art of writing *renga*. A place where people discuss the merits of Japanese monster movies. A place where the preservation of cave fish is more important than housing developments. One where men grapple with feminism and what it means to their lives — and where women can be alone for a moment without the presence of men. One where new languages are being invented and learned even as you read this. One where workers, from old-line unionists to new burger-flippers, talk about work in their own words. One where the battle over where to hold science-fiction conventions is a matter of the gravest importance. One where millions of facts, near-facts, rumors, suspicions and downright lies are available to anyone who cares to look for them. The place? It's the very small press.

I'm excited about the very small press, whether you call it the underground press, the alternative press, or simply "zines" (short for "fanzines," a contraction of "fan magazines" which originated with lovers of science fiction). I don't mean, for the most part, things like *Whole Earth Review*. On the scale I'm considering, *WER* is a *mega*zine, so large as to be almost frightening. No, what I'm excited about are publications like *Gray Matter, Flipside, Greed, Yellow Silk, Kick It Over, Sign of the Times, It's, Union of Opposites, Philly Zine, Ju'i Lobypli, Quimby,* and *The Kvinde Hader Klub*: things with a circulation in the thousands, the hundreds, and sometimes only in the tens. This is where the action is, where information (and disinformation) is free, where things are happening.

Of course, when you're immersed in a sea of hammers, it's sometimes difficult to remember that not everyone wants to drive nails all the time. I've been collecting the very small press since about 1977, seriously so since 1982 when I started publishing *Factsheet Five*. In mid-1990, I don't have an exact count except in archivist's terms: about 150 linear feet of files (with close to another foot coming in each week). As near as I can figure, that amounts to about 25,000 separate issues of some 10,000 titles. And at best, I'm only getting about 10 percent of what gets published in the United States alone — not even thinking about the rest of the world.

These figures are a bit less impressive when you think about the people at the other end of the information pipeline: the readers. Out of those 10,000 zines, only a few hundred have ever had a circulation over 1,000. Of these at least half have gone out of business — the half-life of a zine is on the order of two years (that is, two years from now half the current zines will be out of business).

Even when they don't go bankrupt, editors on this scale tend to move on to other things as their interests change. Since for most of us there is no fortune and darned little fame to be made from publishing a zine, this is quite understandable. All in all, there are at most a couple of million people who read any of these things, and only a handful of hardcore zine junkies who, like myself, read lots of them.

So then why am I excited? Because these people, the few thousand publishers and the few million readers, are the ones at the cutting edge of social change. Even when they think they're just writing or reading about punk music, kite-flying, the revival of Asatru, or new sculpture, these people are part of A Phenomenon. Our industrial society has finally brought things to the point where almost anyone can own the means of production of a zine. Cheap photocopiers, cheap computers and (if you don't believe me, look at other countries) cheap postage have

at's what happens to Vivian nd Roger at the end of the book. We were interested in that newness and freshness, the discovery of a lost thing, which is the basis for their relationship."

"The sense that the past is past and the future is possible," Erdrich says. "We try to grapple with time — the impact of history. What creates the present."

Although the setting and some of the circumstances of "The Crown of Columbus" are similar to aspects of their own lives, the only real trace of autobiography in the book, Erdrich and Dorris say, is in the person of Violet, the baby girl whom Vivian bears near the beginning of the book and who ends up perilously abandoned and rediscovered at its end.

"We don't write autobiographically, but we did have a baby daughter, Aza, while we were writing this book," Dorris says. "And we knew early on she had to be in there because she was certainly making herself felt."

"A lot of times, one of us would write that the baby was crying," Erdrich confirms, "and the baby *was* crying."

The story of Columbus is of an ethnically confused man introducing ethnic confusion to a continent. In a way, this represents a deeper autobiographical theme. Vivian might be speaking for Erdrich when she says of her mixed heritage: "There are advantages to not being this or that. You have a million stories, one for every occasion, and in a way they're all lies and in another way they're all true. . . . There are times when I control who I'll be, and times when I let other people decide. I'm not all anything, but I'm a little bit of a lot. My roots spread in every direction, and if I water one set of them more often than others, it's because they need it more."

And the overall thematic conflict of the book — the question Dorris posed as "What do you do when you discover something you didn't expect to discover?" — flips back in an intriguing way on "The Broken Cord," which is a narrative about Dorris's discovery of his son's problems, a discovery that ran counter to his expectations and that he strongly resisted. The issue of Dorris and Erdrich's relationship with their son is symbolically reconstructed in "The Crown of Columbus" in the person of Nash, Vivian's 16-year-old son by an earlier marriage. Roger's rage at Nash, a diffi-

(Continued on Page 76)

IN DEFENSE OF HACKERS

Computer buffs use modems, money and a new foundation to fight Government prosecution.

BY CRAIG BROMBERG

WHEN JOHN PERRY BARLOW picked up the phone at his home in Pinedale, Wyo., on a sunny morning last May, the last thing he expected was a call from the Federal Bureau of Investigation. But as a sometime writer and electronic gadfly who has been, among other things, a cattle rancher, Republican county chairman and, for 20 years, a lyricist for the rock band the Grateful Dead, he wasn't exactly surprised.

Special Agent Richard H. Baxter was polite, but he wouldn't explain what the bureau wanted over the phone. Barlow didn't mind. He just assumed that the Feds wanted to talk to him about some comments he had recently made in a Harper's Magazine forum on computer cracking — obtaining illegal access to giant computer networks over the telephone — comments that the editors had seen fit to put on the cover.

"Americans who believe in democracy have little choice but to shred the barricades of secrecy at every opportunity," Barlow, 43 years old, wrote in an excitable moment. "It isn't merely permissible to break into the White House computer system. It is a moral obligation." Barlow saw as how the F.B.I. might think those provocative words, but as soon as Agent Baxter arrived at the door with a long list of questions scrawled on his clipboard about what he called the "New Prosthesis League," Barlow knew that all bets were off.

It turned out that Agent Baxter was interested in the "nuPrometheus League," a shadowy conspiracy that had been sending morsels of Apple Computer's highly guarded source code for the Macintosh computer — the copyrighted set of instructions governing the look and operation of the screen — to various computer-world luminaries. But since Agent Baxter could not, in Barlow's words, "tell a ROM-chip from a Vise-Grip," the electronic cowboy spent the next two hours tutoring the G-man in the rudiments of telecomputing, showing him how one could use a computer and modem to "log on" to various electronic services, how to upload and download files, and how to identify source code, the very stuff of computer programming. "I realized right away before I could demonstrate my innocence," Barlow later wrote in a newsletter on computer privacy issues, "I would first have to explain to him what guilt might be."

As it happened, the visit by Baxter was just one episode in a major Government campaign to prosecute computer criminals. That same month, the United States Secret Service, which investigates a wide variety of electronic crimes from credit card fraud to illegal computer trespass for the Department of the Treasury, made public its largest computer crime investigation ever. Operation Sun Devil, using more than 150 Secret Service agents who served 28 search warrants in 14 cities, seized some 23,000 diskettes and 42 computers. According to Garry M. Jenkins, then assistant director of the Secret Service, Sun Devil was "sending a clear message to those computer hackers who have decided to violate the laws of this nation in the mistaken belief that they can successfully avoid detection by hiding behind the relative anonymity of their computer terminals."

For the Government, Sun Devil represented a drastic change of direction. Law enforcement had for years treated computer crime as a white-collar con, a second-fiddle felony.

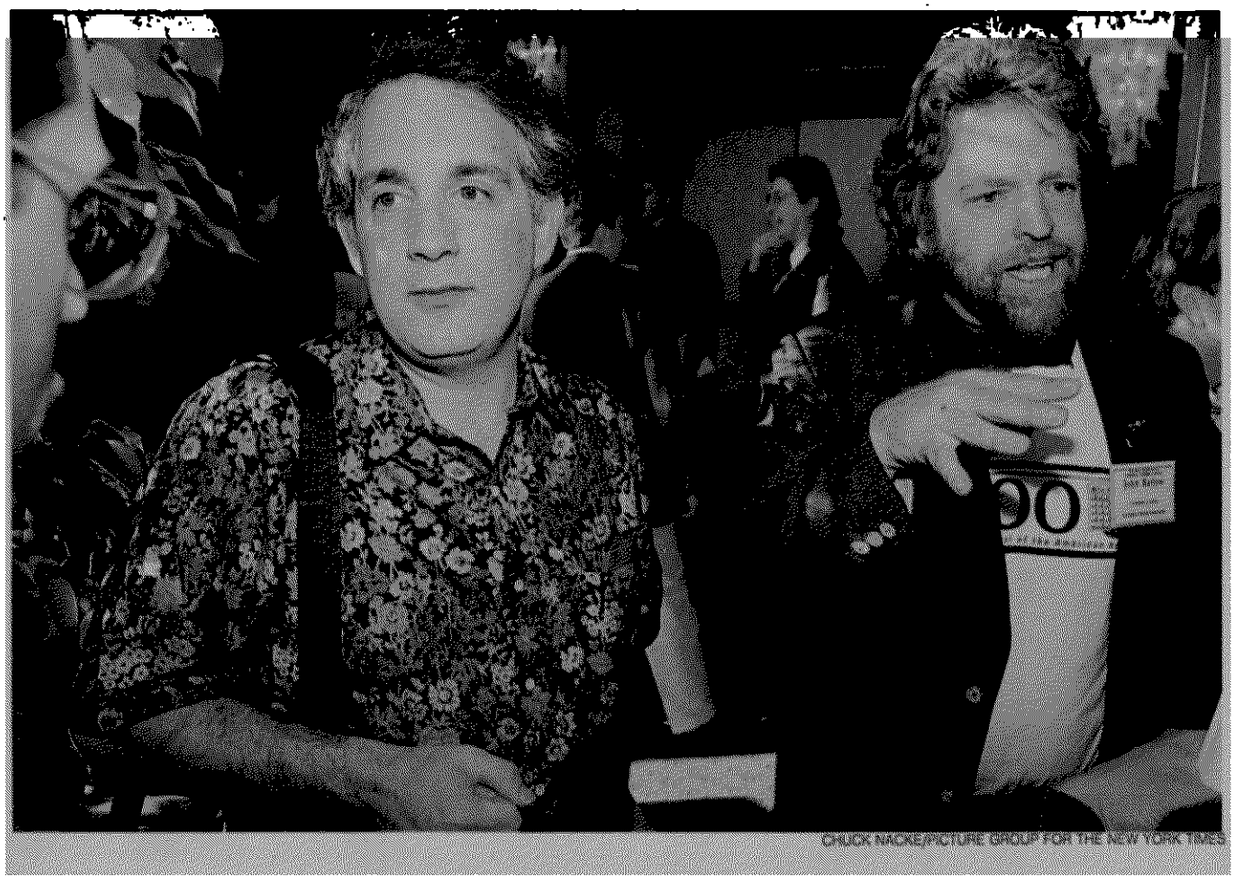
But after Robert Tappan Morris, the Cornell University student who brought the nation's largest computer network to the verge of a breakdown with a malfunctioning "worm" program, was caught in 1988, the Government seemed ready to find a criminal behind every computer with a modem, the device that turns digital data into electronic signals to be sent over the phone.

Suddenly, the high-school and college students who had only recently been tolerated as joy riders on the nation's information networks didn't seem so innocent. They were electronic swindlers. Criminals. Possibly even spies. Cliff Stoll, a young astronomer-turned-computer sleuth, discovered an infiltrator burrowing through unclassified but sensitive military files about the Strategic Defense Initiative, and caught the Government unprepared. After a frustrating (and ultimately successful) campaign to interest the F.B.I., Central Intelligence Agency and National Security Agency in his quest for the intruder, Stoll tracked him to Hanover, Germany, where he was working for the K.G.B. Stoll got lucky. There may well have been other infiltrations of America's electronic networks by agents of the Eastern bloc countries and the K.G.B. intent on altering, stealing or destroying proprietary corporate information and classified U.S. military data. "Much of

Craig Bromberg is a freelance writer whose work has appeared in Rolling Stone and Vanity Fair.

Compared to his ranch, John Perry Barlow says, "the computer was clean." It was, he says, "the one place I found I could really manipulate reality."

TED WOOD FOR THE NEW YORK TIMES



CHUCK NACKE/PICTURE GROUP FOR THE NEW YORK TIMES

The software designer Mitch Kapor, left, and John Barlow began the Electronic Frontier Foundation. It helps hackers in trouble with the law.

today's spying is garden-variety electronic surveillance," says Stoll, who turned his tale of tracking the Hanover hacker into a best seller, "The Cuckoo's Egg." "The spy risks embarrassment and even death, but the computer programmer whose aim is stealing information doesn't even have to leave home." Computer crime, the United States Government decided, wasn't just costing the country billions of dollars and endangering the very basis of intellectual property in the electronic age; it was becoming a potential threat to national security.

But how to police the new electronic frontier? As Barlow explained to Agent Baxter, there are millions of computer owners around the globe who possess the capacity — phone, computer, modem and simple software — to tap into this vast interconnective universe.

The very essence of what Barlow calls "the culture of the nerd — the solitary libertarian down in his basement saying 'Don't tread on me' " — is resistance to standardization and control. Hackers, the computer wizards of this brave new world, had long adopted a rather strict code of honor on their own: not to erase or damage others' files; not to change data; not to use a system for personal gain. And for the most part, the system worked, encouraging the free exchange of ideas via technology.

The first hackers, mostly students at the Massachusetts Institute of Technology in the early 60's, were hardware buffs with an obsessive passion for circumventing whatever limitations prevented them from working on the few computers then around. To these hackers, the goal was to gain access to a system — any system. They would go to extreme lengths to do it: breaking down computer-room doors, exploiting program bugs, staying up for days on end until the new machines yielded their secrets. "Further!" has always been the hacker's cry.

As computer hardware and software became increasingly accessible and interconnected, the game changed. Hackers came to see access to computer networks as the real challenge. They loved to see what systems they could dial onto, either by "social engineering" — persuading a system operator that they needed immediate access — or sheer guesswork, lobbing passwords like "root," "admin," or "system" at a remote network until it finally opened up. Nor was this just the aberrant behavior of a few wayward computer fiends: Steve Wozniak and Steve Jobs first acquired the capital to start Apple Computer by selling "blue boxes," devices that enabled "phone phreaks" to make calls around the world for a dime.

Most hackers haven't taken "further" as an invitation to trespass, but there are always those hackers who will operate with criminal intent, "crackers" who put personal gain before the creative power of computing. Operation Sun Devil was just one of a half-dozen law-enforcement operations around the country aimed at them.

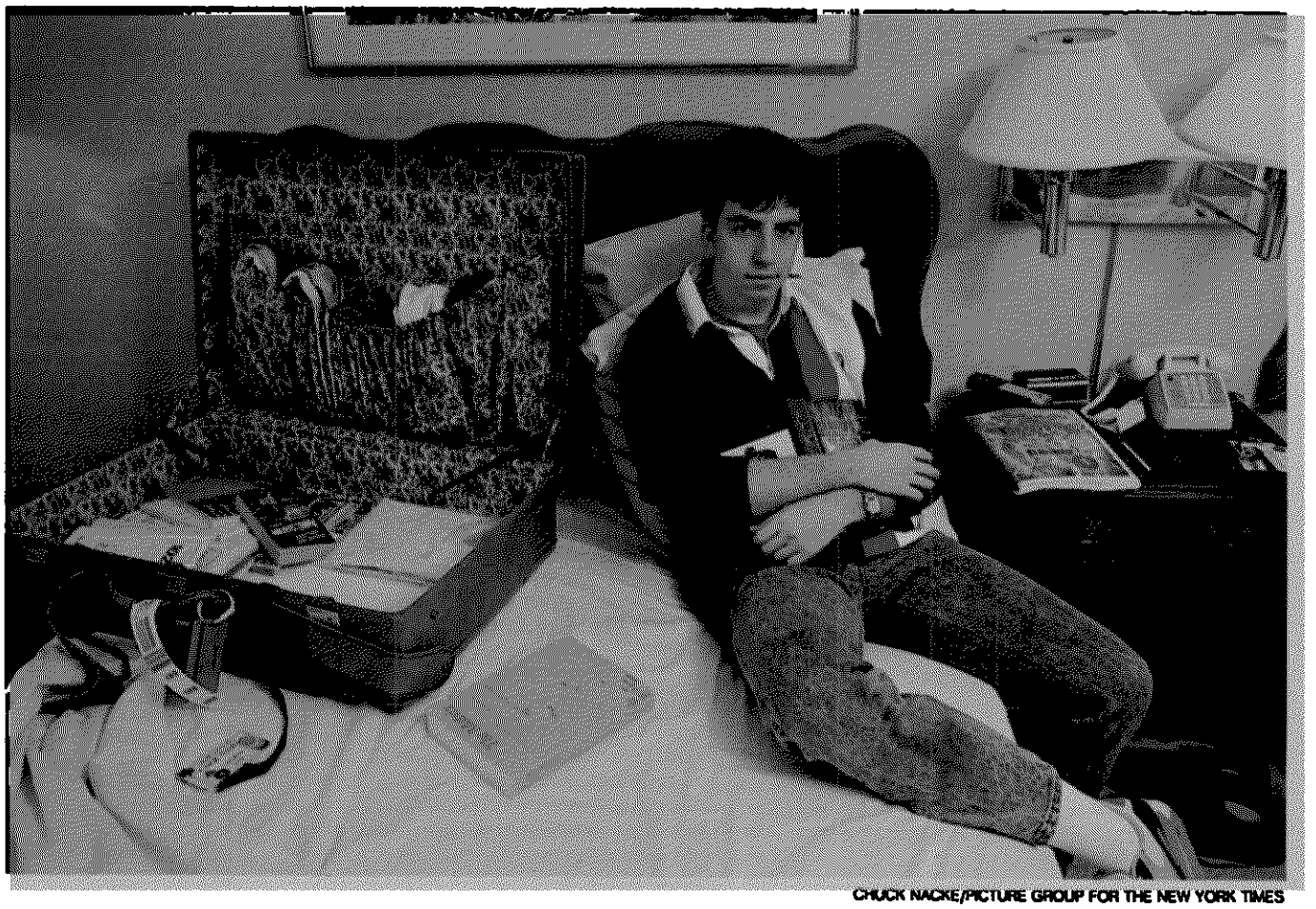
Among the Government's first targets was Craig Neidorf, a 19-year-old University of Missouri student who published an electronic magazine called Phrack; he was indicted in February 1990 on felony charges of wire fraud and interstate transportation of stolen property, accused of publishing a stolen Bell South memorandum on the emergency 911 telephone system. A month later, on a drizzly March day, the United States Secret Service paid a visit to Steve Jackson Games, a small computer game-book publisher in Austin, Tex. Armed with guns, crowbars, a search warrant and accompanied by representatives of the Austin police, the agents confiscated three computers, one laser printer, numerous hard drives, hundreds of disks and a large bag of screws. No arrests were made, no charges were filed and no explanations were given.

Steve Jackson was mystified by the raid on his premises. What could the Secret Service want with a small book publisher's computer equipment? The search warrant affidavit had been sealed by the Austin court at the request of the Secret Service. One clue to the raid was that the agents had confiscated most of the materials used to produce Jackson's latest book, "Gurps Cyberpunk: High-Tech Low-Life Roleplaying Sourcebook." It was true that "Gurps Cyberpunk" included a chapter giving instructions on computer cracking — a crime that was under the service's purview — but he was publishing a book about the future, a bleak Baedeker in which game players adopted the identities of various dystopian criminals.

It would be four months before the Secret Service returned the "Gurps Cyberpunk" material, and Steve Jackson would be forced to lay off nearly half of his 17 employees in the interim. But what else was Jackson to do? With the warrant sealed, and the Secret Service ignoring the pleas of Representative J. J. Pickle (Jackson's Congressman) and both Texas Senators, there was no way to know what the Secret Service had been looking for. It was almost as if the First Amendment had never existed.

AS SOON AS AGENT BAXTER headed back to the F.B.I.'s office in Rock Springs, Wyo., John Barlow wrote up his experience with the F.B.I. and posted it on the WELL.

The WELL — Whole Earth 'Lectronic Link — is a powerful computer conferencing network that was started in 1985 as a kind of computer adjunct to the Whole Earth Catalogue, Stewart Brand's massive "access to tools" supply book, and has since taken on a life of its own. (The Whole Earth Review published Barlow's essay as "Crime and Puzzlement" last summer.) Conference systems like the WELL and its more recent New York counterpart, Echo, have been compared to silicon salons or digital nightclubs, 24-hour-a-day electronic villages where the residents meet each other through their fingertips. With 5,000-odd "WELLbeings" paying monthly charges



CHUCK NACKE/PICTURE GROUP FOR THE NEW YORK TIMES

Craig Neidorf, a 19-year-old who published an electronic magazine called Phrack, was charged with publishing a stolen phone company memo.

and "connect time" to participate in conferences on everything from gardening to global business to the Mac and I.B.M. PC, virtual reality, spirituality, sex and the Grateful Dead, the WELL seems very much like a small town that has sprung from the mind of a very hip Silicon Valley yuppie.

Barlow soon found that he wasn't the only one on the WELL who had been interviewed by the F.B.I. Eventually he would meet many others, among them Mitchell Kapor, 40, the software supernova who co-developed the classic business spreadsheet program Lotus 1-2-3 and is now chairman of ON Technology, which is based in Cambridge, Mass. Kapor had received a copy of the nuPrometheus diskette in the mail.

Thinking it might be a clever ploy to infect his computer with a virus, he promptly tossed the diskette in a drawer — until the summer of 1989, when he read reports of the nuPrometheus case in Macworld magazine. At that point he had his chief technologist examine the disk. Sure enough, the disk contained a portion of the code to Apple's Color Quickdraw, the software behind the Mac's famous graphic capabilities. Kapor called his attorney, who advised him to send the disk to Apple as soon as he could. A few months later, the F.B.I. paid a visit to Kapor's office.

Until Barlow posted his story on the WELL months later, Kapor had filed the F.B.I.'s visit to his office under inexplicable events. But reading the electronic version of "Crime and Puzzlement" put everything in perspective for him. "I suddenly realized I wasn't alone," he says, "that I had some direct connection to this, that nuPrometheus was connected to all the other arrests of computer hackers at the time, and I began to see how great an injustice could be taking place within such a huge investigation as Sun Devil."

Kapor didn't doubt that there were serious criminal violations going on in computer networks. But he wondered whether the rumors he was hearing about Sun Devil — searches and seizures with guns drawn against 16-year-old crackers and their families, confiscations of every piece of electronic equipment in their homes, from computers to clock radios — could possibly be true. The more he thought about how the F.B.I. had required a virtual Berlitz course in computers simply to do its meager interview with him, the more he began to worry about those kids. As a former "nerd" himself, he identified with them, understood how their boredom and lack of socialization could lead them to go joy riding through the vast networks of the electronic frontier.

A few weeks later, as Kapor was making plans to fly to California — one of the luxuries of his Lotus success is a private jet — he phoned Barlow and asked if he would mind very much if Kapor touched down in Pinedale, Wyo. It was not an offer the computer cowboy could refuse.

John Perry Barlow really does live on the frontier. Even if you drive at top speed, the nearest city, Jackson, Wyo., is over an hour away, past wide pastures of grazing elk, cows and wild horses. Barlow rarely goes there anyway. He can usually get what he needs in Pinedale, and what he can't get eventually comes to him by mail or over the phone — by fax and modem.

On the WELL, he is the No. 1 digital Deadhead, equal parts beat poet and P. T. Barnum. One minute he delivers a scalding jeremiad on the "droids" who run Microsoft and Apple, turning people into "knowledge workers" and computers into "personal productivity tools"; the next, he is carrying on about the dream of an electronic virtual reality in which cyberspace is "given actual human-scale interaction so that you're not reduced to what you can squeeze through your fingertips with just typing."

Barlow rarely "just types." His old drinking buddies have left the sign reading "Pinedale Thinking Service" over the door of a nearby saloon, and you can discern in his craggy, bearded face the psychic toll that his attempt to straddle two disparate cultures — rock-and-roll and computing — has taken over the years.

His office is surrounded with books and mementos that reflect these divided allegiances: Eliot Janeway's "Economics of Chaos" next to Allen Ginsberg's "Howl"; signed photographs from President Bush and Senator Alan K. Simpson of Wyoming next to platinum records by the Grateful Dead; a list of rules headed "Principles of Adult Behavior" next to psychedelic pinwheels and an awesome-looking six-shooter. Barlow is at least as much a man of the 60's as he is of the 90's.

Barlow's grandfather, Perry Jenkins, came to Wyoming's Upper Green River Valley at the turn of the century by train and wagon from New York where he had been a teacher of mathematics at Columbia University. As soon as Jenkins arrived, he began surveying the land for what Barlow calls "the purposes of boosterism and reclamation," building dams, starting the family's Bar Cross ranch, getting himself elected to the State Senate, and eventually proposing that a new county, the size of Connecticut and Rhode Island combined, be created on the basis of the natural watersheds formed by the tributaries of the Upper Green. Sublette County, as the new jurisdiction was to be called, soon elected Jenkins to the State Senate; Barlow's father, Norman Barlow, a cattle rancher, succeeded him there.

A prototype rebel with a Honda motorcycle and a fixation on "The Wild Ones," John Perry Barlow had already had more than enough of his family's civilizing urges by the time he was 14, when he was sent to boarding school in Colorado. It was there that he met Bob Weir, who became his best friend and, much later, the rhythm guitarist for the Grateful Dead. But it wasn't until he helped lead the psychedelic revolution at Wesleyan University, where he was a poet and S.D.S. mischief-maker, that Barlow discovered what he calls "the frontier inside you." For the first time in his life, he says, "I knew who I was because I was someone on the frontier of consciousness, right on the edge of the known and peering off into the unknowable."

