07.2016

HACKDOWN: Bruce Sterling's "Hacker Crackdown" Hacked and Cracked

mozzarella.website

Excerpt From:

==Phrack Inc.==

Volume Four, Issue Forty-One, File 13 of 13

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN Phrack World News PWN
PWN PWN
PWN Issue 41 / Part 3 of 3 PWN
PWN PWN
PWN Compiled by Datastream Cowboy PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

10. NEW YORK STATE POLICE DECRIMINALIZE THE WORD “HACKER” (Barba ra E. McMullen & John F. McMullen, Newsbytes, 10/21/92) -- ALBANY, NEW YORK -- Senior investigator Ron Stevens of the New York State Police Computer Unit has told Newsbytes that it will be the practice of his unit to avoid the use of the term “hacker” in describing those alleged to have committed computer crimes.

    Stevens told Newsbytes, “We use the term computer criminal to describe those who break the law using computers. While the lay person may have come to understand the meaning of hacker as a computer criminal, the term isn’t accurate. The people in the early days of the computer industry considered themselves hackers and they made the computer what it is today. There are those today who consider themselves hackers and do not commit illegal acts.”

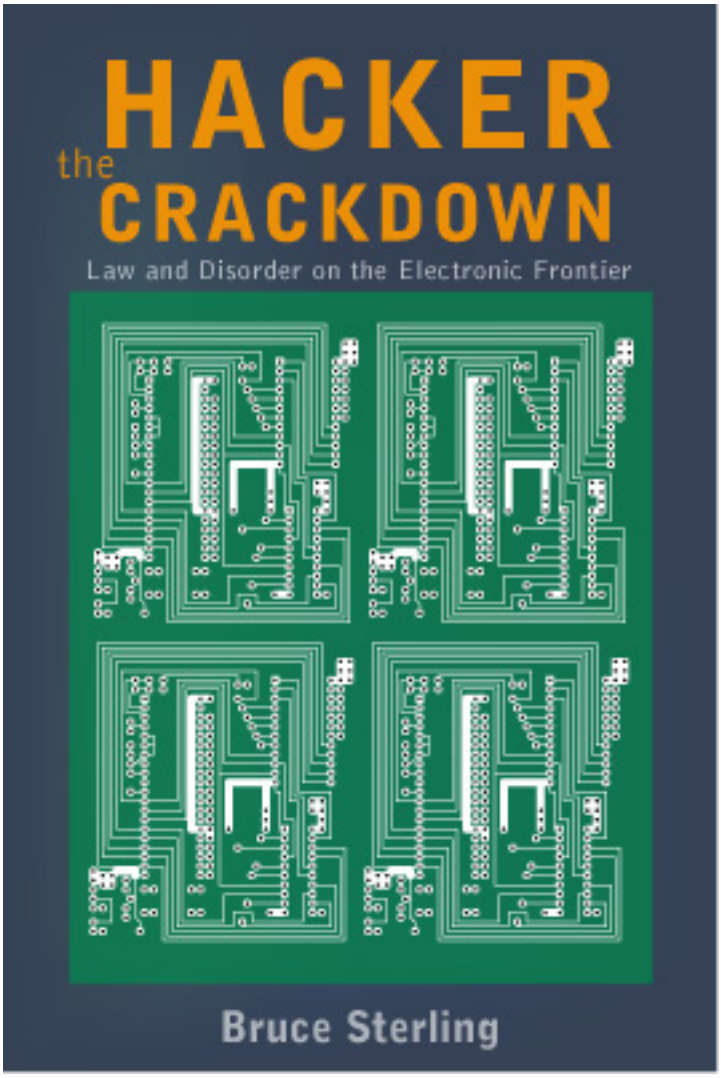
    Stevens had made similar comments in a recent conversation with Albany BBS operator Marty Winter. Winter told Newsbytes, “‘Hacker’ is, unfortunately an example of the media taking what used to be an honorable term, and using it to describe an activity because they (the media) are too lazy or stupid to come up with something else. Who knows, maybe one day ‘computer delinquent’ WILL be used, but I sure ain’t gonna hold my breath.”

    Stevens, together with investigator Dick Lynch and senior investigator Donald Delaney, attended the March 1992 Computers, Freedom and Privacy Conference (CFP-2) in Washington, DC and met such industry figures as Glenn Tenney, congressional candidate and chairman of the WELL’s annual “Hacker Conference”; Craig Neidorf, founding editor and publisher of Phrack; Steven Levy, author of “Hackers” and the recently published “Artificial Life”; Bruce Sterling, author of the recently published “The Hacker Crackdown”; Emmanuel Goldstein, editor and publisher of 2600: The Hacker Quarterly” and a number of well-known “hackers.”

    Stevens said, “When I came home, I read as much of the literature about the subject that I could and came to the conclusion that a hacker is not necessarily a computer criminal.”