By the time he returned to the Bar Cross, after his father had a stroke in 1971, Barlow had already written a novel (never published), traveled around the world with what he calls "the

international useless hippie brigade," and was writing lyrics for the Grateful Dead ("Mexicali Blues," "The Music Never Stopped," "I Need a Miracle"). For the next 17 years, he tried to turn the Bar Cross from a psychedelic dude ranch into a working farm. But even though he had been raised to be a cowboy in a place where cowboys had won it all, he ultimately wound up with an Indian's perspective on the land — it would not be tamed and, despite all efforts, could not be owned by anyone, including him.

And so by 1987, heavily in debt, he tried to run for the State Senator's seat his father and grandfather had held before him; he missed getting on the ballot by a single vote. To Barlow it was a sign, and he sold the Bar Cross to return to writing, moving his wife and three children from the family homestead to a suburban ranch house in nearby Pinedale. By then, he was already in the thrall of computers, a hacker in the rye. "Compared to the cattle ranch where I was floating around on nothing but hope and baling wire for 17 years, the computer was clean," he says. "It was the one place I found I could really manipulate reality."

Eventually Barlow found himself being sucked into the vortex of telecomputing, and was invited by Apple Computer to write its history. Over the next few months, he became so frustrated with Apple's institutional politics that he shucked the project to begin a book called "Everything We Know Is Wrong," a title that could serve as his epigram for the way interpersonal computing — using the computer as a cross between the telephone and a writing machine — is radically changing the way information is understood.

Barlow has passed beyond using computers to store alphanumeric data; for him, the frontier is now in sharing images, music and texts in real time, connecting individuals in places as far-flung as Pinedale, Wyo., and Cambridge, Mass. It's a dream of a community tied together by high-tech computer power, a technological utopia.

Oddly, Barlow's fantasy of a global electronic village wasn't far from what Mitch Kapor, himself something of a 60's-90's man, had in mind. Not even Kapor's post-Lotus project, ON Technology — which boldly predicted it would reinvent the way we comprehend information and then gradually settled into a promising software company — lit Kapor's fire like Barlow's *cri de coeur* for the hacking community. Somehow it made sense that the silicon god from M.I.T. and the computer cowboy from Wyoming would end up together. For Kapor, as for Barlow, it seems only the frontier would do.

Within weeks of Kapor's visit to Wyoming, he and Barlow decided to establish the Electronic Frontier Foundation. Among their immediate aims was the protection of those hackers who had found themselves being persecuted by the Government campaign against computer crime. They were promptly offered money (from John Gilmore, an early employee of Sun Microsystems, and Steve Wozniak of Apple Computer fame), criticism and appeals for help.

One of the first people they heard from was Craig Neidorf, Phrack's publisher, who was facing charges over the publication of the 911 document. To the Government, the Neidorf case was a straightforward example of a crook republishing proprietary information — estimated by the Government to be worth $79,940 — without its authors' permission. And for this crime, it wanted a jail sentence for Neidorf suitably severe to send a message. The E.F.F. helped find an expert witness who proved that the information was not only not proprietary, but was available to the

CHUCK NACKE/PICTURE GROUP FOR THE NEW YORK TIMES

Steve Jackson, a game-book publisher, was the target of a raid by the Secret Service.

public in a booklet from another Bell system for just $13.50. On the fourth day of trial, the case was dismissed.

Then there was Steve Jackson, whose misfortune it was to have on his staff Loyd Blankenship, who was also suspected of having been involved in the publication of that 911 document. Blankenship, a cyberpunk author, had run an electronic bulletin board from his home that made Phrack available — as had perhaps thousands of others nationwide. The E.F.F. sought to unseal Jackson's search affidavit and is now about to sue the Government for violation of Steve Jackson's First and Fourth Amendment rights. After all, say the E.F.F. attorneys, if an employee of Random House was suspected of theft, would the Secret Service confiscate its computers? First and Fourth Amendment rights simply haven't been extended to the electronic media in the same way they have been to traditional print media. The E.F.F. and its chief legal advisers are beginning the long campaign to persuade state and Federal legislators that digital media are different in kind, and require different laws. (Computer Professionals for Social Responsibility, a national association based in California, has also been on the case.)

While legal defense is central to the E.F.F.'s purpose, Kapor and Barlow are the first to point out that their job is as much cultural as legal. "There's a basic conflict of paradigms," Kapor says. "This isn't just a question of the supposed criminality of hackers. There's a failure to account for these kids who have basically become exploiters of technology. The E.F.F. has to close that gap, find new ground rules for the discussion, new balances between property rights and the right to free expression."

Ultimately, the E.F.F.'s primary goal must be to create a sense of community between those they regard as legitimate computer hackers and those who believe that the Constitutional protections that

The First and Fourth Amendments, the argument goes, haven't extended to the new electronic media the protection they give to print.

currently exist for books or magazines are an anachronism in an age of infinitely reproducible, interactive digital media — an anachronism they feel is long past due for a concerted evolutionary attack. There are those in the E.F.F. who would like to spread the wealth, distributing it more evenly between the "knows" and the "know-nots," those who have been left behind by the technological revolution. Such a complicated consensus will take a great deal of time to develop, John Barlow says, but without it there will never be any way of definitively settling conflicts in the new frontier.

The Government doesn't see it that way. "Out here in the Wild West, when it was just a few settlers on the land, frontier justice had its place," says Gail Thackeray, former Assistant Attorney General of Arizona. (Sun Devil headquarters is in Phoenix.) "You could rustle up wild horses, have Saturday night shoot-'em-ups, do whatever you wanted. But as the West became more settled, there were still a few guys who wanted to go out and have shoot-'em-ups on Saturday night. But now they also wanted to shoot at the telegraph poles. And as the shooters began to attack things the community valued, the community acted to protect its rights."

As far as Thackeray is concerned, the electronic frontier is over. "The early hackers had a self-enclosed system with dumb terminals so that even if someone broke in, it wouldn't do much harm," she said. "They were working in universities where systems were deliberately left open for exploration and research. Now, computers connect to things that matter. We rely on them. People can get hurt if they're not accurate."

For John Perry Barlow, the issue of reliability is irrelevant. Computers are there to foster a sense of community. It's not a question of law, but of ethics. "For many years, nobody ever went to prison for the crime of murder in Sublette County," he explains one day after a long session of editing his electronic mail. "And that wasn't the result of no one ever getting killed. It was just the result of a couple of cultural trajectories that happened to hang together. First, nobody ever really knows the nature of another person's business; second, there really is such a thing as justifiable homicide; third, in any real community, there aren't ever any clear lines. Behavior is monitored by the community, and when somebody's stepped over the line, a consensus develops. So whenever someone died violently, they just convicted the deceased. The jury sadly shook its head, said, 'It's a pity you had to kill him, Ralph,' and Ralph said, 'Yes it is,' and walked away scot-free.

"Of course, today the only thing that's right is what you can demonstrate in court. But we're not really at that point yet in the electronic frontier. We still need to work things out. We're entering a period of great ambiguity, and we've got to take our time or else the ambiguo-phobes are going to try to make the rest of us suffer. They're going to try to draw all kinds of precise delineations where it's not possible to do that." Barlow lets out a deep sigh, and looks deep into the flickering glow of his computer. "I guess we wouldn't be doing this, if they weren't already trying." ■

Bathing Beauties

Left: The British designer Andrea de Montal took three small rooms in her East Sussex manor house and transformed them into a bathroom and dressing area. She enclosed a Victorian bathtub in old teak and used teak to frame the sink and counters. Her Victorian porcelains, each embellished with roses, decorate every surface.

Right: An early-19th-century staircase is the focal point of the fashion designer Karl Lagerfeld's bathroom in his Rome apartment. The plaster walls feature neo-classical bas relief details; the curtains are a blue and green tartan taffeta. Three late-18th-century Roman ballroom chairs, from a set of 20, are both functional and sculptural.

AS PURVEYORS OF SOCIAL HISTORY HAVE recently observed, it is the bathroom that has grown both in size and prominence in homes across America. According to Kitchen & Bath Business, a New York trade publication, Americans are expected to spend $9.5 billion on bathrooms this year alone. Call it an attempt to create spa life at home or simply a return to sybaritic pleasures, but bathrooms have attained a status once reserved for living rooms, libraries or bedrooms. "We used to decorate a whole house and the bathrooms would be an afterthought," the Manhattan designer Juan Montoya says. "Now they're a priority. Everyone wants a beautiful bathroom."

Beauty, however, comes in many guises. Indeed, the bathrooms on these pages span all tastes, styles and budgets. The most popular look is the decorated bathroom — a space bedecked with artwork and wallpaper, antiques and painted surfaces. "Since we all spend so much time in bathrooms, they should be pretty," says the veteran New York decorator Sister Parish. "I've treated mine as a visual extension of the bedroom." Architects often have a decidedly different esthetic. Many create purposely pristine, cold spaces that seem almost too frosty to bathe in. One iconoclastic architect, for example, doesn't deign to speak of bathrooms. Instead, he christens them "wet rooms." — CAROL VOGEL

PHOTOGRAPHS BY FRITZ VON DER SCHULENBURG FOR THE NEW YORK TIMES

EFFECTOR

Effector – The Newsletter of the Electronic Frontier Foundation

March 1991
Volume 1 Number 1

Goals of the EFF

1. To engage in and support educational activities that increase the popular understanding of the opportunities and challenges posed by computing and telecommunications.

2. To develop among policy-makers a clearer comprehension of the issues underlying free and open telecommunications.

3. To support the creation of legal and structural approaches which will ease the assimilation of these new technologies by society.

4. To raise public awareness about civil-liberties issues arising from rapid advances in computer-based communications media.

5. To support litigation in the public interest to preserve, protect, and extend Constitutional rights to the realm of computing and telecommunications technology.

6. To encourage and support the development of new tools which will endow non-technical users with full and easy access to computer-based telecommunications.

A Man From the FBI:

The Origins of the Electronic Frontier Foundation

By John Perry Barlow

The Electronic Frontier Foundation was started by a visit from the FBI.

In late April of 1990, I got a call from Special Agent Richard Baxter of the Federal Bureau of Investigation. He asked if he could come by the next day and discuss a certain investigation with me. His unwillingness to discuss its nature over the phone left me with a sense of global guilt, but I figured turning him down would probably send the wrong signal.

On Mayday, he drove to Pinedale, Wyoming, a cow town 100 miles north of his Rock Springs office (where he ordinarily investigates livestock theft and other regional crimes). He brought with him a thick stack of documents from the San Francisco office and a profound confusion about their contents.

He had been sent to find out if I might be a member of the NuPrometheus League, a dread band of info-terrorists (or maybe just a disaffected former Apple employee) who had stolen and wantonly distributed source code normally used in the Macintosh ROMs. Agent Baxter's errand was complicated by a fairly complete unfamiliarity with computer technology. I realized right away that before I could demonstrate my innocence, I would first have to explain to him what guilt might be.

The three hours I passed doing this were surreal for both of us. Whatever this source code stuff was, and whatever it was that happened to it, had none of the cozy familiarity of a few yearling steers headed across the Wyoming border in the wrong stock truck.

What little he did know, thanks to the San Francisco office, was also pretty well out of kilter. He had been told, for example, that Autodesk, the publisher of AutoCAD, was a major Star Wars defense contractor and that its CEO was none other than John Draper, the infamous phone phreak also known as Cap'n Crunch. As soon as I quit laughing, I started to worry.

I realized in the course of this interview that I was seeing, in microcosm, the entire law enforcement structure of the United States. Agent Baxter was hardly alone in his puzzlement about the legal, technical, and metaphorical nature of datacrime.

I also found in his struggles a framework for understanding a series of recent Secret Service raids on some young hackers I'd met in a Harper's magazine forum on computers and freedom. And it occurred to me that this might be the beginning of a great paroxysm of governmental confusion during which everyone's liberties would become at risk.

When Agent Baxter had gone, I wrote an account of his visit and placed it on the WELL, a computer BBS in Sausalito which is digital home to a large collection of technically hip folks, including Mitch Kapor, the father of Lotus 1-2-3.

Turns out Mitch had also been visited by the FBI, owing to his having unaccountably received of one of the source code disks which NuPrometheus scattered around. Mitch's experience had been as dreamlike as mine. He had, in fact, filed the whole thing under General Inexplicability until he read my tale on the WELL. Now he had enough corroboration for his own strange sense of alarm to begin acting on it.

Several days later, he found his bizjet about to fly over Wyoming on its way to San Francisco. He called me from somewhere over South Dakota and asked if he might literally drop in for a chat about Agent Baxter and related matters.

So, while a late spring snow storm swirled outside my office, we spent several hours hatching what became the Electronic Frontier Foundation. I told him about the sweep of Secret Service raids that had taken place months before and their apparent disregard for the Bill of Rights.

Alarmed, he gave me the phone number of Harvey Silverglate, whose willingness to champion unpopular causes was demonstrated by his current defense of Leona Helmsley. He said that Harvey would probably know if this were as bad as it was starting to sound. He also said that he would be willing to pay the bills that generally start to appear whenever you call a lawyer.

I finally found Harvey in the New York offices of Rabinowitz, Boudin, Standard, Krinsky and Lieberman, a firm whose long list of successfully defended civil-liberties cases includes the Pentagon Papers case. I told him and Eric Lieberman what I knew about recent government flailings against cybercrime. They were even less sanguine than I had been.

The next day a trio code-named Acid Phreak, Phiber Optik, and Scorpion entered the walnut-panelled chambers of Rabinowitz, Boudin and told their tales to a lawyer there named Terry Gross. While EFF as a formal organization would not exist for two months, its legal arm was already flexing its muscle.

A few days later I received a phone call from the technology writer for the Washington Post. He was interested in following up on the Harper's forum, and knew nothing of Mitch's and my joint endeavors. I filled him in, hoping to expose the Secret Service. Several days later, the Post published the first of many newspaper stories, all of which could have shared the headline: "Lotus Founder Defends Hackers."

continued page 2

Why Defend Hackers?

By Mitchell Kapor

An all-too-common perception of the EFF that prevails in the computer industry and those who report on it—from John Sculley to the Wall Street Journal—is that the EFF is an organization that has "something to do with hackers." (They use "hackers" as a term not of approbation but of rebuke). Most of these sometime colleagues and associates of mine are puzzled as to why I would be doing such a thing. (A few think I've just become a loony.) Anyway, they've heard about the terrible problems caused by hackers who break into computer systems, they worry that I'm out to defend such practices, and they disapprove.

But their disapproval is based on the pure misconception that the EFF's purpose is to defend people's right to break into computer systems. Let me clear up that misconception now.

I regard unauthorized entry into computer systems as wrong and deserving of punishment. People who break into computer systems and cause harm should be held accountable for their actions. We need to make appropriate distinctions in the legal code among various forms of computer crime, based on such factors as intent and the degree of actual damage. In fact, the EFF has drafted a bill that has the backing

continued page 3

Washington Watch

by Marc Rotenberg

• *Computer Crime Legislation*

Several proposals to expand computer crime law were introduced in the past Congress. In the end, a modest proposal, introduced by Senator Leahy, passed the Senate but did not make it through the House. Senator Leahy's bill would have penalized reckless computer acts that place computer systems at risk and would have required that the Justice Department report annually to Congress on computer crime prosecutions

• *National ID Card*

A proposal to begin a national ID card pilot project, tucked into amendments to the Immigration Control and Reform Act, was knocked out when civil libertarians objected.

• *Electronic Dissemination Policy*

A proposal to establish principles for the dissemination of electronic information by the federal agencies narrowly failed to pass the Congress as last minute negotiations on a related measure collapsed. The proposal grows out of a report from the Office of Technology Assessment "Informing the Nation" that stressed the need to develop new information policy to promote the development of CD-ROMs and on-line information services.

• *Caller ID*

A bill to allow the offering of Caller ID by regional phone companies if a per-call blocking feature is also provided failed to gather support this past Congress. Several states have already adopted similar measures.

• *Computer Security Policy*

The Presidential directive on computer security policy was revised finally to comply with the Computer Security Act of 1987. The Act reestablished control for computer security at a civilian agency — the National Institute for Standards and Technology — after the previous administration attempted to place computer security authority at the National Security Agency.

• *Upcoming Policy*

CPSR hosted the first Computing and Civil Liberties policy roundtable on February 21 and 22, 1991 at the American Association for the Advancement of Science in Washington, DC. The purpose of the roundtable was to bring together leading experts to explore two issues: free speech and computer networks, and searches of computer bulletin boards. What speech restrictions currently exist? Should federal agencies or private companies be allowed to restrict the content of a computer message and, if so, in what circumstances? The second issue was the investigation of computer bulletin boards by law enforcement agents. Are there any restrictions on the ways that police may monitor computer communications and computer bulletin boards? If not, should such restrictions be developed? The conference was the first in a series of policy roundtables that will be held in Washington, DC and that are made possible with funding from the Electronic Frontier Foundation.

EFFECTOR

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

The Board of the Electronic Frontier Foundation:
Mitchell Kapor, John Barlow, John Gilmore, Stewart Brand, Steve Wozniak
Staff Counsel: Mike Godwin
Staff Volunteer: Leila Gallagher

EFFECTOR was edited and produced by Gerard Van der Leun

Art Direction and design by Lisa DeFrancis, DeFrancis Studio, 80 Trowbridge Street, Cambridge, MA 02138

FBI *continued*

While this was an irritating misrepresentation, we were more interested in defending the Constitution than digital miscreants, the publicity produced a couple of major supporters: Steve Wozniak, who called and offered an unlimited match to Mitch's contributions, and John Gilmore (Sun Microsystems employee #5) who e-mailed me a six figure offer of support.

Operation Sundevil

Meanwhile, the list of apparent outrages lengthened. We learned about an Austin role-playing games publisher named Steve Jackson whose office equipment had been confiscated by the Secret Service in an apparent effort to restrain his publication of a game called Cyberpunk which they thought, with ludicrous inaccuracy, to be "a handbook for computer crime."

All over the country computer bulletin boards were being confiscated, undelivered e-mail and all. A Secret Service dragnet called Operation Sundevil seized more than 40 computers and 23,000 data disks from teenagers in 14 American cities, using levels of force and terror which would have been more appropriate to the apprehension of urban guerrillas than barely post-pubescent computer nerds.

And there was the Craig Neidorf case. Neidorf, also known by the nom de crack Knight Lightning, had published an internal BellSouth document in his electronic magazine Phrack. For this constitutionally protected act, Neidorf was being charged with interstate transport of stolen property with a possible sentence of 60 years in jail and a $122,000 in fines.

I wrote a piece about these events called "Crime & Puzzlement." I did so at the request of the Whole Earth Review—it made its first print appearance in the Fall 1990 issue of WER—but I "published" it on the Net in June and was astonished by the response. It was like planting a fence-post and discovering that the ground into which you've driven it is actually the back of a giant animal that quivers and heaves at the irritation.

By July, I was receiving up to 100 e-mail messages a day. They came from all over the planet and expressed nearly universal indignation. I began to experience datashock, but I also realized that Mitch and I were not alone in our concerns. We had struck a chord.

The Law in Cyberspace

In Cambridge, Mitch was having something like the same experience. Since the Washington Post story, he found himself bathed in media glare. However, the more he learned about ambiguous nature of law in Cyberspace, the more of his considerable intellectual and financial resources he became willing to devote to the subject.

In late June, Mitch and I threw several dinners in San Francisco, to which we invited major figures from the computer industry. We weren't surprised to learn than many of them had exploits in their past which, undertaken today, would arouse plenty of Secret Service interest. It appeared possible that one side-effect of current government practices might be the elimination of the next generation of computer entrepreneurs and digital designers.

It also became clear that we were dealing with a set of problems which was a great deal more complex and far-reaching than a few cases of governmental confusion. The actions of the FBI and Secret Service were symptoms of a growing social crisis: Future Shock. America was entering the Information Age with neither laws nor metaphors for the appropriate protection and conveyance of information itself.

We realized that our legal actions on behalf of a few teen-age crackers would go on indefinitely without much result unless something were done to ease social tensions along the electronic frontier. The real task at hand was the civilization of Cyberspace. Such an undertaking would require more juice and stamina than two men could muster, even amplified by the Net and a solid financial supply. We would need some kind of organizational identity.

With this in mind, we hired a press coordinator, Cathy Cook (who had formerly done PR for Steve Jobs), set a squad of lawyers to work on investigating the proper organizational tax status, and, over a San Francisco dinner with Stewart Brand, Nat Goldhaber, Jaron Lanier, and Chuck Blanchard, we selected a name and defined a mission.

Founding the Foundation

We announced the formation of the Electronic Frontier Foundation at the National Press Club on July 10. Mitch and I were joined for the announcement by Harvey Silverglate, Terry Gross, and Steve Jackson.

We were also joined by Marc Rotenberg of the Washington office of Computer Professionals for Social Responsibility. One of our first official acts had been to grant that organization $275,000 for a project on computing and civil liberties. CPSR would keep a wary eye on developments "inside the Beltway" and work in conjunction with congressional staffers to see that any legislation dealing with access to information was sensibly drafted.

While in Washington, we also took inventory of the terrain, meeting with congressional staffers, the Washington civil liberties establishment, and officials from the Library of Congress and the White House. The area to be covered, from intellectual property to telecommunications policy to law enforcement technique, was daunting, as were the ambient levels of confusion and indifference.

We also generated an enormous amount of press. And it became apparent that not everyone was persuaded of our cause. Business Week called Mitch naive for his willingness to believe that computer crackers were somehow less dangerous that drug kingpins. Various burghers of the computer establishment, ranging from the executive director of the Software Publishers Association to a columnist for ComputerWorld, called us fools at best and, more likely, dangerous fools.

The Wall Street Journal printed a particularly hysterical piece which alleged that the document Craig Neidorf (into whose case we had entered a supporting amicus brief) had published was a computer virus capable of bringing down the emergency phone system for the entire country. In fact, the text file which Neidorf distributed dealt with the bureaucratic procedures of 911 administration in the Bell-South region and contained nothing which could be used to crack a system. Indeed, it contained nothing which could not be easily obtained through by legal means.

Neidorf's first major break came in late July. Thanks in part to the independent work of John Nagel, who was prepared to testify that the prosecutors had seriously overstated the value of the E911 document, the government was forced to abandon its case against Neidorf after 4 days in Chicago's Federal Court.

Although our briefs supporting Neidorf's activities under the First Amendment were not admitted, it became apparent, before such loftier matters could even be broached, that the government had indicted him with no clear understanding of the purpose or availability of the document he had distributed. Like Agent Baxter, they knew too little to critically examine the misinformation they had been given by the corporate masters, in this case, officials at Bellcore.

Following the resolution of the Neidorf case, and, to some extent because of it, skepticism of EFF has moderated considerably. If anything, the most recent press accounts of our activities have been almost fulsome in their praise. Recent favorable coverage has appeared in the New York Times, The Economist, Infoworld, Information Week, PCweek, and Boston Magazine.

Since July, we have been absurdly busy on numerous fronts: We've worked on raising public awareness of the issues at stake. We are organizing legal responses to the original and continuing intemperance of law enforcement. We have worked on the political front, developing and lobbying for rational computer security legislation. We have started to create a network of interested experts on computer security, intellectual property, telecommunications policy, and international information rights. And lately we've been attending to the organizational demands of the non-profit equivalent of a hyper-successful computer startup.

The Expanding Mission

When we first defined the mission of the Electronic Frontier Foundation, we saw our task as assuring the application of the U.S. Constitution to digital media. And this remains much of what we are about.

However, information has little natural regard for national borders or local ordinances. Cyberspace is transnational. During the tsunami of e-mail which Crime & Puzzlement elicited, there were many items from foreign countries. Their authors wanted to know how they could protect or establish their rights of free expression. And I had no idea what to tell them.

The question arose again at Esther Dyson's recent East-West Technology Conference in Budapest which Mitch and I attended. EFF was well-known among the Soviets at this meeting, some of whom were already involved in drafting what they called an Information Bill of Rights. (One young Moscow programmer had managed to hack together an Internet connection through Finland in order to contact me.)

Like intellectual property and telecom policy, the development of international principles of free digital speech is a large angel to wrestle with. We will have to be careful not to allow this immense task to divert EFF from its specific legal agenda. But neither can we ignore the fact that Cyberspace is hardly an American territory.

The Electronic Frontier Foundation grew from an effort to fight a specific legal brushfire into a full-fledged Cause much faster than we could have imagined. And, like any explosive start-up, it spends a lot of time playing catch-up.

Reaching Out

Electronically amplified, Mitch and I were able to personally conduct much of EFF's business in the first few months of operations. But gradually we had to confront the fact that while the Net is very broad, it is also quite shallow. Without even a sense of their physical location, we have been unable to marshal the hundreds of people who have e-mailed us with their volunteered services. Also, we found ourselves administering a significant cash-flow in both donations and expenditures. (By year's end, EFF will have spent around $220,000. Our tentative 1991 budget predicts expenses of almost half a million.)

So, despite a mutual terror of bureaucracy and organizational sclerosis, we have started to adopt some institutional trappings.

First, in order to satisfy the requirements for a 501c3 tax status (which we should have in about six months), we found that we needed something more substantial than two guys with modems. Thus, on October 9, we held our first official board meeting and formally elected Stewart Brand, Steve Wozniak, and John Gilmore to join us as board members.

And we have started to take on staff. We recently hired Mike Godwin, a freshly minted Texas lawyer and USENET adept, to sort through the factual and legal details of the many cases we are being asked to intervene in. In his short time with us, he has investigated several cases to determine their fit with EFF's constitutional mission, their winnability, and their likelihood of producing clear legal precedent.

We are determined that EFF will remain an agile, swift-moving sort of outfit. We will adopt any new bureaucratic manifestations with the greatest skepticism. But we are being bombarded with many legitimate requests for assistance, advice, and information. In order to respond rapidly and appropriately, the Electronic Frontier Foundation has had to become an institution. One method by which we hope to maintain organizational lightness involves keeping a clear distinction between strategy and tactics.

On the strategic level, EFF has a very broad mission involving such amorphous endeavors as defining intellectual property, helping establish a transnational culture of information, designing telecommunications policy, sponsoring humane software design... civilizing Cyberspace. With an appropriate sense of their limitations, the board members will remain responsible for these matters.

This will prevent the staff's losing tactical focus on more tangible action items like litigation, political action, communicating through the press and across the Net, and organizational care and feeding.

The problem with history is that it keeps happening. Today, as I was working on this EFF mini-biography, I learned that Mitch has just had his fingerprints subpoenaed by the FBI. Turns out they are now examining the NuPrometheus distribution disks for fingerprints and want to be able to sort his out. Or, perhaps, search for their appearance on other disks...

So the Wheels of Justice grind blindly on. And we will go on trying to prevent anyone's being ground up in them.

Postcard from the Edge

"I went on to test the program in every way I could devise. I strained it to expose its weaknesses. I ran it for high-mass stars and low-mass stars, for stars born exceedingly hot and those born relatively cold. I ran it assuming the superfluid currents beneath the crust to be absent — not because I wanted to know the answer, but because I had developed an intuitive feel for the answer in this particular case. Finally I got a run in which the computer showed the pulsar's temperature to be less than absolute zero. I had found an error. I chased down the error and fixed it. Now I had improved the program to the point where it would not run at all."

George Greenstein,
"Frozen Star: Of Pulsars, Black Holes and the Fate of Stars"

How Prosecutors Misrepresented the Atlanta Hackers

Reading Between the Lines of the BellSouth Sentences

By Mike Godwin

Although the Electronic Frontier Foundation is opposed to unauthorized computer entry, we are deeply disturbed by the recent sentencing of Bell South hackers/crackers Riggs, Darden, and Grant. Not only are the sentences disproportionate to the nature of the offenses these young men committed, but, to the extent the judge's sentence was based on the prosecution's sentencing memorandum, it relied on a document filled with misrepresentations.

Robert J. Riggs, Franklin E. Darden, Jr., and Adam E. Grant were sentenced Friday, November 16, in federal court in Atlanta. Darden and Riggs had each pled guilty to a conspiracy to commit computer fraud, wire fraud, access-code fraud, and interstate transportation of stolen property. Grant had pled guilty to a separate count of possession of access codes with intent to defraud.

All received prison terms; Grant and Darden, according to a Department of Justice news release, "each received a sentence of 14 months incarceration (7 in a halfway house) with restitution payments of $233,000." Riggs, said the release, "received a sentence of 21 months incarceration and $233,000 in restitution." In addition, each is forbidden to use a computer, except insofar as such use may be related to employment, during his post-incarceration supervision.

The facts of the case, as related by the prosecution in its sentencing memorandum, indicate that the defendants gained free telephone service and unauthorized access to BellSouth computers, primarily in order to gain knowledge about the phone system. Damage to the systems was either minimal or nonexistent. Although it is well-documented that the typical motivation of phone-system hackers is curiosity and the desire to master complex systems, the prosecution attempts to characterize the crackers as major criminals, and misrepresents facts in doing so.

Examples of such misrepresentation include:

1. Misrepresenting the E911 file.

The E911 file, an administrative document, was copied by Robert Riggs and eventually published by Craig Neidorf in the electronic magazine PHRACK. Says the prosecution: "This file, which is the subject of the Chicago [Craig Neidorf] indictment, is noteworthy because it contains the program for the emergency 911 dialing system. As the Court knows, any damage to that very sensitive system could result in a dangerous breakdown in police, fire, and ambulance services. The evidence indicates that Riggs stole the E911 program from BellSouth's centralized automation system (i.e., free run of the system). Bob Kibler of BellSouth Security estimates the value of the E911 file, based on R&D costs, is $24,639.05."

This statement by prosecutors is clearly false. Defense witnesses in the Neidorf case were prepared to testify that the E911 document was not a program, that it could not be used to disrupt 911 service, and that the same information could be ordered from Bell South at a cost of less than $20. Under cross-examination, the prosecution's own witnesses admitted that the information in the E911 file was available in public documents, that the notice placed on the document stating that it was proprietary was placed on all Bell South documents (without any prior review to determine whether the notice was proper), and that the document did not pose a danger to the functioning of the 911 system.

2. Guilt by association.

The prosecution begins its memorandum by detailing two crimes: 1) a plot to plant "logic bombs" that would disrupt phone service in several states, and 2) a prank involving the rerouting of calls from a probation office in Florida to "a New York Dial-A-Porn number."

Only after going to some length describing these two allegations does the prosecution state, in passing, that *the defendants were not implicated in these crimes.*

Elsewhere in the memorandum, the prosecution attempts to suggest the defendants' responsibility in a third offense—another person's crime. Because the defendants "freely and recklessly disseminated access information they had stolen," says the memorandum, a 15-year-old hacker committed $10,000 in electronic theft. Even though the prosecution does not say the defendants intended to facilitate that 15-year-old's alleged theft, the memorandum seeks to implicate the defendants in that theft.

3. Guilt by knowing too much.

The prosecution goes to great lengths describing the crimes the defendants *could* have committed with the kind of knowledge they had gathered: "During the course of the conspiracy, the defendants and other LOD [Legion of Doom] members illegally amassed enough knowledge about the telecommunications computer systems to jeopardize the entire telephone industry!"

The prosecution does not mention, however, that the mere possession of dangerous knowledge is not a crime, nor does it state, explicitly, that the defendants never conspired to cause such damage to the phone system.

4. Misrepresentation of motives.

As noted above, it has been documented that young phone-system hackers are typically motivated by the desire to understand and master large systems, not to inflict harm or to enrich themselves materially. Although the prosecution concedes that "[d]efendants claimed that they never personally profited from their hacking activities, with the exception of getting unauthorized long distance and data network service," the prosecutors nevertheless characterize the hackers' motives as similar to those of extortionists: "Their main motivation [was to] obtain power through information and intimidation."

5. Failure to acknowledge the outcome of the Craig Neidorf case.

In evaluating defendants' cooperation in the prosecution of Craig Neidorf, the government singles out Riggs as being less helpful than the other two defendants, and recommends less leniency because of this. Says the memorandum: "The testimony was somewhat helpful, though the prosecutors felt defendant Riggs was holding back and not being as open as he had been in the earlier meeting." The memorandum fails to mention, however, that Riggs's testimony tended to support Neidorf's defense that he had never conspired with Riggs to engage in the interstate transportation of stolen property or that the case against Neidorf was dropped.

Perhaps the most egregious aspect of the governments's memorandum is the argument that Riggs, Grant, and Darden should be imprisoned, not for what *they* have done, but to send the right "message to the hacking community." The government focuses on the case of Robert J. Morris Jr., the computer-science graduate student who was sentenced to a term of probation in May of this year for his release of the worm program that disrupted many computers connected to the Internet. Urging the court to imprison the three defendants, the government remarked that "hackers and computer experts recall general hacker jubilation when the judge imposed a probated sentence. Clearly, the sentence had little effect on defendants Grant, Riggs, and Darden."

The government's criticism is particularly unfair in light of the fact that the Morris sentencing took place almost a year *after* the activities leading to the defendants' convictions!

The memorandum raises other questions besides those of the prosecutors' biased presentation of the facts. The most significant of these is the government's uncritical acceptance of BellSouth's statement of the damage the defendants did to its computer system. The memorandum states that "In all, [the defendants] stole approximately $233,880 worth of logins/passwords and connect addresses (i.e., access information) from BellSouth. BellSouth spent approximately $1.5 million in identifying the intruders into their system and has since then spent roughly $3 million more to further secure their network."

It is unclear how these figures were derived. For one thing, the stated cost of the passwords is highly questionable: What is the dollar value of a password?

And it's similarly unclear that the defendants caused BellSouth to spend $4.5 million more than they normally would have spent in a similar period to identify intruders and secure their network. Although the government's memorandum states that "[t]he defendants ... have literally caused BellSouth millions of dollars in expenses by their actions," the actual facts as presented in the memorandum suggest that BellSouth had already embarked upon the expenditure of millions of dollars *before* it had heard anything about the crimes the defendants ultimately were alleged to have committed.

Not only are there questions about the justice of the restitution requirement in the sentencing of Riggs, Darden, and Grant, but there also are Constitutional issues raised by the prohibition of access to computers. The Court's sentencing suggests a belief that anything the defendants do with computers is likely to be illegal; it ignores the fact that computers are a communications medium, and that the prohibition goes beyond preventing future crimes by the defendants—it treads upon their rights to engage in lawful speech and association.

EFF does not support the proposition that computer intrusion and long-distance theft should go unpunished. But we find highly disturbing the misrepresentations of facts in the prosecutors' sentencing memorandum as they seek disproportionate sentences for Riggs, Darden, and Grant—stiff sentences that supposedly will "send a message" to the hackers and crackers.

The message this memorandum really sends is that the government's presentation of the facts of this case has been heavily biased by its eagerness to appear to be deterring future computer crime.

Why Defend Hackers *continued*

of the Governor and Attorney General of Massachusetts and that embodies these principles.

But if the EFF isn't trying to advance the cause of computer hackers, you may ask, what is it doing and why? What is it that was sufficiently powerful to motivate me to help start a whole organization?

As I began to find out the real story behind government raids and indictments last summer, I became incensed at the fact that innocent individuals were getting caught up in the blundering machinations of certain law enforcement agencies and large corporations. These were kids really, young people with whom I identified, who faced the prospect of having their lives ruined.

Take Craig Neidorf for example. Neidorf, a defendant in one case and the publisher of an electronic newsletter, was indicted on felony charges of wire fraud and interstate transportation of stolen property. Neidorf had published a document about administrative procedures used in the 911 emergency response telephone system that someone else had removed from a BellSouth computer. On the fourth day of the trial, the prosecution dropped the case after it became clear that the information in the "highly confidential" BellSouth document at issue was publicly available for less than $20.

Justice was served by the government's decision to drop the case, but it was expensive justice. Neidorf and his family face $100,000 in legal bills, to say nothing of the disruption and suffering caused by the trial for an action that should never have been brought against him to begin with.

In a second case, the EFF continues to assist Steve Jackson, a game manufacturer in Austin, Texas, who has suffered substantial business losses after a Secret Service raid in early March. The seizure of Jackson's computer equipment caused him to lay off nearly half of his staff and threatened the survival of the business. As subsequent revelations have showed, there was no good reason for this raid. It never should have been permitted to occur in the first place.

While helping defend the innocent is one role for the EFF to play, there is more at stake than trying to prevent individuals from being wronged. It is also a matter of rights for all of us.

The legal protections afforded Craig Neidorf's electronic newsletter and its publisher and the computer bulletin board system (BBS) seized in the Steve Jackson raid are neither clear nor well-established. I believe it is terribly important to extend to these new digital media the same strong First Amendment protections of freedom of speech and freedom of expression which we enjoy in our own lives and in the print media. The government should not be able to seize a BBS any more easily than they can seize a printing press. We must find ways for law enforcement to do its job in protecting the property of some of us without violating the freedom of speech of the rest of us. This is clearly a matter of protecting civil liberties and familiar to those who take an interest in upholding the Bill of Rights, but it is also more than that.

These embryonic media of electronic mail, BBSs, and conferencing systems, provide open forums of communication. They are an antidote to the corrosive effects of the power of large, centralized institutions, private and public, and to the numbness induced by one-way, least-common-denominator mass media.

In the global suburbs in which more and more of us live, one's horizon is limited to the immediate family. Even close neighbors are often anonymous.

In the realities that can be created within digital media there are opportunities for the formation of virtual communities—voluntary groups who come together not on the basis of geographical proximity but through a common interests. Computer and telecommunications systems represent an enabling technology for the formation of community, but only if we make it so. I believe it is urgent, as a matter of national policy, that we encourage and further stimulate the social experiments and developing infrastructure that are taking place on the Net every day. The ultimate mission of the EFF is to help articulate this vision and play a constructive role in the working out of the new legal and social norms which we are faced with developing.

As John Barlow and I meditated together last June on the broader implications of the initial events—a meditation that catalyzed the formation of the EFF—we could see that what was at stake was not merely seeing justice be served in the case of a few individuals, nor simply the preservation of the civil liberties of all of us, although these goals are vitally important.

The larger issue is how our society will come to terms with the onrush of transformative technology. If we take the right steps now—and EFF is working to take those steps—new and increasing access to information technology will enhance rather than inhibit the positive growth and development of individuals, of communities, and of society as a whole.

---

20 Things You Can Do to Advance Electronic Freedom

1. **Spread the word about EFF as widely as possible, both on and off the Net.**
2. **Be alert for any local, state or national legislation that effect electronic freedom.**
3. **Put the immense processing horsepower of your mind to the task of finding new metaphors for the realities of the physical world which seem up for grabs in these less tangible regions.**
4. **Try to communicate to technically unsophisticated friends the extent to which their future freedoms depends on understanding digital communication.**
5. **If you are online, spread the word to local boards.**
6. **If you are at a school, inform interested people about the goals of the EFF.**
7. **Connect responsibly.**
8. **Work locally for an understanding of what the electronic frontier means in a global sense.**
9. **Learn and use the technology. Only by having an understanding of computers can one evaluate statements about computer crime.**
10. **Stop and think, about the many ways in which we rely on information in our lives, and what the effect might be if that information were distorted, corrupted, limited, or denied us.**
11. **Remember that words on a computer are SPEECH, protected by the Constitution.**
12. **Help your non-computerized friends see the potential of the net: search out a low airline fare for them, or send a fast cheap message to friends across the country.**
13. **Check to see if your local and state representatives understand the potential of electronic communication.**
14. **Reject techno-elitism and recognize that entry into the networking domain is a rite of passage and that someone else probably helped you with it.**
15. **Do your backups.**
16. **Educate your local librarians about electronic freedoms.**
17. **Welcome all interested participants.**
18. **Argue in a way that informs a the participants in the argument.**
19. **Develop better tools for linkin people and networks.**
20. **Keep in touch with us. Pass o your thoughts, concerns, insight contacts, and news.**

CPSR Announces the First Conference on Computers, Freedom & Privacy

Tutorials & Invitational Conference, Limited to 600 Participants

About Computers, Freedom & Privacy —
We are at a crossroads, as individuals and organizations conduct more and more of their activity using computers and computer networks. By the end of the 1990s, most information will be collected, distributed and utilized electronically.

Thus far, an uncoordinated jumble of policies and procedures is rapidly developing as each group develops ways of collecting, manipulating, extracting, sharing and protecting information in its computers and exchanged on its networks.

Information on individuals and groups is being computerized by numerous organizations, agencies and special interests, often without the knowledge or approval of those it concerns.

Computerization can greatly assist individuals, organizations and government in making sound decisions based on efficient access to adequate information.

Or, it can seriously threaten the fundamental freedoms, personal privacy, and democratic processes that are at the very foundation of this nation.

More and more people are concerned about how organizations handle personal, family and lifestyle information about individuals. Many feel powerless to prevent private organizations and government from building, marketing and distributing confidential dossiers on them. Valuable information about government is increasingly computerized in government systems, but freedom of access to it in useful, computerized form by interested citizens, researchers and the press remains difficult and often prohibited.

Governments' regulation of national and international information exchange is increasing, often restricting it in the name of protecting competitiveness or confidentiality. There are increasing protests from business leaders unable to conduct effective business in a global economy.

Businesses are losing millions of dollars and thousands of work-hours, annually, to computerized mischief, vandalism, fraud and theft. Perpetrators are usually individuals abusing their authorized access.

Instances of computer misuse by young people raise special questions about the values that adults are practicing and passing along to these children.

Each year, new laws are proposed responding to the latest type of abuse or misuse of computers. Penalties applied to uncharged suspects and convicted computer criminals vary wildly from case to case, with little consistency relative to the seriousness of the alleged crime.

Law enforcement officials are using increasingly aggressive strategies and sophisticated countermeasures as they seek to serve and protect, vigorously applauded by some interest groups and increasingly criticized by others.

Diverse groups are often polarizing around narrow self-interests, rather than working together to assure responsible practices and equitable policies.

About this Conference —
This is an intensive, multi-disciplinary survey Conference for those concerned with computing, teleconferencing, electronic mail, computerized personal information, direct marketing information and government data — and those concerned with computer-related legislation, regulation, law enforcement and international policies that impact civil liberties, responsible exercise of freedom and protection of privacy in the global Information Age.

A maximum of 600 applicants will be invited to attend. Balanced representation from the diverse interest groups is being encouraged.

To inform participants about topics beyond their specialties, half-day and full-day seminars are scheduled for the first day (Monday, Mar. 25th). These parallel tutorials will explore relevant issues in computing, networking, civil liberties, the law and law enforcement. Each seminar is designed for those who are experienced in one area, but are less knowledgeable in some of the other disciplines.

To explore the issues and their interactions and ramifications, conference talks and panel discussions are scheduled for the remaining three days (Tuesday-Thursday, Mar. 26th-28th). These will emphasize balanced representation of all major views, with ample opportunity for probing questions and discussion.

The opening conference session on Tuesday will include major policy proposals by one of the nation's best known Constitutional scholars: Laurence H. Tribe, Professor of Constitutional Law, Harvard University Law School: "The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier"

The Tuesday evening session will feature a leading expert in the areas of telecommunications regulation, international telecomm policies and economics: Professor Eli M. Noam, Professor & Director Center for Telecommunications and Information Studies, Columbia University Graduate School of Business

Tuesday-Thursday Conference sessions offering diverse speakers & panel discussions include:

- Computers & Network Trends
- Personal Information & Privacy
- International Perspectives & Impacts
- Law Enforcement Practices & Problems
- Law Enforcement & Civil Liberties
- Legislation & Regulation
- Computer-Based Surveillance of Individuals
- Ethics & Education
- Electronic Speech, Press, & Assembly
- Access to Government Information
- Where Do We Go From Here?

The conference is sponsored by Computer Professionals for Social Responsibility –A nonprofit educational corporation. Telephone: (415)322-3778 Fax: (415) 851-2814 Conference e-mail: cfp@well.sf.ca.us

Co-sponsors & cooperating organizations include: Electronic Frontier Foundation, Electronic Networking Association Association for Computing Machinery, American Civil Liberties Union, ACM Special Interest Group on Software, Videotex Industry Association, IEEE-USA Intellectual Property Committee Cato Institute, IEEE-USA Committee on Communications and Information Policy, Institute of Electrical and Electronics Engineers-USA, ACM Committee on Scientific Freedom and Human Rights, ACM Special Interest Group on Computers and Society, The WELL, Autodesk, Inc., Portal Communications. ⇨

March 25-28, 1991, Monday-Thursday in the Bicentennial Year of the Bill of Rights

Airport Marriott Hotel, Burlingame, California on the San Francisco Peninsula, near San Francisco International Airport

Sponsored by: Computer Professionals for Social Responsibility –A nonprofit educational corporation

Chair: Jim Warren, Autodesk & MicroTimes, fax/415-851-2814, e-mail/jwarren@well.sf.ca.us

Request for Invitation
To facilitate useful dialogue and balanced participation by representatives from all of the diverse groups that are interested in these issues, this First Conference on Computers Freedom & Privacy (March 25-28, 1991) is limited to 600 invited participants (Conference facility capacity is also limited). All interested parties are encouraged to apply for an invitation. To receive information about the 50-60 speakers & panelists, the tutorials and an invitation Application form, forward the following information to: e-mail/cfp@well.sf.ca.us -or- fax/(415)851-2814 -or- CFP Conference, 345 Swett Road, Woodside CA 94062

Name:
Title (if any):
Organization (if any):
Mailing address:
City/state/ZIP:
Phone number:
Alternate phone (if any):
Fax number (if any):
Electronic-mail address (if any):
Your particular interests (maximum of one page, please):

Plans and Actions:

Current EFF Activities

The Len Rose cases
The EFF legal department has been working to provide litigation support in the two criminal cases involving Baltimore computer consultant Len Rose. In the first case, we have been particularly active in helping develop the factual and legal issues in the case, and in locating and screening potential witnesses. We believe Baltimore case raises important issues concerning both the application of the federal Computer Fraud and Abuse statute (which we have challenged on the basis of unconstitutional overbreadth), the federal wire-fraud statute, and the federal Interstate Transportation of Stolen Property statute (which we believe should not be applied in cases of unauthorized copying of copyrighted software).

We have been providing similar support in Rose's state criminal case in Illinois. Among the issues in that case is whether the Illinois "computer tampering" statute is overbroad, and whether it in fact criminalizes the activity that Rose is alleged to have committed. In both cases, we have relied extensively on communications over the Net to initiate and maintain contact with potential witnesses.

The RIPCO BBS case
We have also been giving significant time to reviewing the warrant affidavits in the RIPCO BBS seizure. In addition, we have been reviewing the available archived files from that BBS to determine what, if any, justification there was for seizing the equipment.

We believe the RIPCO case potentially raises important issues about the valid scope of searches and seizures, the chilling effect of such seizures on First Amendment-protected speech and association, and the limits of sysop liability for the activities of third parties.

Other matters
We have continued our ongoing investigations of cases that raise issues that may be of EFF interest. In many of these cases we have chosen either not to become involved, or to wait until the cases reach a procedural stage (such as an appeal) at which it would become more appropriate for the Foundation to intervene.

The EFF phone line has become, to some extent, a "hotline" for people who are curious and/or worried about how their rights as citizens and as computer users may be threatened specifically or generally by government action. We have been in contact with people who were convicted of computer crimes before the EFF came into existence, and occasionally have been able to provide useful information to the lawyers handling appeals of these cases. We also have become a center for general information, with phone calls, mail, and e-mail every day requesting information about EFF and its work.

Two versions of the Massachusetts Computer Crime Bill have been introduced in the Massachusetts legislature, one of which is identical to the EFF bill which didn't pass last year. Mike, Sharon, and Mitch will all be working toward passage of the bill this year.

Conferences and Meetings
On December 19th John and Mitch spent half a day at Lawrence Livermore National Labs in Livermore, California at the invitation of the computer security management there. The trip was arranged by Russell Brand. We spoke to a large general audience of lab employees as well as had meetings with smaller groups of security experts concerned with security both at Lawrence Livermore and on the large Department of Energy computer network generally.

John and Mitch also appeared on a panel at Mac World at the Moscone Center on Friday, January 11th, which was chaired by Jim Warren. Also appearing was Alameda Country District Attorney Don Ingraham. John spoke in Los Angeles at a combined SIGGRAPH and ACM meeting in early January.

Compuserve
Scott Loftesness, who is a Well member, EFF supporter, and Compuserve veteran is about to open a Telecommunications forum on Compuserve which will feature an EFF sub-forum. Library materials from the Well have already been ported over. We will announce this in the EFF conference on the Well and encourage people to seed the Compuserve forum with their participation to help it get off to a good start. ⇦

Contact

How to get in touch with the EFF:

Via Computer Networks:
Send requests to be added to or dropped from the EFF mailing list or other general correspondence to eff-request@well.sf.ca.us. We will periodically mail updates on EFF-related activities to this list.

If you receive USENET newsgroups, your site may carry two new newsgroups in the INET called comp.org.eff.news and comp.org.eff.talk. The former is a moderated newsgroup of announcements, responses to announcements, and selected discussion drawn from the unmoderated "talk" group and the mailing list.

Everything that goes out over the EFF mailing list will also be posted in comp.org.eff.news, so if you read the newsgroup you don't need to subscribe

Postings submitted to the moderated newsgroup may be reprinted by the EFF. To submit a posting, you may send mail to eff@well.sf.ca.us

There is an active EFF conference on the Well, as well as many other related conferences of interest to EFF supporters. As of August 1990, access to the Well is $8/month plus $3/hour. Outside the S.F. Bay area, telecom access for $5/hr. is available through CPN. Register online at (415) 332-6106.

A document library containing all of the EFF news releases, John Barlow's "Crime and Puzzlement" and others is available on the Well. We are working toward providing FTP availability into the document library through an EFF host system to be set up in Cambridge, Mass. Details will be forthcoming.