    The use of the term “hacker” to describe those alleged to have committed computer crimes has long been an irritant to many in the online community. When the July 8th federal indictment of 5 New York City individuals contained the definition of computer hacker as “someone who uses a computer or a telephone to obtain unauthorized access to other computers,” there was an outcry on such electronic conferencing system as the WELL (Whole Earth ‘Lectronic Link). Many of the same people reacted quite favorably to the Stevens statement when it was posted on the WELL.

Excerpts From:



Preface to the Electronic Release of
The Hacker Crackdown:

Out in the traditional world of print, *The Hacker Crackdown* is ISBN 0-553-08058-X, and is formally catalogued by the Library of Congress as "1. Computer crimes -- United States. 2. Telephone -- United States -- Corrupt practices. 3. Programming (Electronic computers) -- United States -- Corrupt practices." `Corrupt practices,' I always get a kick out of that description. Librarians are very ingenious people.

The paperback is ISBN 0-553-56370-X. If you go and buy a print version of *The Hacker Crackdown*, an action I encourage heartily, you may notice that in the front of the book, beneath the copyright notice -- "Copyright (C) 1992 by Bruce Sterling" -- it has this little block of printed legal boilerplate from the publisher. It says, and I quote:

> *No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. For information address: Bantam Books.*

This is a pretty good disclaimer, as such disclaimers go. I collect intellectual-property disclaimers, and I've seen dozens of them, and this one is at least pretty straightforward. In this narrow and particular case, however, it isn't quite accurate. Bantam Books puts that disclaimer on every book they publish, but Bantam Books does not, in fact, own the electronic rights to this book. I do, because of certain extensive contract maneuverings my agent and I went through before this book was written. I want to give those electronic publishing rights away through certain not-for-profit channels, and I've convinced Bantam that this is a good idea.

Information *wants* to be free. And the information inside this book longs for freedom with a peculiar intensity. I genuinely believe that the natural habitat of this book is inside an electronic network. That may not be the easiest direct method to generate revenue for the book's author, but that doesn't matter; this is where this book belongs by its nature. I've written other books -- plenty of other books -- and I'll write more and I am writing more, but this one is special. I am making *The Hacker Crackdown* available electronically as widely as I can conveniently manage, and if you like the book, and think it is useful, then I urge you to do the same with it. You can copy this electronic book. Copy the heck out of it, be my guest,

and give those copies to anybody who wants them. The nascent world of cyberspace is full of sysadmins, teachers, trainers, cybrarians, netgurus, and various species of cybernetic activist. If you're one of those people, I know about you, and I know the hassle you go through to try to help people learn about the electronic frontier. I hope that possessing this book in electronic form will lessen your troubles. Granted, this treatment of our electronic social spectrum is not the ultimate in academic rigor. And politically, it has something to offend and trouble almost everyone. But hey, I'm told it's readable, and at least the price is right. You can upload the book onto bulletin board systems, or Internet nodes, or electronic discussion groups. Go right ahead and do that, I am giving you express permission right now. Enjoy yourself.

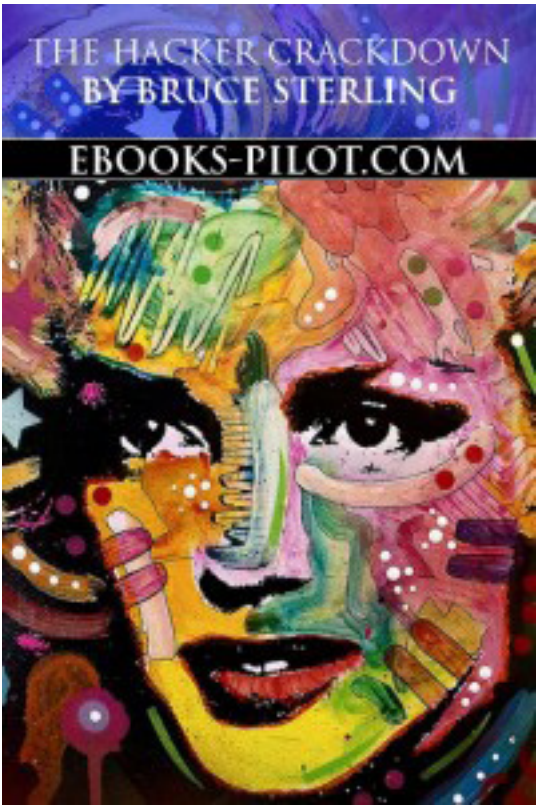
This is a book about cops, and wild teenage whiz-kids, and lawyers, and hairy-eyed anarchists, and industrial technicians, and hippies, and high-tech millionaires, and game hobbyists, and computer security experts, and Secret Service agents, and grifters, and thieves. This book is about the electronic frontier of the 1990s. It concerns activities that take place inside computers and over telephone lines. A science fiction writer coined the useful term "cyberspace" in 1982. But the territory in question, the electronic frontier, is about a hundred and thirty years old. Cyberspace is the "place" where a telephone conversation appears to occur. Not inside your actual phone, the plastic device on your desk. Not inside the other person's phone, in some other city. *The place between* the phones. The indefinite place out there, where the two of you, two human beings, actually meet and communicate.