Via Mail or Telephone:
The Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141
Telephone: (617) 864-0665
Fax: (617) 864-0866

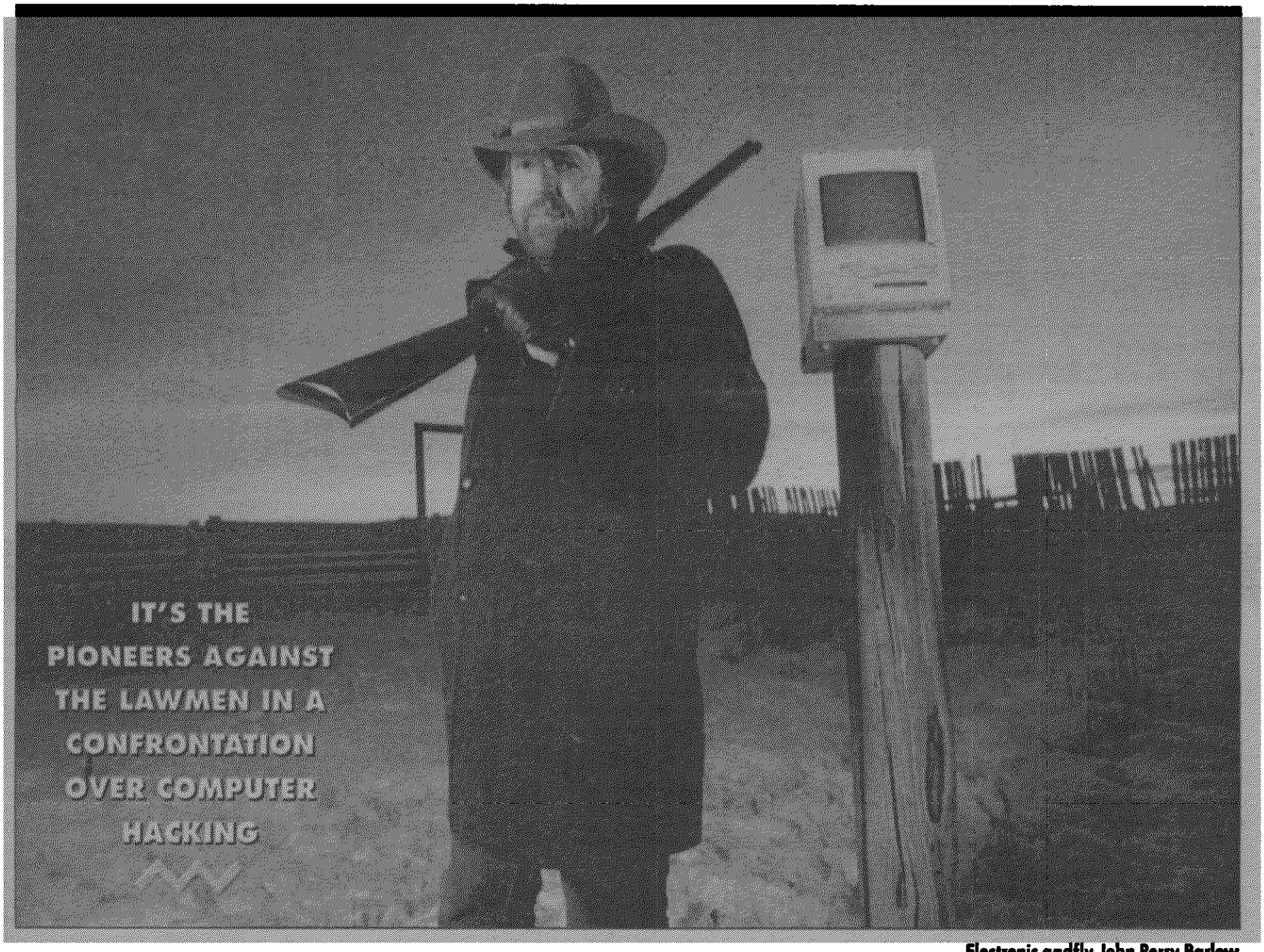
EFFECTOR

The Electronic Frontier Foundation, Inc.
155 Second Street Cambridge, MA 02141

ef.fec.tor n, Computer Sci. A device for producing a desired change in an object in response to input.

San Francisco Chronicle

SHOOTOUT ON THE ELECTRONIC FRONTIER



Electronic gadfly John Perry Barlow on his ranch in Pinedale, Wyoming

PHOTO BY TED WOOD/SPECIAL TO THE CHRONICLE

Is the Satanism Scare Overblown?

The Real Crisis in Education

This World

May 12, 1991

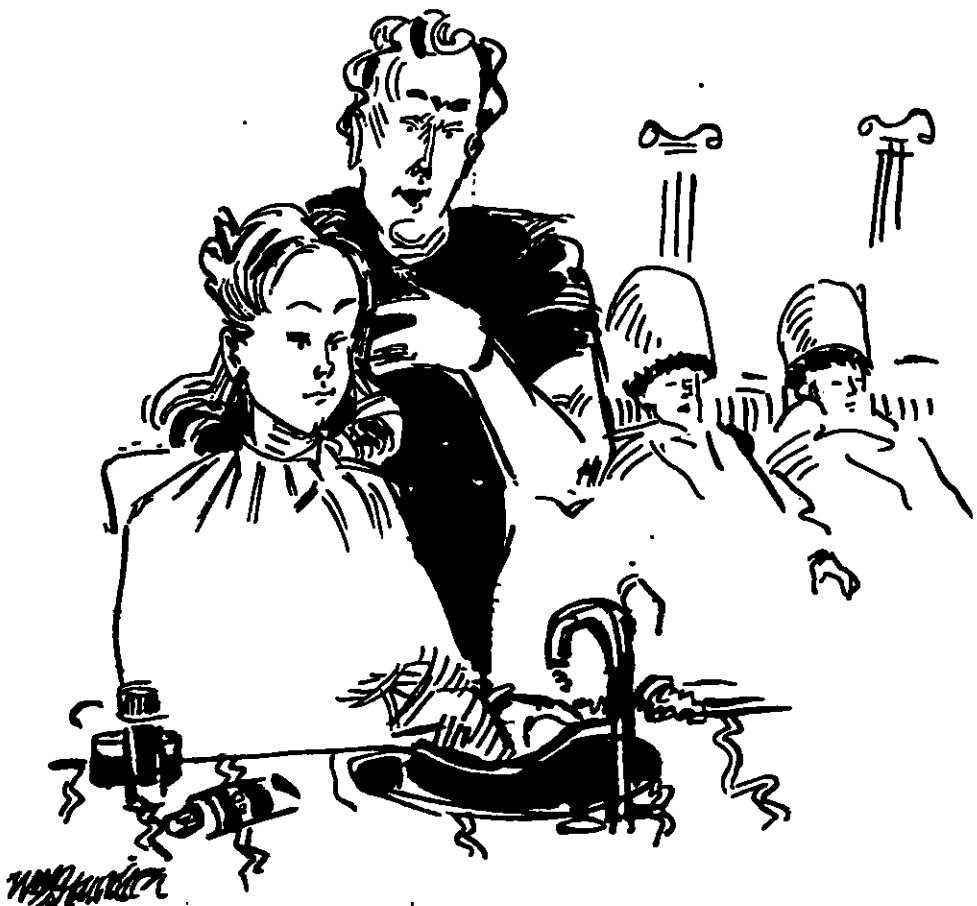
FEATURES

DEPARTMENTS

This World is edited by the San Francisco Chronicle. Unsolicited manuscripts can be returned or acknowledged only if accompanied by a stamped, self-addressed envelope. Letters to This World may be edited for space and clarity. Send letters or manuscripts to Lyle York, editor, This World, The San Francisco Chronicle, 901 Mission Street, San Francisco, CA 94103

A SECTION OF THE SAN FRANCISCO EXAMINER & CHRONICLE

THE NOW SOCIETY *Wm. Hamilton*



Did you know you have incredibly normal hair?

Paradise for the Homeless

Last resort
ANDY ROONEY

When I drive past the squalid living quarters of permanently unemployed Americans living in our biggest cities — or look down with pity and a touch of remorse, or even contempt, at a homeless man lying on a piece of cardboard, up against a building, on a busy street in New York City — I wonder why the unhappy unemployed and the desperate homeless don't go someplace else and get a new start. Why don't they get out of this harsh city of New York and make their way to one of 10,000 good small towns in America?

New York is the last place in the United States I'd want to be if I were broke and homeless. It's the best city in the world if you have money and the worst if you don't. It's inhospitable and indifferent. It's cold in the winter, hot in the summer. It's no place to sleep on the street.

Recently I was in Palo Alto. It was an especially pleasant day — the kind of day that has brought so many Easterners west. I walked 10 blocks around the pleasant little downtown area and was struck by how nice everything seemed.

Residents of Palo Alto probably would have run me out of town if they'd known what I was thinking. "If I were poor, unemployed, homeless and sleeping on the street in New York," I was thinking, "I believe I'd find a way to get to Palo Alto and be homeless and unemployed here instead."

In New York City there are a million people on welfare. That's reason enough for a homeless person on welfare to get out. If you're in trouble, you get more attention if there aren't many people in the same trouble you're in. That's the case for Palo Alto but there's a case against it, too.

It's an unfair fact that the cities that do the most for the homeless get the most homeless. New York pays out more money in welfare than any city in the world, so it gets a disproportionate number of America's poor.

I called the police department in Palo Alto to ask about its policy on the homeless. The officer on the desk told me they have a food program and occasionally provide temporary shelter but that most of the homeless "migrate to San Francisco or San Jose because they have adequate shelters for them." In other words, if you want to solve your homeless problem, don't help them.

The poor of New York's streets don't go to Palo Alto for the same reason most of us don't move. We're trapped where we are. We have ties that bind. There are a thousand reasons we can't pick up and leave even if we hate it where we are. We have a job we don't dare leave, we have family, financial obligations, a home that could be hard to get out of, or rid of, and a familiar lifestyle we are afraid to abandon even if it's not what we really want.

Even though the poor and homeless are not usually bound by the same things that bind the rest of us to the status quo, they have their own problems moving. What they lack is the ability to get up and get out. The homeless person doesn't have a nickel and wouldn't know how to leave if he had 10,000 nickels. He's a victim of his own incompetence. It's part of why he's where he is, but if some people are, as I suspect, simply inept at living, it doesn't mean they should be sentenced to a life of unhappiness.

There's an unspoken "It's their own damn fault" attitude toward the poor. Even if that's part true, it's irrelevant. Something has to be done for them, both for our sake and for theirs. I realize moving to Palo Alto isn't the answer. ■

Finally — Justice for a Child

Sarah wins

BOB GREENE

Sarah won. In language bordering on cold fury, the Illinois Appellate Court recently overturned virtually everything that Chicago Juvenile Court Judge Walter Williams has ordered in the case of the child we are calling Sarah.

It has been one year since I began reporting about Sarah. In previous columns ("Home Is Where the Heart Is," May 13, 1990; "A Child Learns to Hate," June 24, 1990; "Sarah — at the Mercy of the Court," December 16, 1990), I told what had been done to her.

Sarah, who was abandoned by her heroin-addicted mother at birth, lived with Joseph and Marge Procopio of Bridgeview, Illinois, until she was 5. Then the Illinois Department of Children and Family Services (DCFS) recommended that she be turned over to her birth mother and the boyfriend. Williams ruled late last year that Sarah would not be allowed to visit, see or speak to her foster parents. Rejecting the recommendation of the children's psychiatrist he had asked to evaluate Sarah, the judge ordered that the wishes of the birth mother must prevail. Sarah would live with her.

The appellate justices ruled that when Williams had turned Sarah over to the birth mother and her boyfriend, the judge was in violation of federal law.

From the appellate decision:

"What happened to (Sarah) as a result of (Williams') total ignorance or total disregard of the federal law is shocking. (Sarah's) story is the account of a helpless child caught in the quagmire of the bureaucratic maze which we mistakenly call our child welfare system. Unfortunately, the judicial system did not respond to her plight. Instead, it became part of the quagmire, adding to (Sarah's) misfortune.

"There is no doubt that DCFS and our Juvenile Court system are abysmal failures. There are reports that almost as many children are harmed as are benefitted by coming under their common aegis. . . . Every effort must be made . . . to see that what happened to (Sarah) never happens to another child in Illinois."

The appellate judges ruled that Sarah must be allowed to visit with the Procopios and that Sarah must be allowed to receive ongoing therapy to deal with her grief. These were things denied her, on Williams' orders. Legal advocates for Sarah had petitioned the Appellate Court to overturn Williams on those two specific points.

But the appellate judges went beyond that. They also reversed the most crucial ruling in Sarah's case that had turned her over to the birth mother. The appellate judges ruled that when Williams, in 1989, took Sarah from the only home she knew, Williams himself was in violation of the law.

The law referred to by the appellate justices is the Adoption Assistance and Child Welfare Act, which mandates timely judicial disposition in cases such as Sarah's. The appellate justices wrote that Williams' action precipitated "the turmoil and problems (Sarah) has suffered and may suffer the rest of her life . . . (Williams) was wrong. A child's best interest is not part of an equation. It is not to be balanced against any other interest." The judges stated that rulings by Williams were "against the manifest weight of the evidence and . . . an abuse of discretion."

The appellate judges ordered a new hearing to determine where Sarah should live — and mandated the decision be based "solely on the best interest of (Sarah)."

For 75 pages, the appellate judges laid out what had been done to Sarah by DCFS and the Juvenile Court system.

"(Sarah) was born on April 27, 1984, suffering tremors from heroin and cocaine withdrawal. Her mother, age 28, and father, age 32, were not married and both were drug addicts. (Sarah's) mother was also a prostitute. During her pregnancy with (Sarah), she was prostituting and using heroin and cocaine. (Sarah's) mother had two other children when (Sarah) was born. She had been convicted of child neglect and abandonment of her other daughter."

Here is how the appellate judges summed up what Sarah's life was like in the Procopios' home: Sarah "lived a relatively common . . . neighborhood life. She had a dog of her own and she had a back yard with a small swimming pool and swing set. . . . There is no doubt about the fact that the Procopios have done a beautiful job with (Sarah). Not only have they nursed her through her addiction, but they have provided a rich, stimulating environment for her."

That is the home from which Williams — without ever having seen Sarah, and with the backing of DCFS — ordered her removed.

And the home to which Williams sent her? Here is the appellate judges' summation of the birth mother and the boyfriend:

The birth mother and the boyfriend had "a 10-year-history of drug abuse, prostitution, child neglect, child abandonment, forgery convictions, adjudications of being unfit parents and other anti-social behavior."

During the time that Sarah was living with the Procopios, according to the appellate judges, her older sister and brother were taken into protective custody, and the birth mother was charged with abandonment. In 1988 the Circuit Court ruled that the birth mother was an unfit parent.

But the birth mother and boyfriend, in 1989, were able to demonstrate to Williams that they were off drugs. Williams gave her to those people. That is the ruling the appellate judges deemed to be in "total ignorance or total disregard" of the law.

So Sarah has won. But what does that mean? She is still living with the birth mother and the boyfriend, and will remain with them at least until a new custody hearing is held. It is unclear when she will begin visiting the Procopios.

Court testimony during the past year has painted a grim picture of what she may have been told about the Procopios during the 20 months since she was taken away. Lawyers involved in the case fear that she has been turned against the Procopios by being told that they abandoned her and never loved her — that she has been "taught how to hate," according to one lawyer.

What does she believe about love and trust and family — and how can her life possibly be repaired now? Sarah won in court the other day — just before her seventh birthday. ■

All the Roman Numerals Are Wrong!

CXMCXIILXCM

JOE BOB BRIGGS

Let's return to the fourth grade for a moment. Today's topic is Roman Numerals.

They taught us this stuff, and it's made my life hell ever since. The problem was, I remembered it. I didn't remember anything else, but I remembered Roman Numerals. Miss Young did it to me. Miss Young was a knockout in tight-fitting dresses who had no business teaching elementary school, but there she was, diligently explaining Roman Numerals, and so I remembered it.

So today, I can't pass up a copyright notice. At the end of the movie, when it says "All rights reserved, copyright MCMLXXVII," suddenly I'm immersed in the Roman Numeral, trying to figure out whether that means the year 1977 or the year 977 or the year 2977. Because once you've been indoctrinated in Roman Numerals, you can't give it up. Everyone else can go to the Civil War battlefield and peacefully observe the rusting cannons and the monuments to fallen Georgia soldiers. Not me. I'm over by the inscription, where it says *Anno Domino, Requiescat Pace, Inna Gadda Davida MDCCCLXIV*, studying each letter for about five hours until I can yell out "Eighteen sixty-four! It says eighteen sixty-four!" I'm like the Nerd From Hell.

Now. Big problem starting last year. I decided that all the Roman Numerals are wrong. I'm not kidding. But before I explain what I mean, a brief review is in order.

"Roman Numerals, as Taught by Miss Young":

I means one.

II means two.

III means three.

Now it gets tricky.

IV means four.

"What? Why does IV mean four?"

Because V is the symbol for five, and the Romans didn't want to write IIII, so they put a I in front of the V to indicate "five minus one."

"Why not just write IIII?" we asked.

And then she went into a big explanation about how the Romans had to chisel these numbers on sheer granite, and it took a long time, and so they tried to make them as short as possible.

And then she would tell us that X means 10.

So what would nine be?

And maybe one Rhodes scholar in the class would say "IX" and win a cookie.

Stick with me. Now it gets trickier.

C means 100. So how would the Romans write 90?

XC, right?

Now the even trickier question: How would they write 99?

And no one would ever get it. Because the answer was "IC." Meaning 100 minus one.

Because the only other way to write it would be "XCIX," and who could ever figure that out, so why not just write "IC"?

And so every time we had a test, everybody would miss the 99 question, or, better yet, the 999 question. (Answer: "IM.")

Are you following this? It doesn't matter. I have to do this.

Last lesson in Roman Numerals: The largest symbol they had was M. It means 1,000. So when we get to the year 2000, it will be one of the few years in history that the Romans can write down more easily than we can. It's the year MM.

But in the meantime we've got all these difficult years, that lawyers like to use in books and on movies and on legal contracts. The '80s were especially bad. You had stuff like "MCMLXXXVIII" where you've got so many letters in so many different combinations that it takes you about three hours to figure out that's 1988.

But then we got to 1990, and I thought "Thank God." Roman laziness will take over now! The "minus" thing is going to kick in. Those copyrights are going to shrink down to *nothing*.

And so 1990 rolled around, and I was reading the copyright on a videotape, and I saw this weird combination I'd never seen before: "MCMXC." And then I noticed that everybody was using this: "MCMXC," and then, when 1991 rolled around, "MCMXCI."

What's going on here?

Where is Miss Young?

I want every copyright attorney in this country to be summoned to Miss Young's office immediately.

We're making a huge mistake. We're going down a doomed road toward hundreds and thousands of unneeded X's and C's and L's in our future.

Why isn't 1990 "MXM"?

In other words, "1,000 plus 1,000 minus 10."

You ignorant lawyers are making the Romans chisel two extra letters in a block of sheer granite!

And what problems has this already created for the year 1999?

Will we have "MCMXCIX"? It will be a worldwide disgrace. How can we go around subtracting one with the second letter, subtracting one with the fourth letter and subtracting one with the sixth letter, but *refuse* to do the most economical subtraction, which would simply be "MIM"?

I'm telling you, it's been a long time since the fourth grade, but it's vivid in my memory. We're making a huge mistake. We're going down a doomed road toward hundreds and thousands of unneeded X's and C's and L's in our future. We'll have to build a new wing onto the Library of Congress. And we're offending Roman Numeral scholars everywhere.

I'm very agitated about this. I know I'm right. Please, somebody, some scholar of the ancient cultures, write to me and tell me there's *one* thing I learned correctly in grammar school. I feel confident that I'm C percent right and the rest of the world is wrong.

Well, maybe not that confident. But I'm IC percent sure. ■

CALLAHAN

Gulf War Veterans to Be Malled

Yellow and green
MIKE ROYKO

There's been a sharp slump in the sale of yellow ribbons. But that's no reason for those in need of a euphoria-fix to panic. Help is coming in a big way.

An organization of patriots called Yellow Ribbon America is planning a spectacular, nationwide series of rallies to celebrate our Gulf War victory and welcome the triumphant troops.

And the celebrations will be held in settings that couldn't be any more traditionally American. Not in village squares, public parks, in front of town halls, or on Main Street USA.

The gala events will be held in more than 1,000 shopping centers across the nation. And on a Saturday, which is always the best day to be in a shopping center, whether to buy something, hang out, meet a famous disc jockey or celebrate a military triumph.

The organizers of the event say they have lined up scores of corporate sponsors, and others are expected to sign on. Some of the sponsors will provide "gift paks" to all Gulf vets who show up. As they said in a news release: "The package will feature information on special offers and discounts from participating companies."

A spokesman for Yellow Ribbon America said veterans of World War II, the Korean War and the Vietnamese War are also invited to come and be honored at the shopping center rallies, although nothing was said about giving them corporate "gift paks." Nor did he say anything about those who served in Grenada and Panama, but it can be assumed that they would get at least a cup of coffee if they show up.

So if there are shopping centers anywhere near your community, chances are that one of them will be taking part in the big day. They will if they're smart. The organizers expect 10 million people to turn out, so if every one of them spends only $10, it could be one of the biggest retailing days since we last celebrated the birth of Jesus Christ.

As a patriotic American, I was cheered by the news of this coming attraction, although I was momentarily disappointed that I don't qualify for a corporate "gift pak." But then I remembered that in the foreign land where I served, there were no local religious laws against boozing and cavorting with females, and I felt better.

The only flaw in the plans for this grand day is that we have to wait until June 15 for the Super Saturday. And that's unfortunate, because a lot of gloomy party-poopers are on an anti-euphoria kick these days.

The organizers expect 10 million people to turn out, so if every one of them spends only $10, it could be one of the biggest retailing days since we last celebrated the birth of Jesus Christ

For example, I just received a copy of one of his "Essays in Theology" by the Reverend Richard P. McBrien, chairman of Notre Dame's theology department.

Space doesn't permit me to repeat the entire essay — and as a euphoric patriot, I wouldn't, because he actually thinks the war was morally wrong. But here is part of what he wrote:

The glow has faded from the allies' "great military victory" in the Persian Gulf. Instead of basking in the sunlight of a "new world order," the Gulf region is in an even greater mess today than it was on January 15, when President Bush initiated military action against Iraq.

Kuwait is still literally ablaze, its atmosphere thickened with pollution, its skies darkened at midday, its waters and shores coated with oil, its national character sullied by incidents of brutal revenge against Iraqis and Palestinians.

Iraq's own infrastructure is in shambles. Many thousands, even millions, of its citizens have been deprived of the basic necessities of life: water, electricity, housing, transportation and medical care.

Encouraged by President Bush to overthrow Saddam Hussein (but without the necessary military support), the Kurds in the north and the Shiite Muslims in the south were savagely beaten back and then driven from their homes.

Hundreds of thousands of refugees, including countless children and aged, have been devastated by disease, malnutrition and exposure to the elements. Their efforts to escape the Saddam regime have, in turn, created new and overwhelming problems for the bordering nations of Turkey and Iran.

Boy, if there's anything I can't stand it's a nitpicker. I'm surprised that he didn't also complain about the inept surgery that kills patients in some VA hospitals. Or that he didn't mention Saddam's big birthday party, during which Saddam acted like a hero and the band played: "I Did It My Way."

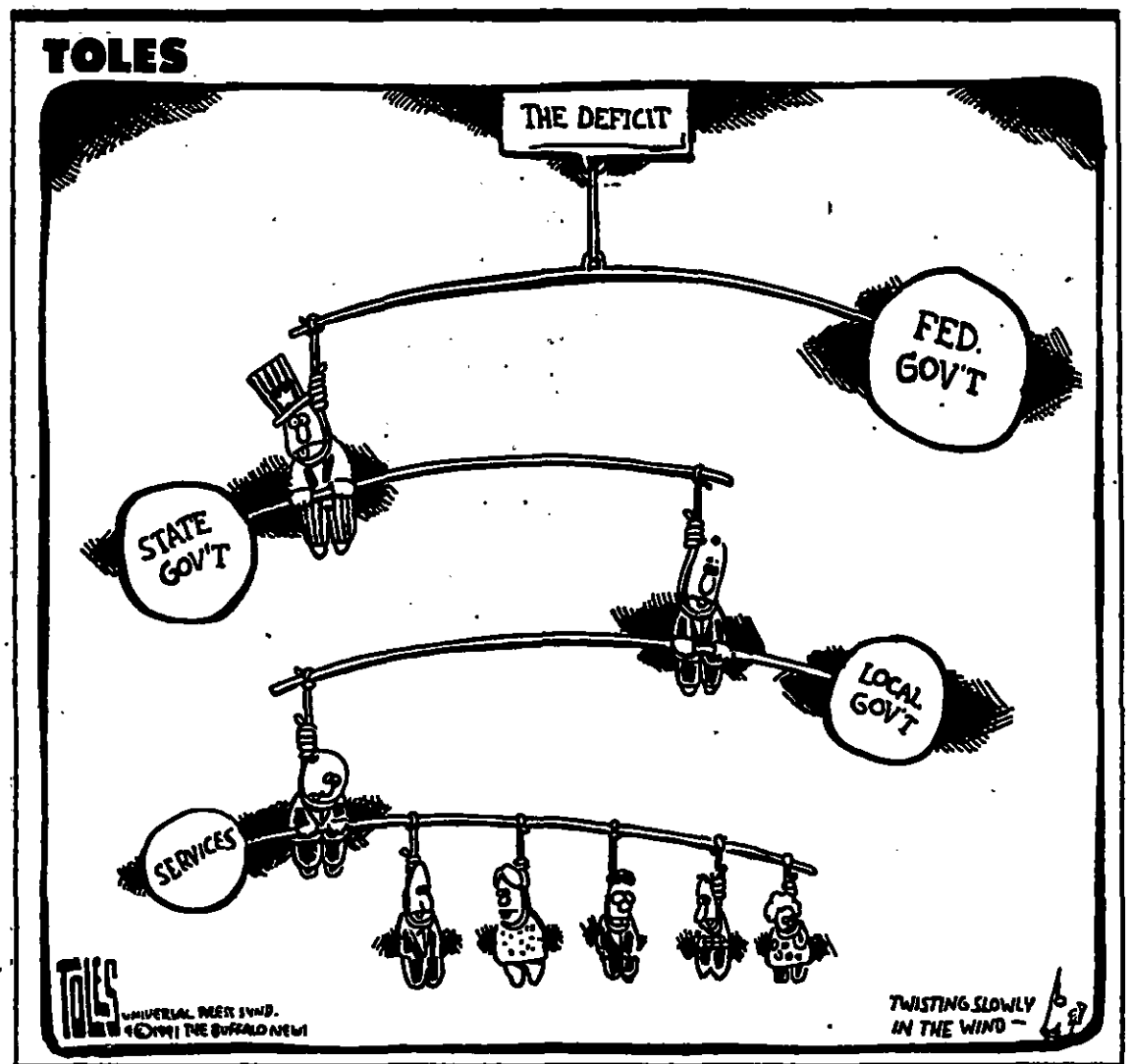
Sure, that part of the world is a bigger mess than it was before we restored the emir of Kuwait to his gold toilet seat, but that's to be expected. After a Super Bowl, the stadium is always covered with glop.