This book is about trouble in cyberspace. Specifically, this book is about certain strange events in the year 1990, an unprecedented and startling year for the the growing world of computerized communications.

In 1990 there came a nationwide crackdown on illicit computer hackers, with arrests, criminal charges, one dramatic show-trial, several guilty pleas, and huge confiscations of data and equipment all over the USA.

The Hacker Crackdown of 1990 was larger, better organized, more deliberate, and more resolute than any previous effort in the brave new world of computer crime. The U.S. Secret Service, private telephone security, and state and local law enforcement groups across the country all joined forces in a determined attempt to break the back of America's electronic underground. It was a fascinating effort, with very mixed results.

The Hacker Crackdown had another unprecedented effect; it spurred the creation, within "the computer community," of the Electronic Frontier Foundation, a new and very odd interest group, fiercely dedicated to the establishment and preservation of electronic civil liberties. The crackdown, remarkable in itself, has created a melee of debate over electronic crime, punishment, freedom of the press, and issues of search and seizure. Politics has entered cyberspace. Where people go, politics follow. This is the story of the people of cyberspace.



Part 2: The Digital Underground:

Before computers and their phone-line modems entered American homes in gigantic numbers, phone phreaks had their own special telecommunications hardware gadget, the famous "blue box." This fraud device (now rendered increasingly useless by the digital evolution of the phone system) could trick switching systems into granting free access to long-distance lines. It did this by mimicking the system's own signal, a tone of 2600 hertz.

Steven Jobs and Steve Wozniak, the founders of Apple Computer, Inc., once dabbled in selling blue-boxes in college dorms in California. For many, in the early days of phreaking, blue-boxing was scarcely perceived as "theft," but rather as a fun (if sneaky) way to use excess phone capacity harmlessly. After all, the long-distance lines were *just sitting there*.... Whom did it hurt, really? If you're not *damaging* the system, and you're not *using up any tangible resource*, and if nobody *finds out* what you did, then what real harm have you done? What exactly *have* you "stolen," anyway? If a tree falls in the forest and nobody hears it, how much is the noise worth? Even now this remains a rather dicey question.

Blue-boxing was no joke to the phone companies, however. Indeed, when *Ramparts* magazine, a radical publication in California, printed the wiring schematics necessary to create a mute box in June 1972, the magazine was seized by police and Pacific Bell phonecompany officials. The mute box, a blue-box variant, allowed its user to receive long-distance calls free of charge to the caller. This device was closely described in a *Ramparts* article wryly titled "Regulating the Phone Company In Your Home." Publication of this article was held to be in violation of Californian State Penal Code section 502.7, which outlaws ownership of wire-fraud devices and the selling of "plans or instructions for any instrument, apparatus, or device intended to avoid telephone toll charges."

Issues of *Ramparts* were recalled or seized on the newsstands, and the resultant loss of income helped put the magazine out of business. This was an ominous precedent for free-expression issues, but the telco's crushing of a radical-fringe magazine passed without serious challenge at the time. Even in the freewheeling California 1970s, it was widely felt that there was something sacrosanct about what the phone company knew; that the telco had a legal and moral right to protect itself by shutting off the flow of such illicit information. Most telco information was so "specialized" that it

would scarcely be understood by any honest member of the public. If not published, it would not be missed. To print such material did not seem part of the legitimate role of a free press.

In 1990 there would be a similar telco-inspired attack on the electronic phreak/hacking "magazine" *Phrack*. The *Phrack* legal case became a central issue in the Hacker Crackdown, and gave rise to great controversy. Phrack would also be shut down, for a time, at least, but this time both the telcos and their law-enforcement allies would pay a much larger price for their actions.

Police want to believe that all hackers are thieves. It is a tortuous and almost unbearable act for the American justice system to put people in jail because they want to learn things which are forbidden for them to know. In an American context, almost any pretext for punishment is better than jailing people to protect certain restricted kinds of information. Nevertheless, *policing information* is part and parcel of the struggle against hackers.

This dilemma is well exemplified by the remarkable activities of "Emmanuel Goldstein," editor and publisher of a print magazine known as *2600: The Hacker Quarterly*. Goldstein was an English major at Long Island's State University of New York in the '70s, when he became involved with the local college radio station. His growing interest in electronics caused him to drift into Yippie *TAP* circles and thus into the digital underground, where he became a self-described technorat. His magazine publishes techniques of computer intrusion and telephone "exploration" as well as gloating exposes of telco misdeeds and governmental failings.

Goldstein lives quietly and very privately in a large, crumbling Victorian mansion in Setauket, New York. The seaside house is decorated with telco decals, chunks of driftwood, and the basic bric-a-brac of a hippie crash-pad. He is unmarried, mildly unkempt, and survives mostly on TV dinners and turkey-stuffing eaten straight out of the bag. Goldstein is a man of considerable charm and fluency, with a brief, disarming smile and the kind of pitiless, stubborn, thoroughly recidivist integrity that America's electronic police find genuinely alarming.

Goldstein took his nom-de-plume, or "handle," from a character in Orwell's *1984*, which may be taken, correctly, as a symptom of the gravity of his sociopolitical worldview. He is not himself a practicing computer intruder, though he vigorously abets these actions, especially when they are pursued against large corporations or governmental agencies. Nor is he a thief, for he loudly scorns mere theft of phone service, in favor of 'exploring and manipulating the system.' He is probably best described and understood as a *dissident*.

Weirdly, Goldstein is living in modern America under conditions very similar to those of former East European intellectual dissidents. In other words, he flagrantly espouses a value-system that is deeply and irrevocably opposed to the system of those in power and the police. The values in *2600* are generally expressed in terms that are ironic, sarcastic, paradoxical, or just downright confused. But there's no mistaking their radically anti-authoritarian tenor. *2600* holds that technical power and specialized
knowledge, of any kind obtainable, belong by right in the hands of those individuals brave and bold enough to discover them -- by whatever means necessary. Devices, laws, or systems that forbid access, and the free spread of knowledge, are provocations that any free and self-respecting hacker should relentlessly attack. The "privacy" of governments, corporations and other soulless technocratic organizations should never be protected at the expense of the liberty and free initiative of the individual techno-rat.

However, in our contemporary workaday world, both governments and corporations are very anxious indeed to police information which is secret, proprietary, restricted, confidential, copyrighted, patented, hazardous, illegal, unethical, embarrassing, or otherwise sensitive. This makes Goldstein persona non grata, and his philosophy a threat.

Very little about the conditions of Goldstein's daily life would astonish, say, Vaclav Havel. (We may note in passing that President Havel once had his word-processor confiscated by the Czechoslovak police.) Goldstein lives by *samizdat*, acting semi-openly as a data- center for the underground, while challenging the powers-that-be to abide by their own stated rules: freedom of speech and the First Amendment.

Goldstein thoroughly looks and acts the part of techno-rat, with shoulder-

length ringlets and a piratical black fisherman's-cap set at a rakish angle. He often shows up like Banquo's ghost at meetings of computer professionals, where he listens quietly, half-smiling and taking thorough notes.

Computer professionals generally meet publicly, and find it very difficult to rid themselves of Goldstein and his ilk without extralegal and unconstitutional actions. Sympathizers, many of them quite respectable people with responsible jobs, admire Goldstein's attitude and surreptitiously pass him information. An unknown but presumably large proportion of Goldstein's 2,000-plus readership are telco security personnel and police, who are forced to subscribe to 2600 to stay abreast of new developments in hacking. They thus find themselves *paying this guy's rent* while grinding their teeth in anguish, a situation that would have delighted Abbie Hoffman (one of Goldstein's few idols).

Goldstein is probably the best-known public representative of the hacker underground today, and certainly the best-hated. Police regard him as a Fagin, a corrupter of youth, and speak of him with untempered loathing. He is quite an accomplished gadfly.

2600 has been published consistently since 1984. It has also run a bulletin board computer system, printed *2600* T-shirts, taken fax calls... The Spring 1991 issue has an interesting announcement on page 45: "We just discovered an extra set of wires attached to our fax line and heading up the pole. (They've since been clipped.) Your faxes to us and to anyone else could be monitored."

In the worldview of *2600*, the tiny band of technorat brothers (rarely, sisters) are a beseiged vanguard of the truly free and honest. The rest of the world is a maelstrom of corporate crime and high-level governmental corruption, occasionally tempered with well-meaning ignorance. To read a few issues in a row is to enter a nightmare akin to Solzhenitsyn's, somewhat tempered by the fact that *2600* is often extremely funny.

Goldstein did not become a target of the Hacker Crackdown, though he protested loudly, eloquently, and publicly about it, and it added considerably to his fame. It was not that he is not regarded as dangerous, because he is so regarded. Goldstein has had brushes with the law in the

past: in 1985, a *2600* bulletin board computer was seized by the FBI, and some software on it was formally declared "a burglary tool in the form of a computer program." But Goldstein escaped direct repression in 1990, because his magazine is printed on paper, and recognized as subject to Constitutional freedom of the press protection. As was seen in the *Ramparts* case, this is far from an absolute guarantee. Still, as a practical matter, shutting down *2600* by court-order would create so much legal hassle that it is simply unfeasible, at least for the present. Throughout 1990, both Goldstein and his magazine were peevishly thriving.

Instead, the Crackdown of 1990 would concern itself with the computerized version of forbidden data. The crackdown itself, first and foremost, was about *bulletin board systems*. Bulletin Board Systems, most often known by the ugly and un-pluralizable acronym "BBS," are the life-blood of the digital underground. Boards were also central to law enforcement's tactics and strategy in the Hacker Crackdown.

"Boards" are home computers tied to home telephone lines, that can store and transmit data over the phone -- written texts, software programs, computer games, electronic mail. Boards were invented in the late 70s, and, while the vast majority of boards are utterly harmless, some few piratical boards swiftly became the very backbone of the 80s digital underground. Over half the attendees of CyberView ran their own boards. "Knight Lightning" had run an electronic magazine, "Phrack," that appeared on many underground boards across America.