I suspect that the Reverend McBrien's problem is that he isn't a sports fan. If he were, he would understand why we are having big celebrations. It has been explained by sports theologian Slats Grobnik:

"Remember, a bloop hit looks like a line drive in the box score.

"Even if you win ugly, a win is a win.

"And the game ain't over until the last Kurd is out." ■



HARPER'S INDEX

☐ Average ratio of U.S. funds spent fighting a war to U.S. funds spent on that war's veterans' benefits: 1 to 3

☐ Number of Americans who received veterans' benefits last year for a relative's service in the Civil War: 51

☐ Death rate, since last August, for American military personnel stationed in the Persian Gulf, per 100,000: 69

☐ Death rate for men between the ages of 20 and 30 living in the United States since last August, per 100,000: 104

☐ Rank of 1991, among years in which the U.S. State Department has warned Americans to avoid the most countries: 1

☐ Number of people who applied to the United States for political asylum last year: 101,000

☐ Number who applied in 1979: 1,000

☐ Number of Soviet Jews who were hired by Israeli manufacturers last year: 12,000

☐ Number of Palestinians who have been laid off by Israeli manufacturers this year: 8,500

☐ Number of countries in which more than half the population is Muslim: 36

☐ Percentage of the population of Kuwait in 1989 who were domestic servants: 25

☐ Number of plastic garbage bags the U.S. Army has estimated will be needed to clean up Kuwait, per month: 1,500,000

☐ Percentage change in federal funding for energy conservation proposed by President Bush this year: minus 36

☐ Number of the solar panels installed on the White House roof by President Carter that are still there: 0

☐ Portion of all cars that will have a microwave oven in the year 2000, according to the Campbell Soup Company: 1 in 4

☐ Rank of Fords, among the cars most often bought by Asian-Americans: 1

☐ Size of one traffic jam in Tokyo last year, in miles: 84

☐ Number of malls that will open in Japan this year, per month: 6

☐ Chances that an employed American works in a shopping center or mall: 1 in 11

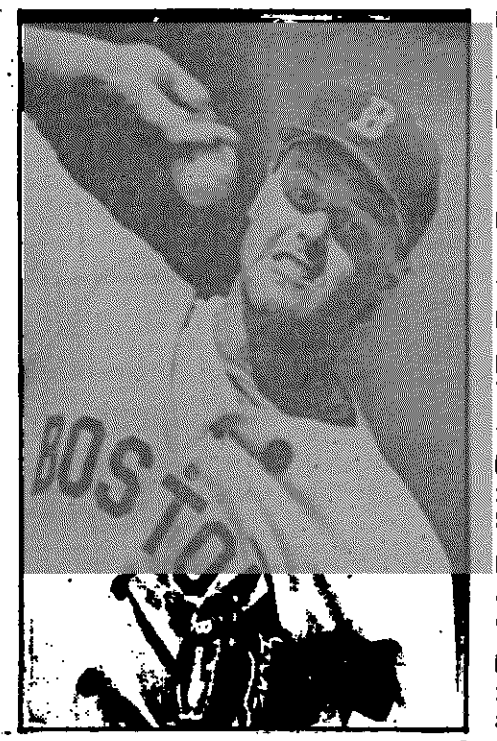
☐ Percentage of fast-food restaurant workers who admit to doing "slow, sloppy work on purpose": 22

☐ Rank of the Navajo tribe, among the largest suppliers of potatoes to Frito-Lay: 1

☐ Number of times a nude or seminude woman accepted a Domino's Pizza delivery in Washington, D.C., last year: 15

☐ Chances that a female inmate in an American prison is a mother: 4 in 5

☐ Portion of Hallmark's 1,200 different Mother's Day cards that do not include the word "mother" or "mom": 4 in 5



Estimated amount that Boston Red Sox pitcher Roger Clemens will earn this season, per strikeout: $20,400

☐ Number of articles in the New York Times this year that have included the phrase "mother of all": 29

☐ Number of photographs of gulf war casualties in the Associated Press photo library: 28

☐ Number of U.S. AIDS deaths last year, expressed as a portion of all U.S. AIDS deaths since 1981: ⅛

☐ Percentage of U.S. hospitals that do not require that patients be told if they test positive for the AIDS virus: 25

☐ Average percentage of disposable income that an American spent on insurance premiums in 1984: 4

☐ Average percentage today: 7

☐ Ratio of the total personal debt owed by Americans to the total federal debt: 1 to 1

☐ Total amount of unclaimed private funds held by state agencies: $5,839,676,660

☐ Percentage change, since 1989, in total assets held by U.S. banks that the FDIC considers "threatened": plus 73

☐ Fee a Norwood, Massachusetts, bank requires from depositors before they can ask a question about their account: $1

☐ Price of a two-week session for high school students at the National Law Camp in Miami Shores, Florida: $1,450

☐ Price of a four-week session at the World Peace Camp for Teens, in Poland Spring, Maine: $1,500

☐ Price of a pair of fluorescent, bullet-proof, desert-camouflage jeans from Neiman Marcus: $800

☐ Amount of time it takes to hand-stitch a major league baseball, in minutes: 11

Colin Powell Didn't Need Affirmative Action

Georgetown flap
MONA CHAREN

The same week that featured General Colin Powell throwing out the first baseball at a Yankees game — to universal acclaim — also featured, at Georgetown University Law School, a new skirmish in the conflict over affirmative action.

Both deserve to be mentioned in the same breath because it is so painfully clear that what many blacks see when whites oppose affirmative action is recrudescent racism. They seem convinced that those who oppose affirmative action are the same people who opposed voting rights and equal education for blacks. They are sure they know the hidden motives behind opposition to quotas.

That is why it is so useful to look at the example of Colin Powell. White racism is easy to see. Perhaps white goodwill isn't so obvious. But it shines forth in the reception of Colin Powell.

Whites love Powell for some of the same reasons blacks do — because he is a successful military leader: bright, poised, commanding and engaging — a great American. Whites can laugh along when Powell relates that some journalists have taken to not mentioning the fact that he is black in their stories. "I think they think this is politeness," he explained in a recent speech. "But I tell them, 'Don't stop now. If I had shot someone, you'd mention my race.' "

Touché. Whites love Powell for another reason as well. They love him because he, like Governor Douglas Wilder of Virginia, fulfills their need for black heroes. Whites want our society to be vindicated. They want to believe that the system is not rigged and that those who strive and struggle and work hard and play by the rules can succeed whatever their color or ethnic origin.

Powell, the black immigrants' child from the South Bronx who is now the highest ranking military officer in the United States, is living proof of those maxims. He got there on merit. He is the embodiment of the American dream. And he believes that what worked for him — determination, hard work, guts — can work for others. That's what he told a group of black teenagers on a return visit to his childhood home in New York.

Fade-out. New scene. At Georgetown University Law School in Washington, D.C., a third-year student contributed an article to the student newspaper decrying the differing admissions criteria for blacks and whites. Using information gained while he was employed at the admissions office, Timothy Maguire noted that "48 out of 81 black applicants had grade point averages below 3.0" while "less than 20 percent of white applicants had similar grade point averages."

Whites want to believe that the system is not rigged and that those who work hard and play by the rules can succeed whatever their color or ethnic origin

The LSAT (Law School Admission Test) is scored on a scale of 10 to 48. Maguire reported that among students accepted to Georgetown Law School, whites averaged a 43, while blacks averaged 36.

Maguire, who is due to graduate May 27, is now in danger of being expelled from the law school. The campus has quite simply erupted since the publication of his article. The Black Law Students Association (BLSA) has demanded his expulsion and also that of the editor of the student newspaper who published the article. The law school dean told the New York Times that expulsion was "among the range of possibilities" currently being considered.

There are two charges against Maguire. The first is that he used confidential information in his article. Perhaps. But he told me that the admissions office never explained its policy on confidentiality to him when he worked there. Besides, that is clearly not the key issue. He named no names. And everyone knows that the question of confidentiality would never arise if those files revealed that blacks were being unjustly *excluded* from the law school.

The second charge is that this article "made disparaging remarks which have injured the BLSA community." Ah yes. So let's expel people who tell the truth. The truth hurts.

The BLSA is trying to suppress what everyone knows — that affirmative action means less qualified black people are given preference over more qualified white people. Unlike Colin Powell, that is the road of advancement they favor.

But when your policy cannot tolerate the intrusion of truth, doesn't that suggest that it has become corrupt? ■

LOW-SELF-WORTH-WORLD™

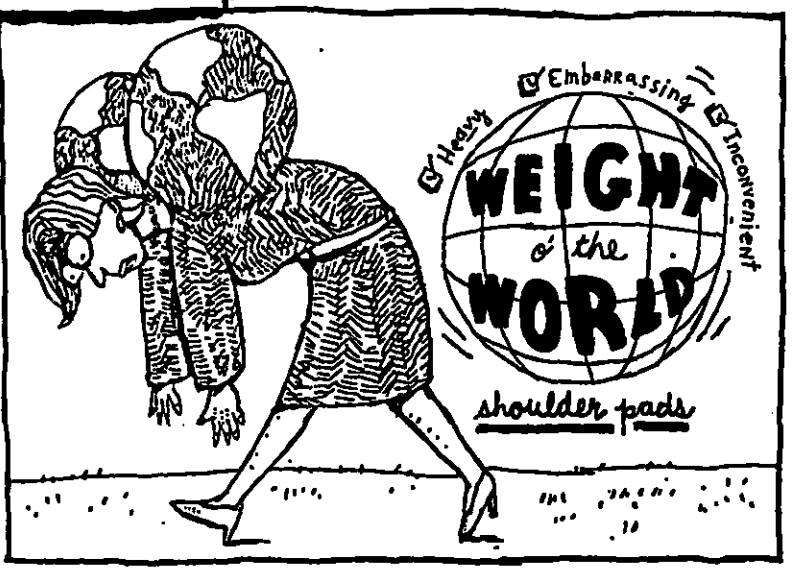
Wear embarrassing clothes! Waste hours and hours playing pointless board games! Travel to lonely places!

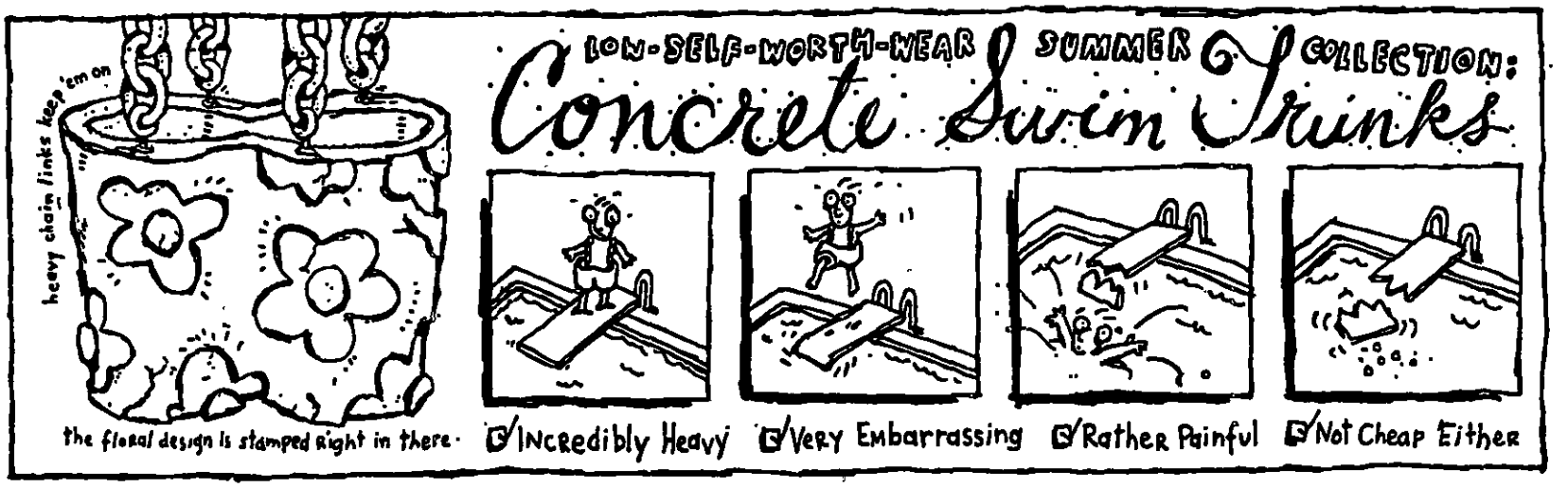
This caters perfectly to my bad taste!

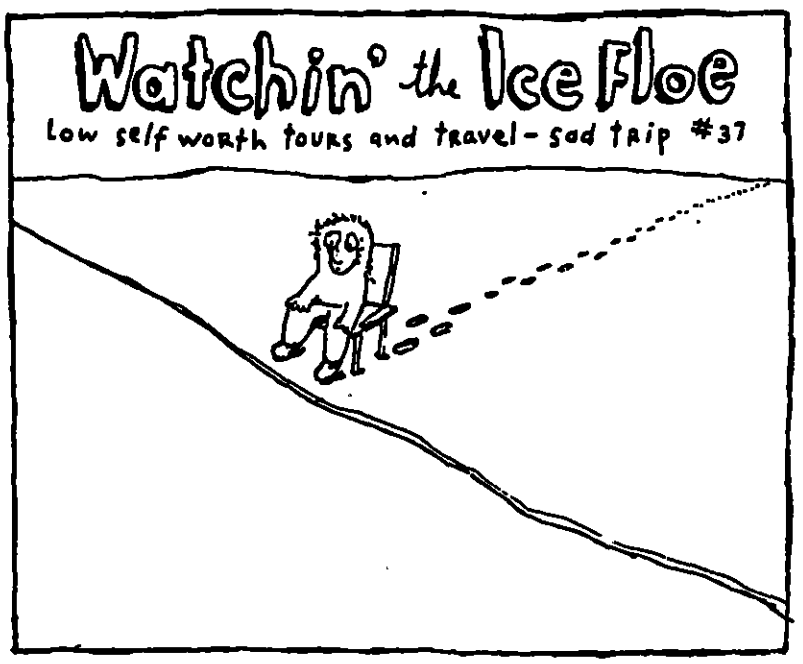
©1991 by Philip LeVine

Introducing

LOW-SELF-WORTH-WEAR™





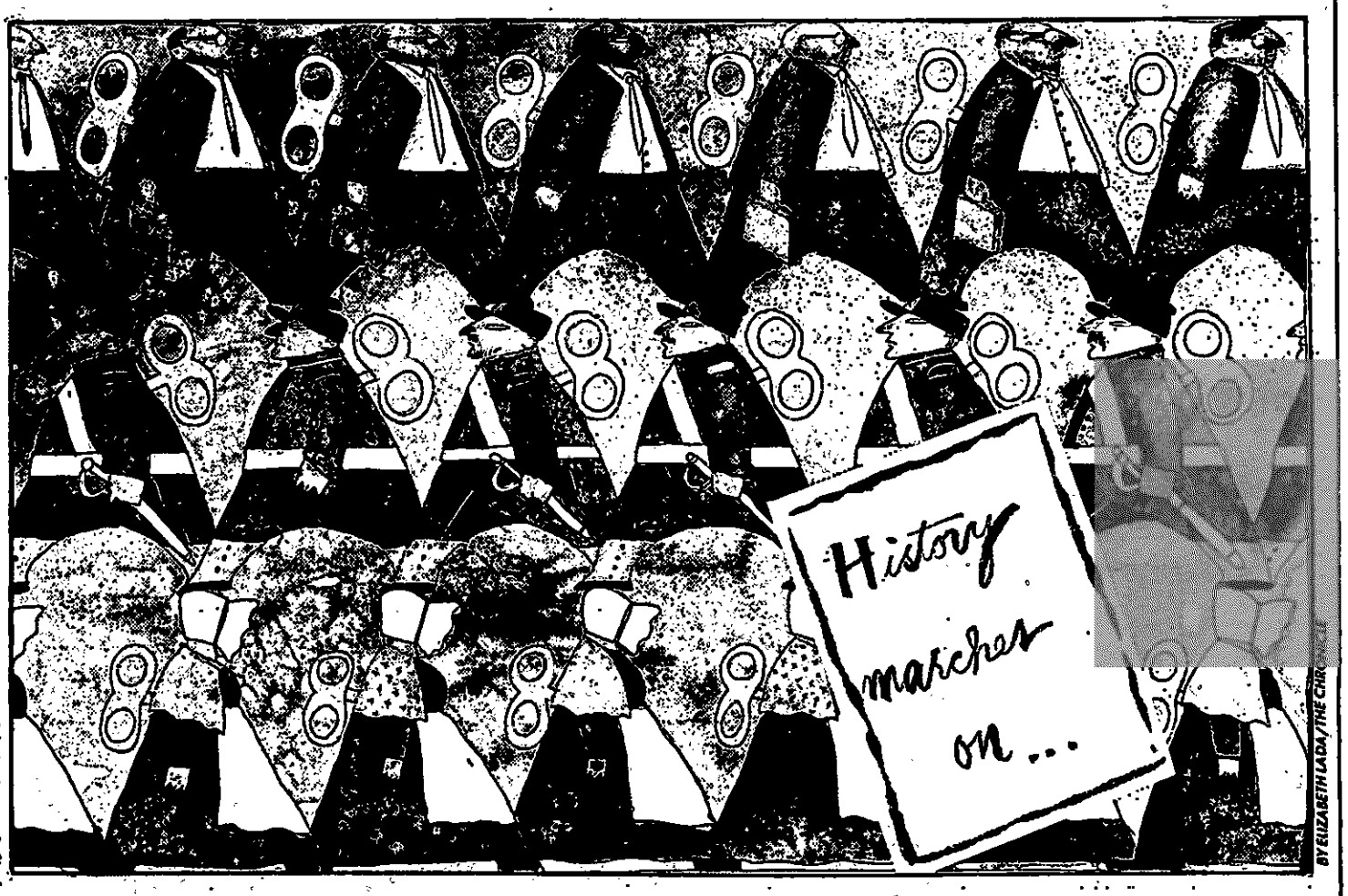


The Way We Are – And Will Be

HISTORICAL ANALYSIS CAN PROVIDE INTRIGUING – AND FRIGHTENING –

GLIMPSES OF AMERICA'S FUTURE

BY WILLIAM STRAUSS AND NEIL HOWE



BY ELIZABETH LADA/THE CHRISTIAN SCIENCE MONITOR

Barely two decades ago, Americans looked upon combat-age youths as moralizers bursting with inner wisdom to teach the world. But no one could mistake the youngsters of 1969 for those of 1991.

On campus, veterans of the '60s don't expect today's students to express any new-found truths, but rather to reaffirm well-worn slogans. In Saudi Arabia, we've heard troops taking pride in their role as blunt instruments of battle, showing a hardness the nation admires on the battlefield but criticizes elsewhere. America's twentysomethings have become, according to the newsweeklies, "the new lost generation."

Are we witnessing a metamorphosis in the American lifestyle? How does one explain such a dramatic transformation in a single age group?

In fact, what is happening is something much different: the aging in place of separate generations. By "generation," we mean a special cohort-group, possessing a distinctive sense of self, born over a span of about 17 to 25 years. Think of these generations as people moving through time, along what we call the "generational diagonal."

As each of us is born, comes of age, reaches the prime of life and grows old, we carry through our life cycle a unique historic signature, an "age location" against the events and trends of our time. And what is true for each of us as individuals is true of generations as a whole.

Thus, the bulk of today's Desert Storm soldiers — born near the "year of Woodstock" — grew up in a time when school and family were under assault, when adults grew disinclined to sacrifice for the sake of children. These kids became sharp-eyed survivalists at a very young age, and remain so still. Meanwhile, the coming-of-age zealots of the late '60s have aged into today's 40ish enforcers of "political correctness." Moralizers then, moralizers still.

The generational diagonal can provide insight where static age groups offer no answers at all. It can help explain why Americans worried about conformity during the 1950s, why inner cities exploded in the 1960s, why SAT scores fell through the 1970s and why old-age entitlements were untouchable during the 1980s.

It can also give new answers to historical questions, such as why the Great Awakening and American Revolution happened when they did, and why the Gilded Age followed the Civil War. Viewing the story of America as a sequence of generational life cycles gives us a new pattern for understanding our history — and anticipating our future.

When you look upon social history as a succession of generations, you see how each generation is shaped by its age-determined role in historic events.

Intuitively, everyone recognizes the importance of this "age location." Consider the Great Depression and World War II. For children at that time (who grew into the "silent" generation of Michael Dukakis and Sandra Day O'Connor), this era meant a smothering parental grip; for rising adults (the GI generation of Presidents Kennedy through Bush), teamwork and achievement; for midlifers (the "lost" generation of Truman, Eisenhower and Hemingway), a slowing down to a new sense of prudence; and for elders (the "missionary" generation of FDR and Douglas MacArthur), an opportunity to champion long-held visions.

This era defined the life trajectory of each of these generations over the next two decades. It planted in the silent generation the seeds of their lonely-crowd conformism, energized the can-do "new generation" of GI builders and achievers, and cast the lost generation in a poor and politically invisible old age.

But the pattern is not the same for every event. Compare the Depression of the 1930s with the "Consciousness Revolution" of the late '60s and '70s. The latter case saw children (whom we call the "13th generation") grow up quickly and on their own; saw rising adult "boomers" fragment and turn inward; saw silent midlifers speed up through "passages" to a new sense of personal adventure; and saw GI elders defend institutions under siege from the young.

AROUND THE YEAR 2020 — ROUGHLY 80 YEARS AFTER D-DAY AND THE FIRST BOOMER BIRTH YEAR — WE ARE SCHEDULED TO REACH THE NEXT GREAT HINGE OF HISTORY. THE CRISIS OF 2020 COULD BE A MOMENT THAT COULD RIVAL THE GRAVEST TRIALS OUR ANCESTORS HAVE KNOWN.

Neil Howe and William Strauss are co-authors of 'Generations: The History of America's Future, 1584-2069' (Morrow), from which this article is adapted.

VIEWING THE STORY OF AMERICA AS A SEQUENCE OF GENERATIONAL LIFECYCLES GIVES US A NEW PATTERN FOR UNDERSTANDING OUR HISTORY — AND ANTICIPATING OUR FUTURE

Just as history produces generations, so do generations produce history. At the heart of this interaction lies a recurring pattern of "secular crises" (threats to national survival and a reordering of public life) and "spiritual awakenings" (social and religious upheavals and a reordering of private life).

Notice the timing of the four great periods of crisis in American history. There were the colonial wars and rebellions culminating in the Glorious Revolution of 1689, the American Revolution, the Civil War and the twin emergencies of the Great Depression and World War II. Each is 80 or 90 years distant from the next — the span of, roughly, four generations.

Notice also how America's five great spiritual awakenings occurred almost 40 or 50 years distant from these events: the Puritans' "City on a Hill" in the 1630s; the "Great Awakening" around 1740; what historians call the "Second Great Awakening" of the early 1800s; the Bible Belt revival and radical populism of the 1890s; and the recent Consciousness Revolution. These events fall into a pattern because of the interaction between a generation's type and its "age location" among the happenings of the era.

Each of America's 18 generations, of course, has had a unique relationship with the story of America. But when we strip away such linear trends as rising living standards and improving technology, we see similar human dramas that repeat again and again. When we link age location with American lifecycles, we find a recurring cycle of four generational personalities — each cycle lasting about 80 or 90 years:

■ First, an Idealist generation grows up as indulged youths after a crisis. It comes of age with a spiritual awakening, fragments into narcissistic rising adults, cultivates principle as midlife moralizers and emerges as visionary elders who guide the next crisis. Examples: John Winthrop's Puritan Generation, the fiery founders and stern patriarchs of America's original New Jerusalem; Benjamin Franklin's Awakeners who, from their 20s to their 60s, took America from the Great Awakening to the American Revolution; Abraham Lincoln's Transcendentals, the most spiritually self-absorbed generation in our history, whose vision of a purifying apocalypse steered the nation toward the Civil War.

■ Next, a Reactive generation grows up under-protected and criticized during a spiritual awakening. It comes of age as alienated risk-takers, mellows into the tough midlife managers of crisis and ages into caustic but undemanding elders. Examples: George Washington's Liberty Generation — wild soldiers in youth, gritty war-leaders in midlife, cautionaries in old age; Ulysses Grant's Gilded Generation of metal and muscle who in midlife repudiated their prophetic next-elders by celebrating Pragmatism; and Harry Truman's Lost Generation, the turn-of-the-century "bad kids" whose early-life appetites electrified the 1920s and whose late-life exhaustion calmed the 1950s.