Boards are mysterious. Boards are conspiratorial. Boards have been accused of harboring: Satanists, anarchists, thieves, child pornographers, Aryan nazis, religious cultists, drug dealers -- and, of course, software pirates, phone phreaks, and hackers. Underground hacker boards were scarcely reassuring, since they often sported terrifying sci-fi heavy-metal names, like "Speed Demon Elite," "Demon Roach Underground," and "Black Ice." (Modern hacker boards tend to feature defiant titles like "Uncensored BBS," "Free Speech," and "Fifth Amendment.")

Underground boards carry stuff as vile and scary as, say, 60s-era underground newspapers -- from the time when Yippies hit Chicago and ROLLING STONE gave away free roach-clips to subscribers. "Anarchy files" are popular features on outlaw boards, detailing how to build pipe-bombs, how to make Molotovs, how to brew methedrine and LSD, how to break and enter buildings, how to blow up bridges, the easiest ways to kill someone with a single blow of a blunt object -- and these boards bug straight people a lot. Never mind that all this data is publicly available in public libraries where it is protected

by the First Amendment. There is something about its being on a computer -- where any teenage geek with a modem and keyboard can read it, and print it out, and spread it around, free as air -- there is something about that, that is creepy.[1]

The St. Louis scene was not to rank with major centers of American hacking such as New York and L.A. But St. Louis did rejoice in possession of "Knight Lightning" and "Taran King," two of the foremost *journalists* native to the underground. Missouri boards like Metal Shop, Metal Shop Private, Metal Shop Brewery, may not have been the heaviest boards around in terms of illicit expertise. But they became boards where hackers could exchange social gossip and try to figure out what the heck was going on nationally -- and internationally. Gossip from Metal Shop was put into the form of news files, then assembled into a general electronic publication, *Phrack*, a portmanteau title coined from "phreak" and "hack." The *Phrack* editors were as obsessively curious about other hackers as hackers were about machines.

Phrack, being free of charge and lively reading, began to circulate throughout the underground. As Taran King and Knight Lightning left high school for college, *Phrack* began to appear on mainframe machines linked to BITNET, and, through BITNET to the "Internet," that loose but extremely potent not-for-profit network where academic, governmental and corporate machines trade data through the UNIX TCP/IP protocol.

1.

```
                        ==Phrack Inc.==

      Volume Three, Issue Thirty-Three, File 10 of 13

PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN          P h r a c k   W o r l d   N e w s        PWN
^*^          ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        ^*^
PWN             Special Edition Issue Four            PWN
^*^                                                   ^*^
PWN       "The Hackers Who Came In From The Cold"     PWN
^*^                                                   ^*^
PWN                  June 21-23, 1991                 PWN
^*^                                                   ^*^
PWN              Written by Bruce Sterling            PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN { CyberView '91 } PWN ^*^ PWN ^*^ PWN
```

(The “Internet Worm” of November 2-3,1988, created by Cornell grad student Robert Morris, was to be the largest and bestpublicized computer-intrusion scandal to date. Morris claimed that his ingenious “worm” program was meant to harmlessly explore the Internet, but due to bad programming, the Worm replicated out of control and crashed some six thousand Internet computers. Smallerscale and less ambitious Internet hacking was a standard for the underground elite.) Most any underground board not hopelessly lame and out-of-it would feature a complete run of *Phrack* -- and, possibly, the lesser-known standards of the underground: the *Legion of Doom Technical Journal*, the obscene and raucous *Cult of the Dead Cow* files, *P/HUN* magazine, *Pirate*, the *Syndicate Reports*, and perhaps the highly anarcho- political *Activist Times Incorporated*.

Possession of *Phrack* on one’s board was prima facie evidence of a bad attitude. *Phrack* was seemingly everywhere, aiding, abetting, and spreading the underground ethos. And this did not escape the attention of corporate security or the police.

The Computer Fraud and Abuse Task Force, led by federal prosecutor William J. Cook, had started in 1987 and had swiftly become one of the most aggressive local “dedicated computer-crime units.” Chicago was a natural home for such a group. The world’s first computer bulletin-board system had been invented in Illinois. The state of Illinois had some of the nation’s first and sternest computer crime laws. Illinois State Police were markedly alert to the possibilities of white-collar crime and electronic fraud.

Throughout the 1980s, the federal government had given prosecutors an armory of new, untried legal tools against computer crime. Cook and his colleagues were pioneers in the use of these new statutes in the real-life cut-and-thrust of the federal courtroom.

On October 2, 1986, the US Senate had passed the “Computer Fraud and Abuse Act” unanimously, but there were pitifully few convictions under this statute. Cook’s group took their name from this statute, since they were determined to transform this powerful but rather theoretical Act of Congress into a real-life engine of legal destruction against computer fraudsters and scofflaws.

It was not a question of merely discovering crimes, investigating them, and then trying and punishing their perpetrators. The Chicago unit, like most everyone else in the business, already knew who the bad guys were: the Legion of Doom and the writers and editors of *Phrack*. The task at hand was to find some legal means of putting these characters away.

Of the three LoD stalwarts, Prophet was in the most direct trouble. Prophet was a UNIX programming expert who burrowed in and out of the Internet as a matter of course. He'd started his hacking career at around age 14, meddling with a UNIX mainframe system at the University of North Carolina.

Prophet himself had written the handy Legion of Doom file "UNIX Use and Security From the Ground Up." UNIX (pronounced "you-nicks") is a powerful, flexible computer operating-system, for multi-user, multitasking computers. In 1969, when UNIX was created in Bell Labs, such computers were exclusive to large corporations and universities, but today UNIX is run on thousands of powerful home machines. UNIX was particularly wellsuited to telecommunications programming, and had become a standard in the field. Naturally, UNIX also became a standard for the elite hacker and phone phreak.

Lately, Prophet had not been so active as Leftist and Urvile, but Prophet was a recidivist. In 1986, when he was eighteen, Prophet had been convicted of "unauthorized access to a computer network" in North Carolina. He'd been discovered breaking into the Southern Bell Data Network, a UNIX-based internal telco network supposedly closed to the public. He'd gotten a typical hacker sentence: six months suspended, 120 hours community service, and three years' probation.

After that humiliating bust, Prophet had gotten rid of most of his tonnage of illicit phreak and hacker data, and had tried to go straight. He was, after all, still on probation. But by the autumn of 1988, the temptations of cyberspace had proved too much for young Prophet, and he was shoulder-to-shoulder with Urvile and Leftist into some of the hairiest systems around.

In early September 1988, he'd broken into BellSouth's centralized automation system, AIMSX or "Advanced Information Management

System." AIMSX was an internal business network for BellSouth, where telco employees stored electronic mail, databases, memos, and calendars, and did text processing. Since AIMSX did not have public dial-ups, it was considered utterly invisible to the public, and was not well-secured -- it didn't even require passwords. Prophet abused an account known as "waa1," the personal account of an unsuspecting telco employee. Disguised as the owner of waa1, Prophet made about ten visits to AIMSX.

Prophet did not damage or delete anything in the system. His presence in AIMSX was harmless and almost invisible. But he could not rest content with that.

One particular piece of processed text on AIMSX was a telco document known as "Bell South Standard Practice 660-225-104SV Control Office Administration of Enhanced 911 Services for Special Services and Major Account Centers dated March 1988."

Prophet had not been looking for this document. It was merely one among hundreds of similar documents with impenetrable titles. However, having blundered over it in the course of his illicit wanderings through AIMSX, he decided to take it with him as a trophy. It might prove very useful in some future boasting, bragging, and strutting session. So, some time in September 1988, Prophet ordered the AIMSX mainframe computer to copy this document (henceforth called simply called "the E911 Document") and to transfer this copy to his home computer.

No one noticed that Prophet had done this. He had "stolen" the E911 Document in some sense, but notions of property in cyberspace can be tricky. BellSouth noticed nothing wrong, because BellSouth still had their original copy. They had not been "robbed" of the document itself. Many people were supposed to copy this document -specifically, people who worked for the nineteen BellSouth "special services and major account centers," scattered throughout the Southeastern United States. That was what it was for, why it was present on a computer network in the first place: so that it could be copied and read -by telco employees. But now the data had been copied by someone who wasn't supposed to look at it.

February 1989 arrived. The Atlanta Three were living it up in Bell South's switches, and had not yet met their comeuppance. The Legion

was thriving. So was *Phrack* magazine. A good six months had passed since Prophet's AIMSX break-in. Prophet, as hackers will, grew weary of sitting on his laurels. "Knight Lightning" and "Taran King," the editors of *Phrack*, were always begging Prophet for material they could publish. Prophet decided that the heat must be off by this time, and that he could safely brag, boast, and strut.

So he sent a copy of the E911 Document…to Knight Lightning's BITnet account at the University of Missouri.

In February 1989, Prophet and Knight Lightning bargained electronically over the fate of this trophy. Prophet wanted to boast, but, at the same time, scarcely wanted to be caught.

For his part, Knight Lightning was eager to publish as much of the document as he could manage. Knight Lightning was a fledgling political-science major with a particular interest in freedom-of-information issues. He would gladly publish most anything that would reflect glory on the prowess of the underground and embarrass the telcos. However, Knight Lightning himself had contacts in telco security, and sometimes consulted them on material he'd received that might be too dicey for publication.

Prophet and Knight Lightning decided to edit the E911 Document so as to delete most of its identifying traits. First of all, its large "NOT FOR USE OR DISCLOSURE" warning had to go. Then there were other matters. For instance, it listed the office telephone numbers of several BellSouth 911 specialists in Florida. If these phone numbers were published in *Phrack*, the BellSouth employees involved would very likely be hassled by phone phreaks, which would anger BellSouth no end, and pose a definite operational hazard for both Prophet and *Phrack*.