■ Next, a Civic generation grows up under new adult protection after an awakening. It comes of age by overcoming a new secular crisis, unites as a heroic and achieving cadre of rising adults, builds institutions as powerful midlifers, and later — during the next awakening — finds itself attacked as worldly elders. Examples: Cotton Mather's Glorious Generation, the colonial war heroes who became advocates of social discipline and material progress; Thomas Jefferson's Republican Generation, nation-builders early in life, whose major disappointment late in life was the ungovernable passions of their children; and today's "Baby on Board" Millennials.

■ Finally, an Adaptive generation grows up as suffocated children of crisis. This generation comes of age as adult-emulating conformists, produces the indecisive mediators of the next awakening, and ages into sensitive and other-directed elders. Examples: William Byrd II's Enlighteners, America's first "silent" generation, with no member whose name most of today's Americans could recognize; Henry Clay's Compromisers, the sober youngsters who watched their parents create a nation and the ambivalent elders who watched their children nearly destroy it; and Woodrow Wilson's Progressives, the shell-shocked youths of the Civil War and the sensitive, process-fixated leaders of circa-1910 America.

As generations layer themselves and age in place, the mood of the constellation itself shifts. A constellation with Civic doers entering elderhood and Idealist moralizers coming of age will set a national mood quite different (recall Watergate) from one with those two generational types in the opposite position (recall Pearl Harbor Sunday). Some constellations produce a national mood of staleness, others of rejuvenation. Some postpone crisis, others congeal it.

From the 16th century forward, this cycle has been constantly turning. It has shown only one aberration: following the Civil War, when the depth of human suffering caused the cycle to miss one beat, weakening rather than strengthening the generation then coming of age.

The generational cycle does not guarantee any particular outcome — for any generation or for society as a whole. Yet it does offer powerful insights into how the national mood will evolve in the decades ahead. In particular, it helps us foresee shifts in the personalities of today's living generations as its members grow older.

Let's locate ourselves on the cycle.

As the Consciousness Revolution recedes deeper into the national memory, we feel a post-awakening mood reminiscent of the years prior to World War I — when the radical turbulence of the 1890s had given way to complex procedural reforms.

Then as now, individualism was flourishing, confidence in institutions was declining and secular problems were deferred. Then as now, a 60ish cadre of post-heroic leaders were designing a legalistic world order, even as new armies massed and old hatreds festered. Then as now, feminism was gaining political power, moralistic attacks were growing against crime and substance abuse and family life was seen as precious but threatened. Antecedents can be found for this kind of national mood (and generational constellation) in the 1840s, 1750s and 1650s.

History records what happened over the two or three decades following these post-awakening constellations. Each time, the sense of drift and pessimism intensified. Then a crisis emerged, compelling all generations to unite in the face of perceived public peril. Each time — guided by the values of elder Idealists, managed by the pragmatism of midlife Reactives and mobilized by the energy of coming-of-age Civics — America passed through a major gate of history, usually in triumph.

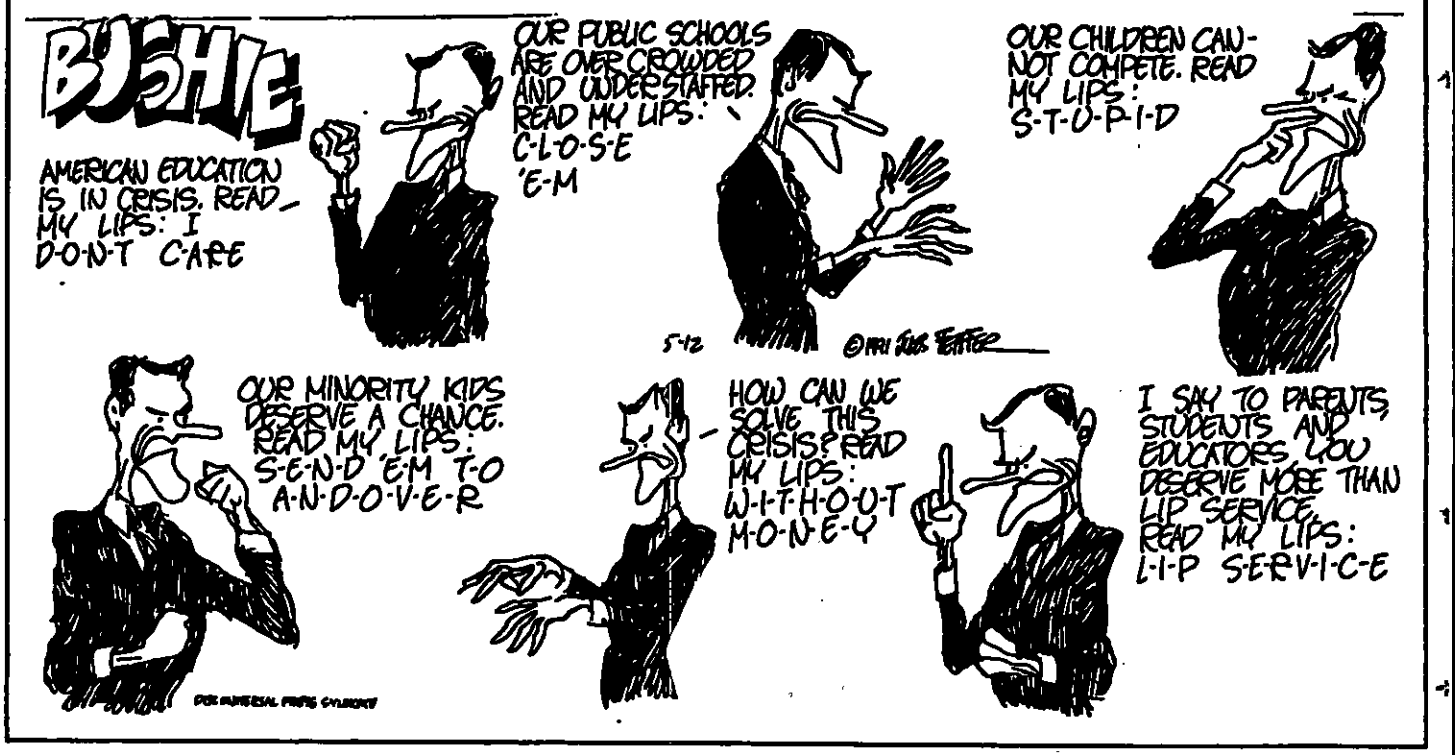
The aging of the current generational constellation has a clear message for the nation as a whole. Around the year 2020 — roughly 80 years after D-Day and the first Boomer birth year — we are scheduled to reach the next great hinge of history. The Crisis of 2020 could be a moment that could rival the gravest trials our ancestors have known. The risk of major war will be very high. The crisis may be about weapons proliferation, or environmental peril, or a collapse in the world economy. Whatever the problems, Americans will be inclined to attack rather than defer them, led by old Boomer priest-warriors who will care far more about inner principle than material sacrifice. The result could be triumph or tragedy beyond anything imaginable today.

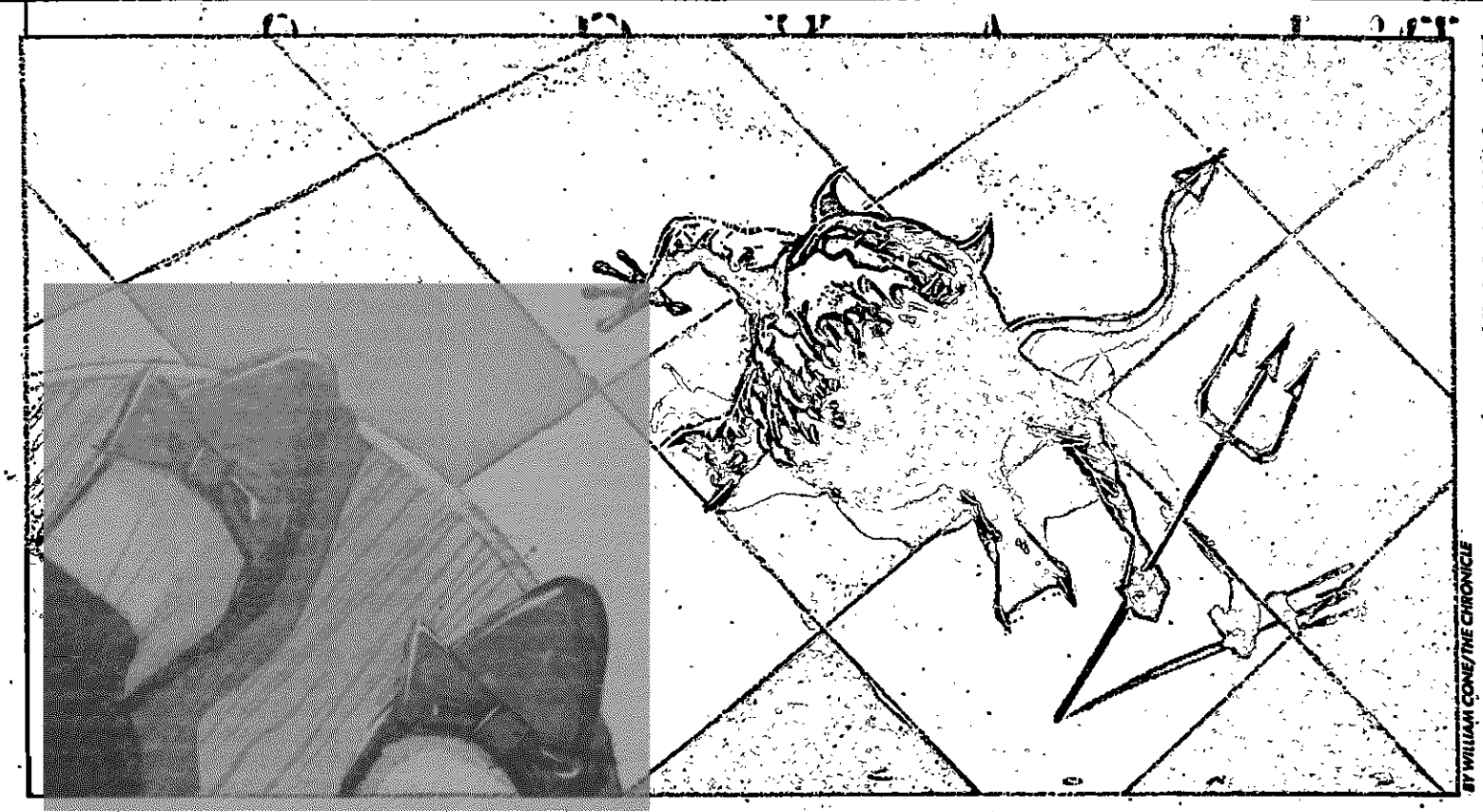
Many are noticing parallels between today and the Edwardian America before World War I. By the late 1980s, observes Paul Kennedy, Americans felt very much as they did in the early 1910s, expressing "contradictory moods of assertiveness mingling with anxiety, of robust self-confidence and profound despair."

Eighty years ago, no one could foresee the Battles of the Marne, the collapse of the League of Nations, the sudden end of prosperity and the test of national will yet to come. No one imagined that prohibitionist moralizers (Missionaries) then entering midlife would later age into the prophetic elders many still remember as America's World War II "Wise Men." Nor was it imagined that the cynical, kinetic teenagers (Lost) then entering rising adulthood would produce the winning midlife generals of the 1940s and the cautious elder anchors of our postwar "American High." Nor that the protected tots then being born would later come of age as nation-saving heroes (GIs). Ultimately, that generation of achievers would fulfill the vision of their parents by building a "Great Society" of friendly and well-ordered prosperity — only to hear their own children attack its spiritual emptiness.

Then — as now — America lay not at the end, but at the beginning of quite a lot of history. ■

FEIFFER





BY WILLIAM CONE/THE CHRONICLE

Satanism Scare May Be Overblown

John Johnson and Steve Padilla
SOCIETY

Jacquie Balodis is talking softly about her bad childhood. How bad was it? It was unbelievably bad.

"I was born into Satanism," said the 49-year-old woman from Garden Grove in Orange County. As she describes it, her early years in Pueblo, Colorado, included devil worship, human sacrifice and cannibalism.

She said that as a teenager she was twice impregnated by her stepfather (now deceased). Both fetuses were aborted and used in rituals, she said. "Part of me believed it was my privilege to give my child to Satan."

The memories were suppressed for years, she insists, then recovered in psychotherapy.

Balodis admits it sounds weird. Weirder yet, such tales are becoming common. Across America, people say that they have regained memories of abuse by parents who belonged to a worldwide network of devil-worshipers.

Authorities say America is witnessing an epidemic of concern over Satan and his minions, especially among fundamentalist Christians. So-called ritual abuse is only part of it.

But are these stories of incest and human sacrifice true? Many mental-health experts think not. And at least two law enforcement officers, with the FBI and the San Francisco police, say they have looked into some of the claims and found nothing.

Some real events probably lend credence to the idea that Satan-worshipers are everywhere. For instance, there is a self-styled Church of Satan. It was founded in 1966 by a former lion tamer and revival-show organist. Preaching the pursuit of pleasure, it employs Satanic symbols such as pentagrams and black robes in its rituals. But it has not been linked with criminal activity.

In a just-concluded Orange County case, two self-proclaimed victims took their elderly mother to court and accused her of having been part of a child-murdering cult. A jury found in their favor April 12, although it did not award them money damages.

Some jurors said the verdict did not mean that they believed the Satanism story, only that the women had been abused. But one of the women's supporters said after the decision, "It's a grand day for victims. Somebody believed them. It's now going to encourage more victims to talk."

A lot of people already are talking.

"The Satanism scare has at various times approached panic levels," said David Bromley, a sociologist at Virginia Commonwealth University. Bromley co-wrote a forthcoming book on the subject called "The Satanism Scare."

Jeffrey Victor, a sociologist at Jamestown Community College in New York, has tracked 33 "rumor panics" in 24 states in the late 1980s. One occurred in 1988 in Breathitt County, Kentucky, where parents kept their children home from school amid rumors that Satanists were plotting to kidnap blond, blue-eyed children. Another caused scores of Jamestown, New York, citizens to arm themselves with clubs and scour the forests for a chimerical band of Satanists.

Moreover:

- A 1989 telephone survey of 1,000 Texans by the Public Policy Resources Laboratory at Texas A&M University found that nearly 80 percent of the respondents thought Satanism had increased over the previous five years and said that they were concerned about it.
- Illinois, Louisiana, Idaho and Texas have enacted laws specifically outlawing violence committed during a religious ritual.
- The Los Angeles County Commission for Women has produced, at taxpayers' expense, a handbook called "Ritual Abuse." It says Satanists "frequently function together in groups in the operation of preschools, day-care services and baby-sitting services." The handbook was a product of the commission's Ritual Abuse Task Force, whose job is to warn the public, therapists and the police of the signs of Satanic abuse, said Myra B. Riddell, the task force chairwoman. Last year 7,500 copies were distributed in the United States and Canada. Ten thousand more were printed in March.
- There is a private agency in Rialto, in San Bernardino County, called the Ritualistic Crime Task Force, that serves as an information clearinghouse. In October it held a press conference in Los Angeles to warn parents that devil-worshipers were plotting to kidnap and sacrifice trick-or-treaters on Halloween. (None did.)
- In 1988, when Geraldo Rivera devoted a program to "Exposing Satan's Underground," Americans in 19.8 million homes tuned in. It was the highest-rated documentary ever aired on NBC.
- Organizations give law-enforcement seminars on ritualistic crime. Speakers discuss everything from the game Dungeons and Dragons to human sacrifice. The privately funded Cult Crime Impact Network in Boise, Idaho, is a clearinghouse on supposed Satanic crimes. It publishes a newsletter with 2,000 subscribers — mostly, it says, police officers.
- Two researchers at Texas A&M University sampled the attitudes of 153 police officers who had attended a seminar on cult crime or subscribed to the Cult Crime newsletter. The consensus among the officers was that Satanism is responsible for one in 10 homicides and one in three teen suicides.

No one has comprehensive statistics on the self-proclaimed survivors of ritual abuse. But believers and scoffers agree that their numbers reach into the thousands. Balodis said that a support group she started hears from at least 40 new "survivors" a month. She said that she knows of at least 500 in Los Angeles.

Sandi Bargioni, a San Francisco police officer who specializes in ritualistic crime, said that she has received scores of calls from women claiming to have been Satanically abused as children. Not one of the stories could be proven, she said, and she is among the skeptics.

So is Kenneth Lanning, who works in the FBI's Behavioral Science Unit in Quantico, Virginia. Considered an expert in cult crime, he has advised police departments on more than 300 cases, many involving survivor tales.

"In the early '80s, the first few times my phone rang, I was inclined to believe it," he said. Then the cases began piling up. There were lots of reports of cults, but no bodies. Lanning said that airplanes with heat-seeking equipment sought out mass graves on the theory that decomposing bodies would give off heat. None was found. Lanning stopped believing.

"What are the probabilities of this?" he said. "Two or three people in Southern California may be able to do this a couple of times and get away with it." But when all the claims of Satanic sacrifice were added up, it amounted to thousands of people murdering thousands more.

Believers say that no evidence is uncovered because the Satanists are so clever. The county's "Ritual Abuse" handbook puts it this way: "Explanations for the absence of found remains include cannibalism, cult access to mortuaries and crematoria, frozen storage of body parts, and the retention by cult members of bones and body parts for further magical practices."

Lanning says that disposing of bodies is not as easy as some people think, and some remains should have been found if cults were systematically sacrificing people.

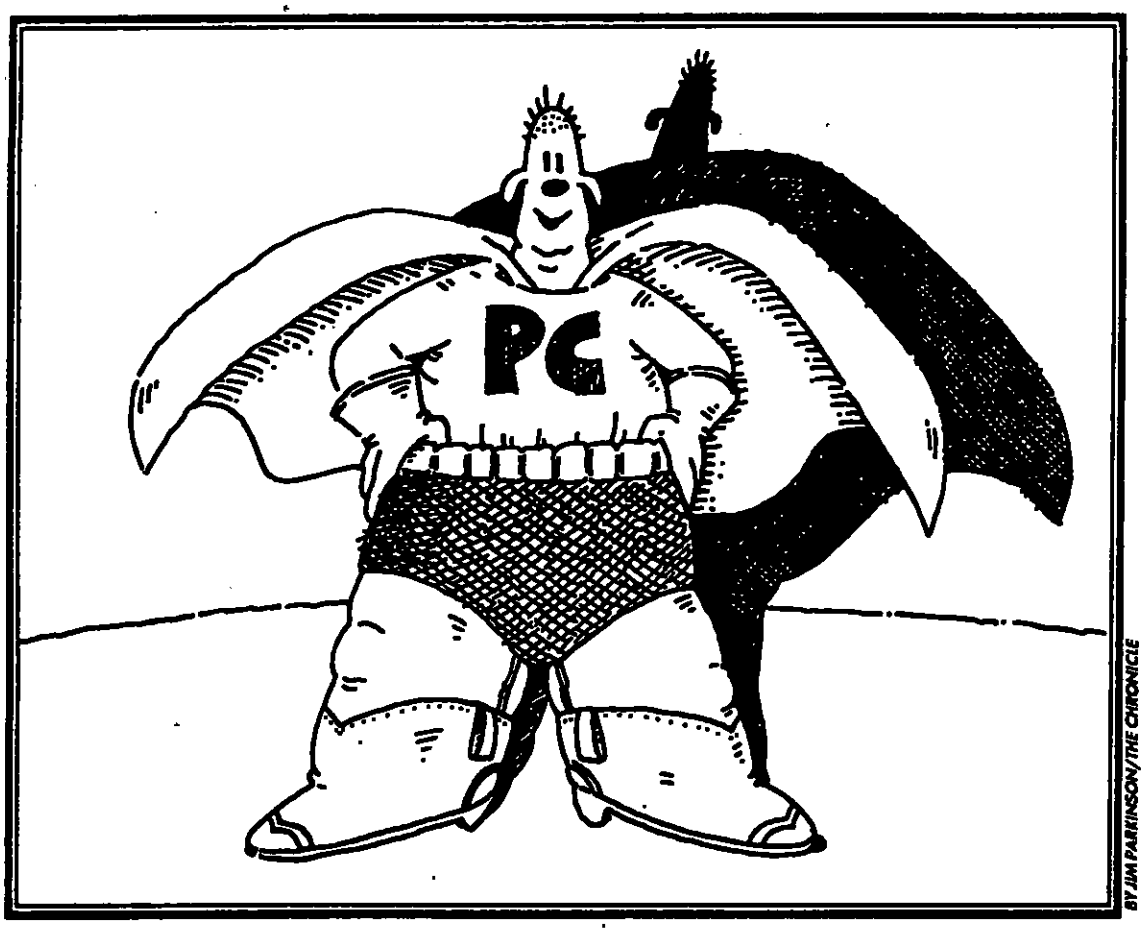
Despite the expert opinion against them, the "survivors" draw support from several sources. Foremost are fundamentalist Christians. The major publishers and producers of books and videos dealing with Satanism have strong fundamentalist ties. Hal Lindsay, author of the best-selling "The Late Great Planet Earth," has been a major supporter of survivors and has linked the rise in Satanism to the Last Days prophesied in the Book of Revelation.

J. Gordon Melton, director of the Institute for the Study of American Religion in Santa Barbara, dismisses the stories as mostly distorted memories of childhood sexual abuse.

If the stories are true, he said, "this means a generation ago there were at least 400 or 500 Satanist groups in the country, functioning, doing things and able to keep their existence not just hidden, but even hidden from the rumor mill. That, to me, is pretty far-fetched." □

Are You Right, or Are You Correct?

Language
WILLIAM SAFIRE



BY JIM PARKINSON/THE CHRONICLE

What does "PC" stand for?

If your impulse is to blurt out "personal computer," you have gone software in the head. If those letters evoke memories of the Peace Corps, you are antediluvian (from "before the Flood," which makes you at least as old as Noah). A percentage of postcards from hypochondriacs will insist that the initials stand for the Latin direction *post cibum*, "after meals," the only digestively conducive time to pop certain pills.

Those of us with slanguistic *Fingerspitzengefuehl*, however, know that the initials stand for the most controversial phrase on college campuses today: *politically correct*. In "Thatch," a comic strip by Jeff Shesol of Brown University, a heroic character slips on a cape and supermanly tights with "PC" emblazoned on his chest. It's not a nerd, it's not a plane, it's ... Politically Correct Person!

Ralph Waldo Emerson held in 1841 that "Whoso would be a man must be a non-conformist." That use of *man* today, in the sense of "one who possesses what were considered 'manly' virtues, like intellectual independence and moral courage," is rightly taken to be sexist; whoso would be a conformist must be *politically correct*.

"There is a new McCarthyism that has spread over American college campuses," writes Max Lerner, an old-line liberal. "We call it 'political correctness.'" The new Random House Webster's College Dictionary (the use of Webster in the name of a dictionary is a form of marketing correctness) defines the term as "marked by or adhering to a typically progressive orthodoxy on issues involving especially race, gender, sexual affinity or ecology."

I would edit that definition to denote *politically correct* as "an adverbially premodified adjectival lexical unit used to attack liberal conformity on sexual, racial, environmental and other voguish issues." (Maybe I should write a dictionary titled "*Not* Webster's.")

Item: "At the State University at Binghamton," Frank Herron wrote in the Syracuse Herald-Journal in March, "a meeting of a group formed to resist the pressure to conform to 'politically correct' speech was crashed by about 150 students, some carrying sticks."

Distantly related item: "A professor at the University of California at Santa Barbara noted that *pet* had become a derogatory term," wrote Stephanie Schorow of the Associated Press, "at the insistence of animal rights activists. The politically correct term was now *companion animal*." When the professor facetiously wondered if some magazine centerfold models, now called *Penthouse* Pets, would soon be called *Penthouse Companion Animals*, 15 women promptly filed sexual harassment charges.

Linguistically sensitive *Newsweek* warns students: "Watch what you say. There's a politically correct way to talk about race, sex and ideas." *The New Republic* rejects that discipline, seeing "the imposition of political correctness" as meaning "our universities, which should strive for an identity in contradistinction to the world at large, have become distillations of our bitterest social divisions."

The first citation I can find for the incendiary phrase dates from a December 1975 statement by Karen DeCrow, then president of the National Organization for Women. She claimed that a dissident faction felt that feminism was only for "white, middle-class, straight women" and insisted NOW was moving in the "intellectually and *politically correct* direction." The phrase began as an assertion by liberal (progressive, concerned) activists and then was turned into an attack phrase by conservative (right-wing, heartless) passivists.

The first word in the phrase is a "premodifier" — an adverb that modifies and then fuses with an adjective to form a compound modifying a noun. (I learned this at a thinly veiled, hastily called news conference.) As Quirk, Greenbaum, Leech and Svartvik note in their "Grammar of Contemporary English," such adverb premodifiers often express viewpoints: *politically expedient, artistically justifiable, economically feasible, theoretically sound, ethically wrong*, and as girls from Brooklyn said of boys from Bronx Science, *geographically undesirable*. Of all these married modifiers, *politically correct* has become the most tightly wedded.

The origin is in *correct thinking*. "Where Do Correct Ideas Come From?" was the title of a 1963 thought by Chairman Mao Zedong, one of those later collected in a little red book that sold in numbers that still make publishers sigh. The chairman thought on: "Do they drop from the skies? No. Are they innate in the mind? No. They come from social practice, and from it alone."

The Maoist phrase was also translated as *correct thinking*, as shown in this 1977 use by Kenneth Turan of the Washington Post on the glories of Dr. Brown's Cel-Ray tonic: "This beverage not only quenches your thirst ... but serves as a talisman and a cultural rite as well, a sign of goodness and correct thinking that even Chairman Mao would have appreciated."

To dedicated Communists, *correct thinking* was "the disciplined inculcation of a party line expressed in all forms of social and political intercourse." When it was adopted self-mockingly by conservatives in the United States, it meant usually "one of us." The columnist George F. Will described Irena Kirkland in 1985 as "a life-affirming person and one of Washington's dozen or so Correct Thinkers."

To both left and right, then, *correct* came to mean "reflecting the opinions of the group"; in the late '80s, when the right went after the conformity of the left on college campuses, the affirmation of *politically correct* became an epithet.

Briefly now to the issue of vocabulary vigilantes who try to enforce "correct" language. Examples of taboo-boos can be found in the list compiled by fellows at the University of Missouri Multicultural Management Program: *feminine* "can be objectionable to some women"; *codger* or *geezer*, "an objectionable reference to a senior citizen"; *Jew*, "some people find use of *Jew* alone offensive and prefer *Jewish person*"; and *swarthy*, "avoid all unnecessary references to skin color, such as yellow."

A Syracuse law student, Dennis F. Chiappetta Jr., notes in a recent letter about all such lingopolicing: "From what I can see, the end they seek is the removal of all language that brings to anyone's mind a negative or in any form degrading image. Is this possible? Can any language be written so 'correctly' as to invoke only pleasant or neutral feelings?"

My correspondent, a profound rather than correct thinker, follows up: "With the removal of terms of derision, will the prejudices also disappear — or will these new terms adopt connotations that users of the old terms may have seen in those terms?"

The opinions of Lex Irregs are solicited; we'll limit the debate here to specific choices of words rather than diatribes about "correct" subjects and attitudes.

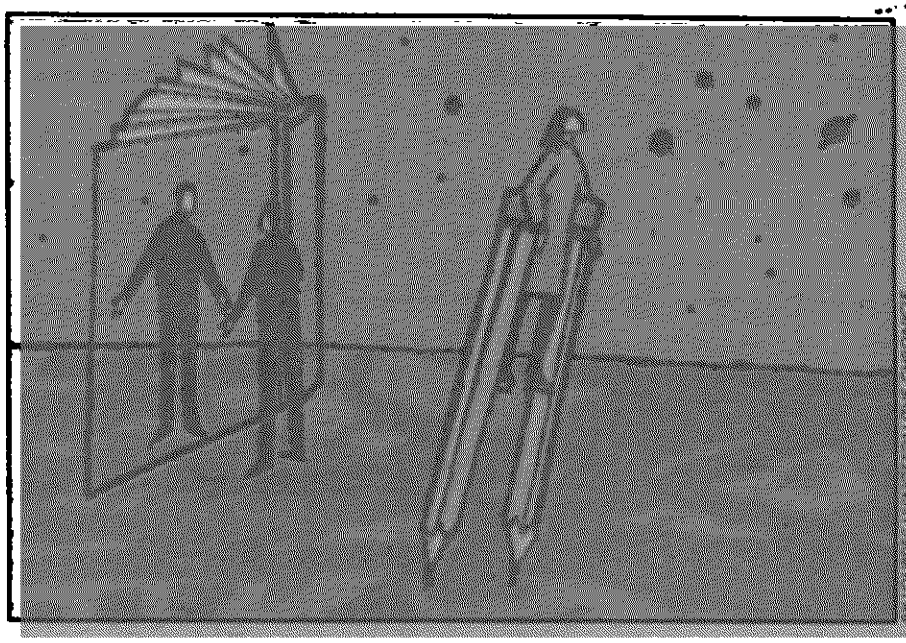
Some words of derision hurt; they should be identified as slurs in at least one sense and avoided. Others — from *pert* and *petite* to *soulful* and *wannabe* — are getting a bad rap from the hypersensitive. The communication question to be asked is not "Could this possibly offend?" but "Does this get the intended point across?" ■

New York Times

SYLVIA

Clark Brown

Teaching: Whatever Works



How should we teach? How should we learn? In these times — perilous for education — who has the answer?

My eighth grade history teacher, a flinty old horror, never gave an A. "Read Chapter Three," she would say, "and we'll have a test tomorrow." We would read Chapter Three and flounder through the exam. The truly gifted might scramble toward a B minus, but most of us wallowed in the marshes of C and D. A few sank from sight.

One night, however, after I had read the assigned chapter, a sinister voice seemed to whisper in my ear. "What if you read the chapter *again*?" it slyly asked. I was shocked. We hadn't been instructed to do anything of the kind. Still, I reread the material and found it much clearer and memorable. Then the serpent hissed a second time. "What if," it suggested in its devilish way, "you went through and looked for questions *she* might ask?"

I began to tremble. My audacity had limits. But I embraced the powers of darkness, and at once potential questions leaped off the page — or rather the answers did; it was a little like playing "Jeopardy."

The next day, to my amazement, "my" questions appeared on the test, and I answered with obscene ease, astonishing the class with the first A anyone could remember the old gal yielding. Affecting an astonishment of my own, I put my success down to luck, but I wasn't being falsely modest; I was scared, frightened that if my diabolical secret became known I would be exposed as a cheater and flunked, or even expelled.

The ironies here are obvious and funny, at least to me. I had learned to study, though I didn't know that's what it was called, and I was covered with guilt — something like the kids in "The Dead Poets Society" who defiantly "rebel" by sneaking into the woods and reading Tennyson! But what if the teacher had *told* us to reread and look for possible questions? It wouldn't have worked. We would have stared at her blankly and gone on as before.

Students think that teachers speak in code, that "Please pass the salt" is a request for pepper. And by forever trying to figure teachers out, students overlook or complicate what should be plain and simple and clear, which drives teachers wild, though I suppose we get used to it.

Clark Brown teaches English at California State University, Chico, and is the author of 'The Disciple,' a novel.

By forever trying to figure teachers out, students overlook or complicate what should be plain and simple and clear, which drives teachers wild

Recently, I signed on to read several hundred essays by students aspiring to credit for a college course they hadn't taken. Again and again the hopeful writers avoided the directions and supplied offerings neither wanted nor asked for, until I began to feel a smothered exasperation. "Look," the schoolmarm in me wanted to say. "You chose to take this test; you didn't have to. Don't you *want* to pass? Why don't you do what you're asked to?" But actually I knew.

Teachers do speak in code because they have to, because they know that the real learning you have to do for yourself, sometimes against the grain; that even Tennyson has to be appropriated, possibly by stealth. So the great teachers seem to cultivate a Zen-like talent for eluding the conventional. They come at us obliquely, as in Timothy Gallwey's *Inner Game of Tennis* story of the flustered pupil — a grown man — answers. "What was that you asked?" Neill said, pretending to misunderstand. "Where do babies come from?" No, the boy protested in fury; he didn't want to know that — and out he stormed, only to return. All right, where *did* they come from? Neill told him, and the questions stopped.

To make us conscious of ourselves, then, the true state of our backhand or our psyche — or what we really want to know — that must be the blessing a fine teacher can give if perceptive enough, understanding that students too speak in code, like the Summerhill boy. Only, is that awareness always such a gift?

In the first grade, I, age 5, was made to stand beside my desk and sing from a songbook; then I was graded — F in this case, since I couldn't carry a tune (nor can I now). The grade was perfectly just, but what was the point? I can tell you the effect — a lifelong inhibition where music is concerned, an inability to enjoy or pursue the stuff except in a fitful and superficial way.

Well, at least we can agree that a teacher should be open, helpful, friendly, encouraging — right? I wish it were that clear, but I keep remembering the time I helped read 300 essays by prospective teachers challenged to describe a teacher of theirs, and to tell why they would or wouldn't emulate such. Paper after paper celebrated all sorts of humane, liberal, kindly virtues, but only one rose above mediocrity. The single essay that could fairly be called "good" came from a student who had been taught to write by some harridan of a nun who screamed and rapped knuckles with a ruler. This student too intended to be humane and helpful and unintimidating — admirable resolves, I guess, but you had to wonder. The whole thing called to mind the Catholic priest who, defending the rod, told me with gloomy resignation, "We find the boys don't like to learn."

I and Aristotle wouldn't like to think so, but I admit to playing football for a high school coach who cursed and slapped us and once decked a refractory lineman. Though dubious as a role model, the man won a lot of games, taught us a good deal of football and produced in us a certain nimble alertness. As George Orwell said, writing of his prep school days, it's a mistake to think such methods don't work. They work very well — for their purposes.

The simple truth seems to be that there is no simple truth. I know how a low grade or unkind remark can rouse some students to furious endeavor and unimagined progress, but I remember others who were like stones until given a little encouragement. There was the young Hispanic who at the semester's end asked if he might hug me (I said he might), so grateful was he that I had let him feel he wasn't a complete idiot. Possessed at last of a little confidence, he had started to blossom.

On the other hand, there were my Stanford minority students who found praise a threat and success a terror, and committed a sort of academic suicide, drifting away not because they couldn't make it in this alien world but because they could — and feared that in so doing they betrayed their roots and falsified their identity.

There's much to be said for removing frustrations and obstacles, and much to be said for installing them. When to be cold-hearted? When sympathetic? When to act shrewd and wise, and when to put on that calculated obtuseness A. S. Neill wore so effectively? When to let the whole student/teacher distinction dissolve? When to sharpen and strengthen it? I wish I knew. And all the while I've been talking as though the application of the proper technique will produce some desired and predictable result, which is nonsense.

In fact, whenever I hear of some book or film or classroom strategy guaranteed to have splendid effects, I think of Anthony Burgess' *A Clockwork Orange* and the juvenile hood who in the interests of reform is given the Gospel and urged to read of Christ's Passion. The boy does so and enjoys fantasizing about wearing a toga and directing the Scourging and Crucifixion.

We have to face it. Learning and teaching are explorations, and explorations by their very nature carry us into the unknown. So a misguided attempt to discover the absolute motion of the Earth leads in a roundabout way to the realization that mass is a form of energy — that is, speculations about the Earth's movement give us Hiroshima and Nagasaki, which no one could have foretold. The universe isn't just queerer than we suppose, said a famous scientist. It's queerer than we *can* suppose.

And we are a part of that universe, and little universes ourselves — spheres, Emerson claimed, that touch only at the points. Here is the real crisis in education, but also what makes it exciting. *We* are the problem, you and I, complicated, unpredictable, perverse, alternately rebellious and docile human beings, certain to modify and very likely overturn all strategies for our improvement. Surely, the prospect of trying to educate such creatures is daunting — but also exhilarating.

Rabelais, imagining his ideal school, chose as its motto, "Do What You Would." I, less sanguine but hopeful still, will take my slogan from Kafka: "Nothing alive can be calculated." ■

ville", Grant. Most of the charges revolved around interstate transport of stolen material worth more than $5000, fraud, and conspiracy. All equipment was of course seized. Ostensibly, the charges carried 40 years in jail and a $2 million fine. On July 9, they pleaded guilty in exchange for suspended sentences. They've agreed to help Bell South fortify its system security.

On March 1, the Secret Service visited Steve Jackson Games of Austin Texas. They turned the place upside down, destroying office furniture, cutting locks, and carried out three computers, a laser printer, various piece parts, and all the paper and diskettes they could find. Their warrant was not signed by any judge and was obtained under seal. It stated only that they were looking for evidence related to data piracy.

Steve Jackson Games publishes games oddly enough. Dungeons and Dragons is perhaps the most widely known of a genre of fantasy games termed Role Playing Games, or RPG. Steve Jackson Games is a rather successful publisher of role playing games. The games do not even run on computers. They tend to be rather complicated books of rules that are played almost entirely on pencil and paper with the aid of dice. These RPG do seem to attract people who become obsessed with them. But that is not the reason for the Hunnish intrusion by the Secret Service.

The managing editor at Steve Jackson Games was a gentleman named Loyd Blankenship. The game of interest to the Secret Service is titled ***GURPS, Cyberpunk.*** GURPS stands for Generic Universal Role Playing System. The game is ABOUT breaking into mythical computers. There are no tips or tricks contained therein for doing so. In fact, whether a player "cracks" a computer in the game or not is strictly a function of a role of the dice. The Cyberpunk game revolves around a dystopian science fiction future evoking a picture of George Orwell in frightful collaboration with Ray Bradbury. The game is almost prophetic in that the future implied pretty much visited Steve Jackson Games this past March 1. According to Steve Jackson, "You couldn't break into a computer using this book to save your life. You can learn more about unauthorized entry into a computer from Clifford Stoll's book ***Cuckoo's Egg***, than you possibly could from GURPS CyberPunk. This is a role-playing game based on dice."

So why the intrusion? There are a couple of theories. Loyd Blankenship did strive to impart the flavor of the hackers world in the game and did in fact assume an online handle of "The Mentor". He attempted to contact members of the Legion of Doom to do some background research on the subject of hacking in general to make the game somewhat realistic.

There are also persistent rumors that the Secret Service is running a program to download massive amounts of data and message traffic from computer bulletin board systems. They then search for keywords pertaining to hacking, phreaking, and online crime. According to Jackson, they would have hit the jackpot there on his BBS, Illuminita (512)447-4449. They had some early drafts of GURPS Cyberpunk online. Lots of keywords. No real tips on hacking.

But one of the terribly techni[illegible] competent Secret Service agent[illegible] tion during the search th[illegible] ered Cyberpunk to b[illegible] computer crime." They also alluded to the fact that they had to take the laser printer to examine the "ribbon".

On June 21st, all the equipment and most of the data was returned to Steve Jackson Games. According to Jackson several pieces were somewhat badly damaged. He doesn't think it was necessary malicious. It appeared to be just gross mishandling. The escapade delayed the introduction of GURPS CyberPunk for six weeks. The episode cost Jackson about $125,000 by his figures. No charges were filed. And they still haven't determined what led to the search warrant. They were simply told it was filed under seal.

In all, 27 warrants were served in 14 cities and 40 such computer systems were confiscated in the May "raid". We haven't yet run across an account of anyone in that particular raid actually committing any crimes and none from the May sweep have been charged. Stories of incredible technical ignorance/ineptitude among the 150 agents involved continue to surface. The story emerging seems to be one of innocent online communicators such as Andrews and Jackson abused by a system gone wild in a frenzy of online witch hunting. We have not yet confirmed reports circulating of households searched while held at gun-point, choke holds on suspects, etc. These stories can perhaps be embellished as they are repeated. We'll try to turn up the facts as we can. Again, even with fairly wide online contacts the going is slow. The real professionals at the larger publications clearly have techniques in the online world we've yet to discover in order to be able to come up with such a quantity of misinformation so quickly.

But there is a counter movement coming to play. It seems that John Barlow had received a visit from an Agent Richard Baxter Jr. of the FBI. Apparently, a group called the NuPrometheus League, comprised of ex-Apple computer employees, had access to the source code for the Macintosh operating system. They posted a small section of it pertaining to the Color QuickDraw function on several BBS. This supposedly sent John Sculley into a fit of apoplexy and he called in the FBI to investigate. Agent Baxter, armed with an impressive array of misinformation from Apple, was canvassing attendees of the annual Hacker's Conference. It seems he was told by Apple that the Hacker's Conference was a hotbed of computer crime. Actually, the Hacker's Conference largely uses the term Hacker in the earlier computer hobbyist sense. It originated in 1984 as an annual convention sponsored by the Point Foundation and The Whole Earth Review. The Whole Earth Review is in some sense the parent organization of The Whole Earth Lectronic Link (THE WELL) a popular Unix based online service.

Each year, about 100 luminaries from the personal computer world are invited to attend, including the likes of Mitch Kapor, Steve Jobs, Steve Wozniak, Bill Gates, etc. - the people who ushered in the personal computer.

According to Barlow, Baxter didn't know a ROM chip from a vice grip, had no idea what source code was or how it could be distributed online, and thought that from the Color QuickDraw segment, millions of clone Apples were about to spring forth from the earth and put Apple Computer out of business. John Draper was ostensibly the CEO of

Autodesk, another heavy in the world of online crime. Autodesk is actually the developer of AutoCAD and John Draper has never been CEO of anything we're aware of. And Baxter was further convinced that the title of the NuPrometheus League was actually the New Prosthesis League.

Back on THE WELL, Barlow engaged in some discussion of this matter with Mitch Kapor, head of Lotus Development. Mr. Kapor actually landed his corporate jet in Pinedale Wyoming to visit Barlow and spent the afternoon listening to such tales of terror. His response was rather swift and convincing. The pair called in the New York law firm of Rabinowitz, Boudin, Standard, Krinsky, and Lieberman. This led to further meetings with some of the victims of the May raid. Out of this, they formed a group titled the Electronic Frontier Foundation dedicated to raising and disbursing funds for education, lobbying, and litigation in the area of extending our constitutionally guaranteed freedoms to the online world.

After Kapor's plans for the Electronic Frontier Foundation were announced in the press, Steve Wozniak, one of the original inventors of the Apple computer, called to announce he would match Kapor "dollar for dollar" in supporting the group. John Gilmore, one of the founders of SUN, likewise joined the group. A number of other luminaries from the origins of personal computers are reportedly jumping into the fray.

Both the general and the trade press have been universally unkind to Mr. Kapor and his stand on this issue. There is little in the way of sympathy for the stereotypical "hacker". One cartoon shows Kapor holding a freedom banner aloft with the aid of a teenage BBS operator. The next panel shows Kapor attacking the kid after he learns that 1-2-3 is available for download on the lad's BBS. We've never seen a copy of 1-2-3 available for download and by and large the BBS community does a pretty good job of policing itself with regards to software piracy. The panel is typical of the type of uninformed drivel we've seen regarding this issue.

It would seem that everyone is for freedom as long as it's for a good cause. The online world is being universally painted with a rather dark brush and freedom is somewhat less important when applied to THOSE people - always more dear when applied to ourselves. The heart of the problem lies in the rampant lack of technical understanding of the online world in our law enforcement bodies, which is somewhat understandable if not acceptable, and the apparent similar lack of knowledge among the trade press, which is NOT understandable and certainly not acceptable. Against such a tidal wave of misinformation and misplaced sentiment, Mr. Kapor's stand would seem enormously disadvantageous to himself and to his company.

Doing "the right thing" as you see it is not so very hard. Doing the right thing when there is little in it for you, and a

great deal of potential harm, is a mark of personal heroism all too rare in our present world. Salute.

Those wishing to join the effort may contact the Electronic Frontier Foundation, 1 Cambridge Center, Suite 300, Cambridge, MA 02142; (617)577-1385 voice; (617)225-2347 fax. Internet address: eff@well.sf.ca.us

INTERNET LINKING UP THE E-MAIL WORLD

For years the chant has been the same. "I would use e-mail, but it seems whoever I would want to send a message to is always on a different e-mail service." It has become a legend of our times that e-mail is inherently made up of islands of service. You can send a message to someone else on the same service instantly. You can't send a message to anyone on another service at all.

Recently, there has been much ado about linking the major e-Mail services using the CCITT X.400 standard. X.400 is a curious animal. It was primarily intended as a standardized ADDRESSING method to allow e-mail links between different services. It hasn't worked out that way. Instead, most of the e-mail services have taken the more esoteric technical elements of X.400 and used them to electronically link their services. Unfortunately, the concept of a universally standard addressing method, or user interface, has been tossed out the window. All services have their own interpretation of what X.400 means and you will notice few similarities between the services.

But e-mail will never reach its full potential in linking services. It must eventually link desktops. A method of addressing must be devised that is rational as well.

While all the X.400 brouhaha was going on, it would appear that an organization titled INTERNET snuck into the switching room and hooked us all together without telling anybody. This minute, from virtually any Fidonet BBS system in the country, you can easily send an e-mail message to another person, not only within Fidonet, but throughout the Unix world and on most public e-mail services as well, including MCI Mail, CompuServe, AT&T E-mail, and Sprint Mail. Best of all, it is essentially FREE and there is currently no effective machinery for charging for it at all.

The key to all of this is Unix. The Unix world is just a bit bizarre. The operating system was created with communications in mind and it does do a credible, if uninspired job of networking through the Unix-to-Unix Copy Program (UUCP). Over the years, a number of government agencies, universities, and private companies have linked together their relatively expensive Unix minis into a hodgepodge of networks.

USENET is simply an impromptu network of some 20,000 Unix machines in 40 nations with roughly a million users connected using UUCP, or its DEC VMS counterpart, to pass mail. Anyone with a Unix machine in their business, and even some individuals who run small Unix BBS systems can be connected to Usenet simply by finding an existing Usenet system willing to allow the connection. USENET News Groups are shared topical message areas similar to Fidonet echomail conferences. There are probably 600 Usenet News Groups covering everything from happenings in China to Rock N' Roll with a few covering neural nets and child care.

In the past, you could conceivably send a message from any Unix machine to any Unix machine on any of the networks. The problem was that you had to know the PATH. Path addressing was the paragon of obtuse, indecipherable messaging. In the address itself, you had to provide a complete routing instruction specifying every machine in the link from the sending system to the receiver. Individual stops were separated by an exclamation point, usually termed a bang. The entire scheme was called bang-path addressing and very few could actually master it. Once two individuals "found" each other, they conventionally saved the bang path in a macro file or other hideaway to whip out if the need arose.

In recent years, this has improved dramatically using name domain addressing. Essentially, the address consists of the user name, the @ symbol, and the

8. Law Enforcement & Civil Liberties **83 mins.**
Interaction of computer crime, law enforcement and civil liberties; issues of search, seizure and sanctions, especially as applied to networked information, software and equipment. Chair: Dorothy Denning.

SHELDON T. ZENNER Atty, Katten, Muchin & Zavis, Chicago

KENNETH ROSENBLATT Deputy District Attorney, Santa Clara County D.A.'s Office

MITCHELL KAPOR Pres., Electronic Frontier Foundation

MIKE GIBBONS Supervisory Special Agent, Federal Bureau of Investigation

CLIFF FIGALLO Executive Director, The WELL

SHARON BECKMAN Atty, Silverglate & Good, Boston

MARK RASCH Trial Attorney, U.S. Dept. of Justice

9. Legislation & Regulation **82 mins.**
Legislative and regulatory roles in protecting privacy and insuring access; legal problems posed by computing and computer networks; approaches to improving government processes; limits on legislation. Chair: Bob Jacobson

CRAIG SCHIFFRIES Congressional Science Fellow, Subcommittee on Technology & the Law, Senate Judiciary Committee

BILL JULIAN Chief Counsel, Utilities & Commerce Committee, California State Assembly

JERRY BERMAN Director, Information Technology Project, American Civil Liberties Union

PAUL BERNSTEIN Atty, LawMUG BBS & Electronic Bar Assn. Legal Information Network

ELLIOT T. MAXWELL Asst V. Pres. for Corporate Strategy, PACIFIC TELESIS

STEVE McLELLAN Policy Strategist, Washington Utilities & Transportation Commission, Olympia

10. Computer-Based Surveillance of Individuals **90 mins.**
Monitoring of electronic mail, public & private teleconferences, electronic bulletin boards, electronic "publications" and their subscribers; computer-aided monitoring of individuals, work performance, buying habits and personal lifestyles. Chair: Susan Nycum.

JUDITH F. KRUG Dir., Office for Intellectual Freedom American Library Association
KAREN NUSSBAUM Executive Director, 9 to 5 National Association of Working Women

GARY T. MARX Prof. of Sociology, Massachusetts Institute of Technology

DAVID H. FLAHERTY Prof. of History & Law, Social Science Ctr., Univ. of Wstrn. Ontario, Canada

11. Security Capabilities, Privacy and Integrity **69 mins.**
Chair: Dorothy Denning.

WILLIAM A. BAYSE Asst. Dir., Technical Svcs., Federal Bureau of Investigation, Washington D.C.
"NCIC - 2000: Balancing Computer Security Capabilities with Privacy and Integrity"

12. Electronic Speech, Press & Assembly **91 mins.**
Freedoms of electronic speech, public & private electronic assembly & electronic publishing; issues of prior restraint & chilling effects of monitoring on freedoms; possible justifications for monitoring; alternatives. Chair: Eric Lieberman.

LANCE ROSE Atty., Wallace & Rose, New York City

JACK RICKARD Editor, BOARDWATCH MAGAZINE, Boardwatch Online Information Service

GEORGE PERRY V. Pres. & General Counsel, PRODIGY SERVICES CO.

JOHN McMULLEN Consultant & Journalist, NEWSBYTES, and McMullen & McMullen, Inc.

ERIC LIEBERMAN Atty, Rabinowitz, Baudin, Standard, Krinsky & Lieberman, New York City

DAVID HUGHES Electronic Citizen & General Partner, Old Colorado City Communications

13. Access to Government Information **89 mins.**
Implementing individual & corporate access to federal, state & local information about communities, corporations, legislation, administration, the courts & public figures; allowing access while protecting privacy. Chair: Harry Hammitt.

HARRY HAMMITT Editor & Publisher, ACCESS REPORTS, Inc

KATHERINE F. MAWDSLEY Associate University Librarian, University of California at Davis

DAVID BRIGHT BURNHAM Co-Director & Writer, Transactional Records Access Clearinghouse

ROBERT VEEDER, Acting Chief, Information Policy Branch, Office of Information Regulatory Affairs, US Office of Management & Budget, Washington D.C.

14. Ethics & Education **83 mins.**
Ethical principles for individuals, system administrators, organizations, corporations and government; copying of data, copying of software, distributing confidential information; relations to computer education & computer law. Chair: Terry Winograd.

DOROTHY DENNING Systems Research Center, DIGITAL EQUIPMENT CORPORATION

DONN B. PARKER Senior Management Consultant, SRI INTERNATIONAL

RICHARD HOLLINGER Assoc. Professor, Dept. of Sociology, University of Florida

JOHN GILMORE Generalist, Cygnus Support

JONATHAN BUDD Pgrm Mgr, Law Enforcement Computer Crime, National Institue of Justice

SALLY BOWMAN Dir., Computer Learning Fndtn.