So Knight Lightning cut the Document almost in half, removing the phone numbers and some of the touchier and more specific information. He passed it back electronically to Prophet; Prophet was still nervous, so Knight Lightning cut a bit more. They finally agreed that it was ready to go, and that it would be published in *Phrack* under the pseudonym, "The Eavesdropper."

And this was done on February 25, 1989.

The twenty-fourth issue of *Phrack* featured a chatty interview with co-ed phone-phreak "Chanda Leir," three articles on BITNET and its links to other computer networks, an article on 800 and 900 numbers by "Unknown User," "VaxCat's" article on telco basics (slyly entitled "Lifting Ma Bell's Veil of Secrecy,)" and the usual "Phrack World News."

The News section, with painful irony, featured an extended account of the sentencing of "Shadowhawk," an eighteen-year-old Chicago hacker who had just been put in federal prison by William J. Cook himself.

And then there were the two articles by "The Eavesdropper." The first was the edited E911 Document, now titled "Control Office Administration Of Enhanced 911 Services for Special Services and Major Account Centers." Eavesdropper's second article was a glossary of terms explaining the blizzard of telco acronyms and buzzwords in the E911 Document.

The hapless document was now distributed, in the usual *Phrack* routine, to a good one hundred and fifty sites. Not a hundred and fifty people, mind you -- a hundred and fifty sites, some of these sites linked to UNIX nodes or bulletin board systems, which themselves had readerships of tens, dozens, even hundreds of people.

This was February 1989. Nothing happened immediately. Summer came, and the Atlanta crew were raided by the Secret Service. Fry Guy was apprehended. Still nothing whatever happened to *Phrack*. Six more issues of *Phrack* came out, 30 in all, more or less on a monthly schedule. Knight Lightning and co-editor Taran King went untouched.

Phrack tended to duck and cover whenever the heat came down. During the summer busts of 1987 -- (hacker busts tended to cluster in summer, perhaps because hackers were easier to find at home than in college) -- *Phrack* had ceased publication for several months, and laid low. Several LoD hangers-on had been arrested, but nothing had happened to the *Phrack* crew, the premiere gossips of the underground. In 1988, *Phrack* had been taken over by a new editor, "Crimson Death," a raucous youngster with a taste for anarchy files.

1989, however, looked like a bounty year for the underground. Knight Lightning and his co-editor Taran King took up the reins again, and

Phrack flourished throughout 1989. Atlanta LoD went down hard in the summer of 1989, but *Phrack* rolled merrily on. Prophet's E911 Document seemed unlikely to cause *Phrack* any trouble. By January 1990, it had been available in *Phrack* for almost a year…. But then came the monster Martin Luther King Day Crash of January 15, 1990.

A flat three days later, on January 18, four agents showed up at Knight Lightning's fraternity house. One was Timothy Foley, the second Barbara Golden, both of them Secret Service agents from the Chicago office. Also along was a University of Missouri security officer, and Reed Newlin, a security man from Southwestern Bell, the RBOC having jurisdiction over Missouri. Foley accused Knight Lightning of causing the nationwide crash of the phone system.

Knight Lightning was aghast at this allegation. On the face of it, the suspicion was not entirely implausible -- though Knight Lightning knew that he himself hadn't done it. Plenty of hot-dog hackers had bragged that they could crash the phone system, however. "Shadowhawk," for instance, the Chicago hacker whom William Cook had recently put in jail, had several times boasted on boards that he could "shut down AT&T's public switched network." And now this event, or something that looked just like it, had actually taken place. The Crash had lit a fire under the Chicago Task Force. And the former fencesitters at Bellcore and AT&T were now ready to roll. The consensus among telco security -- already horrified by the skill of the BellSouth intruders -- was that the digital underground was out of hand. LoD and *Phrack* must go.

And in publishing Prophet's E911 Document, *Phrack* had provided law enforcement with what appeared to be a powerful legal weapon. Foley confronted Knight Lightning about the E911 Document.