15. Where Do We Go From Here? **83 mins.**
Perspectives, recommendations and commitments of participants from differing interest groups, proposing next steps *they* will pursue to protect personal privacy, protect fundamental freedoms and encourage responsible private-sector and public-sector policies and legislation. Chair: Jim Warren.

PAUL BERNSTEIN Attorney, LawMUG BBS & Electronic Bar Association

MARY J. CULNAN Assoc. Professor, School of Business Administration, Georgtown University

DAVID HUGHES Managing General Partner, Old Colorado City Communication

DON INGRAHAM Assistant District Attorney, Alameda County District Attorney's Office

MITCHELL KAPOR President, Electronic Frontier Foundation

ERIC LIEBERMAN Atty., Rabinowitz, Baudin *et al*

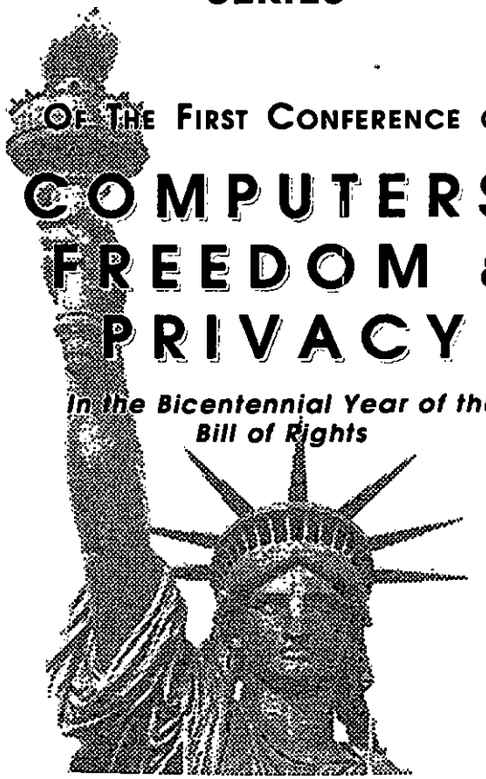
DONN B. PARKER Senior Management Consultant, SRI International

CRAIG SCHIFFRIES Congressional Science Fellow, Subcommittee on Technology & the Law, Senate Judiciary Committee

ROBERT VEEDER Acting Chief, Information PolicyBranch, Office of Information Regulatory Affairs, US Office of Management & Budget

The Complete

VIDEO LIBRARY SERIES



OF THE FIRST CONFERENCE ON

COMPUTERS, FREEDOM & PRIVACY

In the Bicentennial Year of the Bill of Rights

PURSUING POLICIES TO SAFEGUARD AMERICAN FREEDOMS IN THE INFORMATION AGE

THE VIDEO LIBRARY SERIES OF

Of The First Conference on

COMPUTERS, FREEDOM & PRIVACY

CONTENTS

Co-sponsors & cooperating organizations: *Institute of Electrical & Electronics Engineers-USA; Association for Computing Machinery; Electronic Networking Association; Electronic Frontier Foundation; Videotex Industry Association; Cato Institute; American Civil Liberties Union; ACM Special Interest Group on Software; IEEE-USA Intellectual Property Committee; ACM Special Interest Group on Computers & Society; ACM Committee on Scientific Freedom & Human Rights; IEEE-USA Committee on Communications & Information Policy; Apple Computer, Inc.; Autodesk, Inc.; Portal Communications; The WELL*

Sponsored by Computer Professionals for Social Responsibility

Coordinated by Jim Warren

Video production & distribution by
Patric Hedlund Gary Meyer
COMPUTERS, FREEDOM & PRIVACY
VIDEO LIBRARY PROJECT
P.O. Box 912 • Topanga • CA 90290
(213) 455-3257

1. The Constitution in the Information Age 75 mins.
Policy proposals regarding constitutional protections, networked computers and electronic communications.
Chair: Jim Warren

LAURENCE H. TRIBE Professor of Constitutional Law, Harvard University Law School *"The Constitution in Cyberspace: Law & Liberty Beyond the Electronic Frontier"*

2. Trends in Computers & Networks 90 mins.
Overview and prognosis for computing capabilitites and networking as they impact personal privacy, confidentiality, security, one-to-one and many-to-one communications, plus access to information about government, business, technology and society. Chair: Peter Denning.

PETER J. DENNING Research Institute for Advanced Computer Science
"Computers Under Attack"

JOHN S. QUARTERMAN Texas Internet Consulting
"The Matrix as Volksnet"

PETER G. NEUMANN Computer Science Lab, SRI INTERNATIONAL
"Computers at Risk: The NRC Report and the Future"

MARTIN E. HELLMAN Prof., Stanford University
"Cryptography and Privacy: The Human Factor"

DAVID CHAUM Prof., Amsterdam
"Electronic Money and Beyond"

DAVID J. FARBER Prof., Computer & Information Sciences, University of Pennsylvania
"Will the Global Village be a Police State?"

3. International Perspectives & Impacts 75 mins.
Other nations' models for protecting personal information and communications, and for granting access to government information, including the European Community's 1992 trans-border data flow and accountability issues; implications for privacy and personal expression.
Chair: Ron Plesser.

ROBERT VEEDER Acting Chief, Information & Policy Branch, Office of Information Regulatory Affairs, US Office of Management and Budget, Wash. D.C.

TOM RILEY Canadian Specialist in International Computer Privacy Issues

DAVID H. FLAHERTY Prof. of History & Law, Social Science Center, Univ. of Wstrn. Ontario, Canada

RONALD L. PLESSER Atty., Piper & Marbury, Gen. Counsel, US Privacy Protection Study Commission

4. Personal Information & Privacy - I 75 mins.
Government and private collection, sharing, marketing, verification, use, protection of, access to and responsibility for personal data, including, lifestyle, work, health, school, census, voter, tax, financial and consumer information.
Chair: Lance Hoffman.

JANLORI GOLDMAN Dir. of Project on Privacy & Technology, American Civil Liberties Union

JOHN BAKER Sr. V. Pres., Consumer & Government Affairs, EQUIFAX, INC.

DEBATE: Should individuals have absolute control over secondary use of their personal information?

ALAN F. WESTIN Prof. of Public Law & Government, Dept. of Political Science, Columbia University, NYC

MARC ROTENBERG Washington D.C. Director, Computer Professionals for Social Responsiblity

5. Personal Information & Privacy - II 75 mins.
Ethics of "Strip Mining Data" for resale in the Information Economy. Strong int'l perspective. Chair: Lance Hoffman.

SIMON DAVIES Convenor, Faculty of Law, Privacy International, Univ. of New South Wales, Australia

EVAN HENDRICKS Editor / Publisher, PRIVACY TIMES

TOM MANDEL Director, Leading Edge Values & Lifestyles Program, SRI INTERNATIONAL

WILLIS WARE RAND Corporation

6. Network Environments of the Future 41 mins.
Chair: Marc Rotenberg.

ELI M. NOAM Prof., School of Business, Columbia Univ., Ctr. forTelecommunications and Information Studies
"Reconciling Free Speech and Freedom of Association"

7. Law Enforcement Practices & Problems 90 mins.
Investigation, prosecution, due process and deterring computer crimes now and in the future; Use of computers to aid law enforcement. Chair: Glenn Tenney.

ROBERT M. SNYDER Organized Crime Bureau, Public Safety Dept., Division of Police, Columbus, OH

DONALD DELANEY Sr. Investigator, Major Case Squad, New York State Police

DALE BOLL Deputy Director, Fraud Division, United States Secret Service, Wash. D.C.

DON INGRAHAM Assistant District Attorney, Alameda County District Attorney's Office

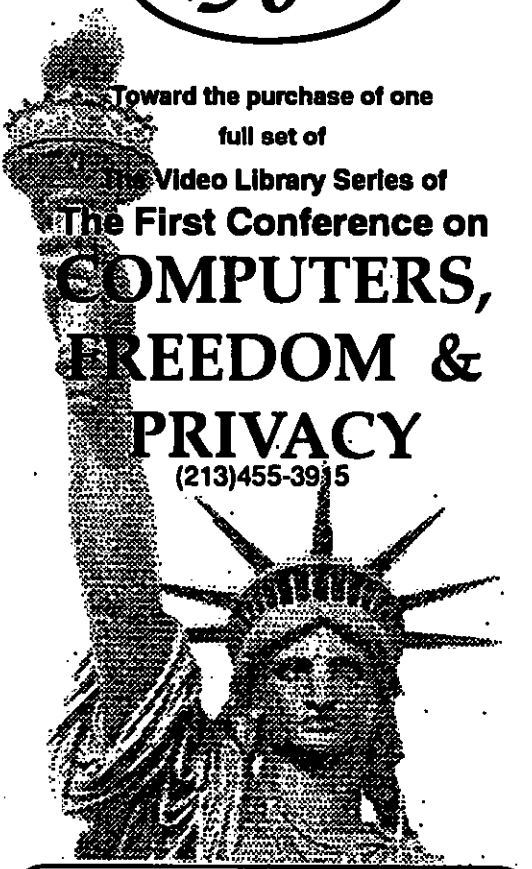
In Recognition of your contribution
to education and understanding

$50.00

Toward the purchase of one
full set of
The Video Library Series of

The First Conference on COMPUTERS, FREEDOM & PRIVACY

(213)455-3915



EDUCATIONAL DISCOUNT CERTIFICATE

Recipient's signature _____

Assigned to: _____

Worth $50 toward purchase of CFP Video Series
if used before November 25th.
(One certificate applicable to purchase of one full set)

$50.00

COMPUTERS, FREEDOM & PRIVACY

VIDEO LIBRARY PROJECT

Conference Chair: **Jim Warren**

P.O. Box 912 • Topanga, CA 90290 • (213) 455-3257 • FAX 455-1384 • ORDERS 455-3915 • EMAIL ctpvideo@well.sf.ca.us

September, 1991

Greetings

One newscaster called the First Conference on Computers, Freedom & Privacy, "The Constitutional Convention of cyberspace." Appropriately, this first-ever event occurred in the bicentennial year of the Bill of Rights — when computers are replacing printing presses as information sources, telecommunications has become a major tool for speech and computer networks are becoming the new Hyde Park.

The event was referenced in Congressional discussions; detailed to top executives in 55 of the largest multinational corporations and has already prompted legislation planned for introduction in California's next legislative session.

Time, Newsweek, Scientific American, the *Wall Street Journal, New York Times, San Francisco Chronicle, Los Angeles Times, Houston Chronicle* and Germany's *Der Spiegel* all carried major reports of the discussions, as did other newspapers and trade and professional periodicals.

For the first time, national and international leaders representing a full range of perspectives met and candidly discussed their differing views of the problems and potentials of computing, communications and civil liberties. One official commented that he had never seen such a diverse collection of people in one place in his life — as the enclosed materials illustrate.

There were three days of intensive discussion of the complex, tightly-interwoven issues that are shaping our society and lives for this Century and most of the next.

The next best thing to having been there is this Library Edition of 15 video tapes — unique "gavel to gavel" coverage.

I highly recommend them — for your reference, for understanding — and for insights into our future.

Jim Warren, Conference Chair

Co-sponsors and cooperating organizations include the Association for Computing Machinery, Electronic Networking Association Institute of Electrical and Electronics Engineers-USA, Videotex Industry Association American Civil Liberties Union, Electronic Frontier Foundation, Cato Institute, The WELL, Autodesk, Portal Communications ACM SIGCAS (Computers and Society), ACM Committee on Scientific Freedom and Human Rights, ACM SIGSOFT (Software) IEEE-USA Committee on Communications and Information Policy, IEEE-USA Intellectual Property Committee

Sponsor: **Computer Professionals for Social Responsibility, Box 717, Palo Alto CA 94302:** *a nonprofit educational corp. [501(c)3]*

COMPUTERS, FREEDOM & PRIVACY

VIDEO LIBRARY PROJECT

P.O. Box 912 • Topanga, CA 90290 • (213) 455-3257 • FAX 455-1384 • ORDERS 455-3915 • EMAIL cfpvideo@well.sf.ca.us

Hello. Thank you for taking a moment to look at this letter.

Every once in awhile an event takes place to change things for the better.
We'd like to tell you about such an event, although its likely you've heard about it already.

Newspapers, magazines and media across the U.S., Canada and Europe have reported on The First Conference on Computers, Freedom & Privacy. Some called it "The Constitutional Convention of Cyberspace." This letter is about what actually happened there. Maybe we should first look at why it matters.

The number of American households with computers doubled in the 1980's. The 1990 census showed 25% of the households surveyed have home computers. Last year, 150 federal, state and local police raided homes in 14 cities to seize 43 computers and 23,000 floppy disks in a cross-country search for teenage computer hackers. Prosecutors say computer-related crime has increased 400%. Civil Liberties advocates counter that law enforcement personnel are engaging in witch hunts because they are confused by technology. Constitutional law experts ask if Free Speech expressed in bits and bytes is adequately protected by the Bill of Rights.

Meanwhile, over 85% of America's businesses and virtually all government operations have computerized. The widespread collection and unauthorized resale of personal data about each of us (our buying habits, credit history, health problems, driving records, children's school activities, etc.) has become a multibillion dollar industry, resulting daily in an avalanche of "direct marketing" junk mail in America's mailboxes. More ominously, international lawyers and scientists point to "surveillance societies" based on American technology developing in Thailand and other parts of the world. They fear it could happen here.

At the first-ever Computers, Freedom & Privacy Conference, national and international leaders representing a full range of perspectives met and candidly discussed their differing views of the problems and potentials of computing, communications and civil liberties. One official commented that he had never seen such a diverse collection of people in one place in his life.

You and the people in your field understand the power of information better than anyone.

That's why *Library Hi Tech News* stopped its presses when it learned that the COMPUTERS, FREEDOM & PRIVACY VIDEO LIBRARY SERIES has just become available. *Library Hi Tech's* special report is 14 pages long. That's how urgent they feel it is for you to know about this video offering. Excerpts from that article are on the other side of this page.

Please look over the enclosed brochure. You'll see why the First Conference on Computers, Freedom & Privacy has already become a classic. The next best thing to having been there is this Library Edition of 15 videotapes—unique, beautifully produced "gavel to gavel" coverage—for reference, for understanding, and for insights into our future.

By the way, for those who place an order before November 25, we've included a Thanksgiving gift certificate worth $50!

LIBRARY HI TECH NEWS

NUMBER 84-85 SEPT/OCT 1991

A PIERIAN PRESS PUBLICATION

COMPUTERS, FREEDOM & PRIVACY

VIDEOTAPED CONFERENCE PROCEEDINGS

by Mary Meernick and Barbara Glover with an introduction by C. Edward Wall

EXCERPTS FROM 14 PAGE REVIEW AND ABSTRACT

Videotaped conference proceedings can be deadly--talking heads--the kind of stuff that puts life-long insomniacs to sleep. The tapes of this conference are curiously different

The tapes of this conference are curiously different.

- **First, they are of high production quality....**
- **Second, most of the presentations are short, pithy, substantive and provocative.**
- **Third, the exchange between panelists and audience is excellent.**

These tapes present a diversity of issues and perspectives in ways not possible in print.

The tapes can be effectively adapted to classroom use and public presentations; excerpts can be shown to initiate--indeed provoke--student and audience discussion.

The definition of "free press" is of necessity evolving. Once a singularly paper medium, it has evolved to encompass the airwaves--radio and television--and is now rapidly extending to computers and related telecommunications infrastructure.

Libraries, which have traditionally acquired, processed and distributed paper resources, are in their infancy in similarly handling computer-based and telecommunications-accessed resources. The related issues such as privacy and freedom are not well understood either by those in the library field or beyond.

These tapes will begin to bring into focus some of the diverse issues that an adolescent electronic world is struggling to understand--and protect.

Computers, freedom, and privacy are core issues for library professionals. There is much here that should be seen, heard, felt and absorbed by those of us who dedicate ourselves to providing free access to information, particularly if we hope to continue doing so in the years ahead.

Conference Overview

What does a conference on "Computers, Freedom and Privacy" have to say to librarians? A great deal. Which is why it may be an ominous portent that no library organization was a co-sponsor of this conference.... In fact, there are indications that many conference participants perceive the traditional library as an anachronism. Telecommunications networks will be the "digital libraries of the future."

Librarians have always been passionate crusaders for intellectual *freedom* and have recently been at the forefront of the *privacy* protection issue with their oppostion to the FBI's Library Awareness Program. But throw *computers* into this equation and libraries seem to be out of the mainstream, not only at this conference but also in the general information marketplace.

The conference participants foresee a "national information infrastructure" -- "a communications network...rich in voice, data, and video." The United States will have a true participatory democracy; a terminal in every home will not only empower citizens through their ability to access all the nation's information resources but will also enable them to participate in the political, economic, and cultural online environment. Of course the conference participants recognize that this scenario is some way off....

But when this dream does become reality, what need will there be for traditional libraries?...We face being left out of the chain--bypassed as electronic information technologies enable publishers, both government and private, to deal directly with the end-user. Our suppliers are becoming our competitors and we are starting to feel the heat.

...Librarians are also having serious problems with the public sector. During the session on Access to Government Information, a university librarian noted that the government's elimination or privatization of many of its publications jeopardize the mission of federal depository libraries as "information centers for free public access." Robert Veeder (U.S. Office of Management and Budget)...would like to "encourage diversity of information sources," avoiding either "government monopolies or private sector monopolies or library monopolies." The implications...are revealing and troubling. How can the concept of monopoly even be applied to an institution whose goal is to ensure that access to all information is as free and equitable as possible? What is at stake here is more than just the future of the library profession; the democratization of information will be threatened, leaving an information elite to control the show...

Librarians must stake out a claim on the electronic frontier and begin to help develop policies that will safeguard their mission.

Libraries must integrate electronic and telecommunications technologies into their services. We must focus more on providing information itself. Electronic technologies allow creative approaches to information delivery; all types of data...can now be pulled from a variety of sources, analyzed, manipulated and repackaged. We will have to become information brokers, intent more on tailoring services to our customers' needs than on warehousing materials....

Protecting privacy and confidentiality will require more vigilance in the online environment. Electronic technologies facilitate incursion, both from the government and private sectors, against our constitutional rights. Judith Krug (Office of Intellectual Freedom, American Library Assn.) discusses the FBI's Library Awareness Program, in which agents seek library circulation information on the reading habits of foreign nationals....Krug points out that the Librairians' Professional Code of Ethics obligates librarians to protect the privacy and confidentiality of our users...This topic resurfaces during the session on Security Capabilities, Privacy and Integrity. Marc Rotenberg of Computer Professionals for Social Responsibility asked William Bayse of the FBI whether there is a similar program to monitor communications of foreign nationals on electronic bulletin boards. Electronic technology should engender a sense of responsibility in those who develop and use it, but the conference was full of horror stories to the contrary. The message is clear: librarians have a critical role to play in preserving access to information and protecting personal privacy in the electronic environment.

April 23, 1991

Mitchell Kapor
President
Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141

Dear Mr. Kapor:

I was inspired by the pioneering spirit of the First Conference on Computers, Freedom, and Privacy, because so much of what I do at the Community Memory Project involves urging people who have never used computers before to participate on-line.

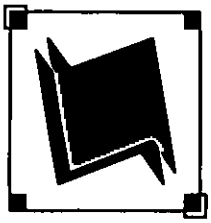
Over Community Memory, I watch people who ordinarily are excluded from telecommunications -- homeless people, low income families, small business people, and at-risk youth -- tap into the power of this technology. I hope you, and the entire Board of the Electronic Frontier Foundation, will support our efforts.

Everybody's Network: Libraries and Laundramats

Our current project is an electronic bulletin board with ten public access computer sites in libraries, laundramats, and community centers. Two thousand people each month use the network to facilitate dialogue, information-sharing and constituency-building. Because we want to include people who are otherwise barred from telecommunications, Community Memory, unlike many bulletin board systems, is organized so information is simple to find. Participants tap into almost 100 different community-created discussion forums or they can create their own. This easy-to-use, communication tool encourages all members of the community to move beyond passive consumption of information to become active builders of an information and opinion exchange.

Public Access and Telecommunications Policy

Like you, I believe that many more individuals and groups have a stake in the development of computer networks than currently participate on-line. I have found that only when ordinary people have access to these tools and see the value of them, do they truly understand why they have a stake in these public policy issues. Ironically, many who see computers as mysterious, impersonal, and threatening may actually have the most to gain from telecomputing. A young single mother who finds a babysitter over Community Memory begins to see computer networks not as instruments for the benefit of big business or the IRS, but as tools which she can use to gain greater control of her life. Over our network, a homeless person can interact with other citizens not as a specimen of social turmoil, but as an equal participant in community life.



Community Memory

A public access information and resource exchange

April 23, 1991

Mitchell Kapor
President
Electronic Frontier Foundation, Inc.
155 Second Street
Cambridge, MA 02141

Dear Mr. Kapor:

I was inspired by the pioneering spirit of the First Conference on Computers, Freedom, and Privacy, because so much of what I do at the Community Memory Project involves urging people who have never used computers before to participate on-line.

Over Community Memory, I watch people who ordinarily are excluded from telecommunications -- homeless people, low income families, small business people, and at-risk youth -- tap into the power of this technology. I hope you, and the entire Board of the Electronic Frontier Foundation, will support our efforts.

Everybody's Network: Libraries and Laundramats

Our current project is an electronic bulletin board with ten public access computer sites in libraries, laundramats, and community centers. Two thousand people each month use the network to facilitate dialogue, information-sharing and constituency-building. Because we want to include people who ~~are~~ otherwise are barred from telecommunications, Community Memory, unlike many bulletin board systems, is organized so information is simple to find. Participants tap into almost 100 different community-created discussion forums, or they can create their own. This easy-to-use, communication tool encourages all members of the community to move beyond passive consumption of information to become active builders of an information and opinion exchange.

Public Access and Telecommunications Policy

Like you, I believe that many more individuals and groups have a stake in the development of computer networks than currently participate on-line. I have found that only when ordinary people have access to these tools and see the value of them, do they truly understand why they have a stake in these public policy issues. Ironically, many who see computers as mysterious, impersonal, and threatening may actually have the most to gain from telecomputing. A young single mother who finds a babysitter over Community Memory begins to see computer networks not as instruments for the benefit of big business or the IRS, but as tools which she can use to gain greater control of her life. Over our network, a homeless person can interact with other ~~community members~~ citizens not as a specimen of social turmoil, but as an equal participant in community life.

2617 San Pablo Avenue, Berkeley, California 94702 415-841-1114

The Community Memory Project proves that computer technology can enhance American society by providing pertinant, user-friendly tools which go far beyond word processing, Nintendo or ATM machines. Unfortunately, most networks remain primarily the province of big business, higher education, the military, and the computer hobbyist.

As a national information infrastructure develops, most people will have no idea of the power this new information highway can bring, or deny, them. It is only the local testing grounds of democratic telecommunications systems that can demonstrate to policy makers, major institutions, and the computer industry, the necessity and potential of broad access to these networks.

Civilizing Cyberspace since 1973

Like the Electronic Frontier Foundation, the Community Memory Project is committed to providing and promoting new tools "which will endow non-technical users with full and easy access to computer-based telecommunications." Since 1973, we've been, in your words, "a petri dish" of experimentation" where individuals and groups can test out the potential of information age technology to enhance their lives.

For 18 years the Community Memory Project has been "civilizing cyberspace" by:

o Creating and managing low-cost, publicly accessible computer networks for entire communities -- young and old, rich and poor, computer savvy or frankly techno-phobic.

o Providing hands-on training and friendly hand-holding for those who might be intimidated by the technology.

o Documenting and sharing effective models of how these tools can strengthen community.

Not that it's ever easy. When the goal is to reach beyond the educated and the well off, issues of access, skills, and trust arise. Consider, the difficulty that some of the country's most literate, educated, and communicative people have when first accessing the Well. Then consider the challenge of motivating people, who have been told their ideas are unimportant or uninformed, to explore these new tools for empowerment. Over the years we've discovered that although the challenge is considerable, the rewards are great.

You see, we believe that effectively designed local networks can become a catalyst in the democratic development of cyberspace. Our project serves five objectives relevant to the Electronic Frontier Foundation:

o to develop tools to enhance free expression and broad participation in society.

o to encourage cross-constituency communication by creating an arena where diverse people and groups can share ideas, opinions, and resources.

o to demonstrate that easy-to-use local networks can be both participatory and accessible to the entire community.

o to confirm that simple networks can serve as stepping stones for participants to utilize more complex networks or services.

o to create replicable, self-sustaining models for low cost community communications.

What the Electronic Frontier Foundation's Support can Mean

Your funding would help us meet those objectives by sustaining the following activities:

o development of user friendly tools which encourage participation by people routinely excluded from these technologies.

o management of a public access computer network that anyone in the community can use to read and write messages.

o assistance to individuals and groups who want to use the network to share knowledge, opinion, resources, and friendship, including help for people who are intimidated by computers.

o evaluation and documentation of the impact of this technology on its participants and the local community.

I am convinced that easy-to-use telecommunications can put diverse people in touch with their communities in ways which revitalize links with neighbors and local institutions. However, the potential of community telecommunications has only begun to be tested. What we do now will determine if the new information infrastructure -- like our streets, town meetings, and city parks -- will be open and meaningful to all.

I look forward to speaking with you about how the Electronic Frontier Foundation can support the Community Memory Project. If you need additional information about our activities or plans, please don't hesitate to contact me.

Best wishes,

Evelyn Pine
Executive Director

enclosure
cc. Lee Felsenstein, Golemics