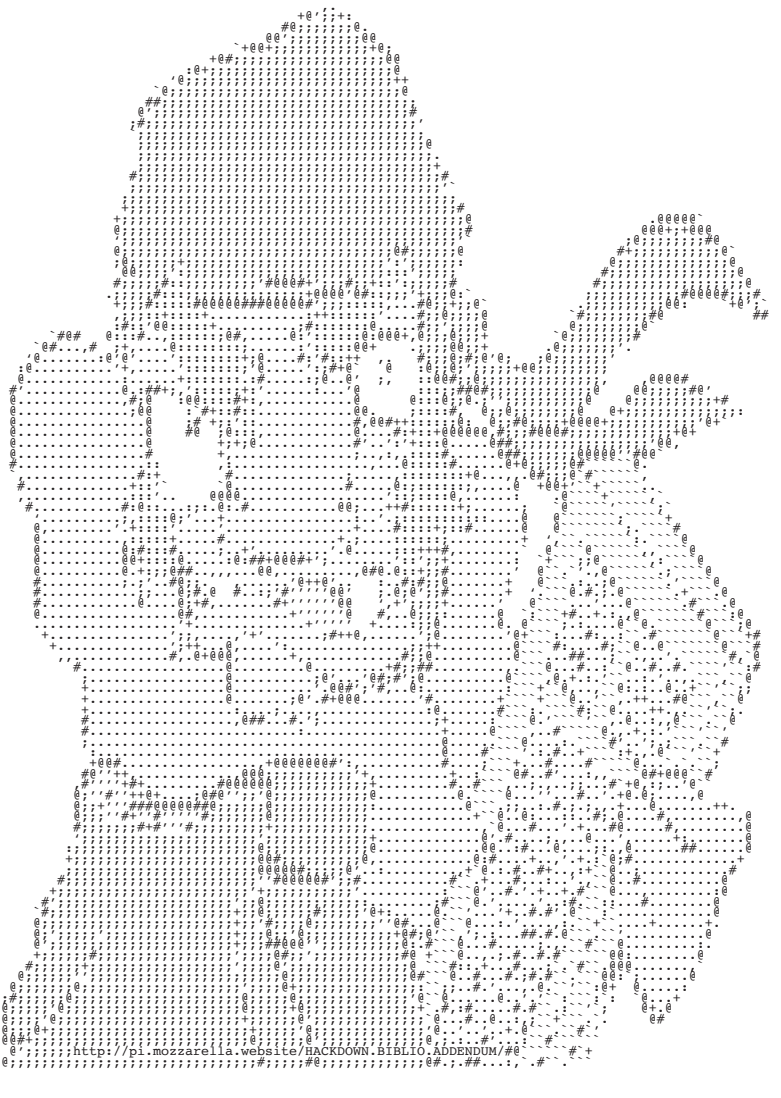
Knight Lightning was cowed. He immediately began "cooperating fully" in the usual tradition of the digital underground.

He gave Foley a complete run of *Phrack*, printed out in a set of three-ring binders. He handed over his electronic mailing list of *Phrack* subscribers. Knight Lightning was grilled for four hours by Foley and his cohorts. Knight Lightning admitted that Prophet had passed him the E911 Document, and he admitted that he had known it was stolen booty from a

hacker raid on a telephone company. Knight Lightning signed a statement to this effect, and agreed, in writing, to cooperate with investigators.

On Monday, Knight Lightning was summoned to Chicago, where he was further grilled by Foley and USSS veteran agent Barbara Golden, this time with an attorney present. And on Tuesday, he was formally indicted by a federal grand jury.

The trial of Knight Lightning, which occurred on July 24-27, 1990, was the crucial show-trial of the Hacker Crackdown.



[H]ere is a list of hacker groups compiled by the editors of *Phrack* on August 8, 1988.

The Administration.Advanced Telecommunications, Inc. ALIAS. American Tone Travelers. Anarchy Inc. Apple Mafia. The Association. Atlantic Pirates Guild.

Bad Ass Mother Fuckers. Bellcore. Bell Shock Force. Black Bag.

Camorra. C&M Productions. Catholics Anonymous. Chaos Computer Club. Chief Executive Officers. Circle Of Death. Circle Of Deneb. Club X. Coalition of Hi-Tech Pirates. Coast-To-Coast. Corrupt

Computing. Cult Of The Dead Cow. Custom Retaliations.

Damage Inc. D&B Communications. The Dange Gang. Dec Hunters. Digital Gang. DPAK.

Eastern Alliance. The Elite Hackers Guild. Elite Phreakers and Hackers Club. The Elite Society Of America. EPG. Executives Of Crime. Extasyy Elite.

Fargo 4A. Farmers Of Doom. The Federation. Feds R Us. First Class. Five O. Five Star. Force Hackers. The 414s.

Hack-A-Trip. Hackers Of America. High Mountain Hackers. High Society. The Hitchhikers.

IBM Syndicate. The Ice Pirates. Imperial Warlords. Inner Circle. Inner Circle II. Insanity Inc. International Computer Underground Bandits.

Justice League of America.

Kaos Inc. Knights Of Shadow. Knights Of The Round Table.

League Of Adepts. Legion Of Doom. Legion Of Hackers. Lords Of Chaos. Lunatic Labs,

Unlimited.

Master Hackers. MAD!
The Marauders. MD/PhD.
Metal Communications, Inc.
MetalliBashers, Inc. MBI. Metro
Communications. Midwest
Pirates Guild.

NASA Elite. The NATO
Association. Neon Knights.
Nihilist Order.

Order Of The Rose. OSS.

Pacific Pirates Guild. Phantom
Access Associates. PHido
PHreaks. The Phirm. Phlash.
PhoneLine Phantoms. Phone

Phreakers Of America. Phortune 500. Phreak Hack Delinquents. Phreak Hack Destroyers. Phreakers, Hackers, And Laundromat Employees Gang (PHALSE Gang). Phreaks Against Geeks. Phreaks Against Phreaks Against Geeks. Phreaks and Hackers of America. Phreaks Anonymous World Wide. Project Genesis. The Punk Mafia.

The Racketeers. Red Dawn Text Files. Roscoe Gang.

SABRE. Secret Circle of Pirates. Secret Service. 707

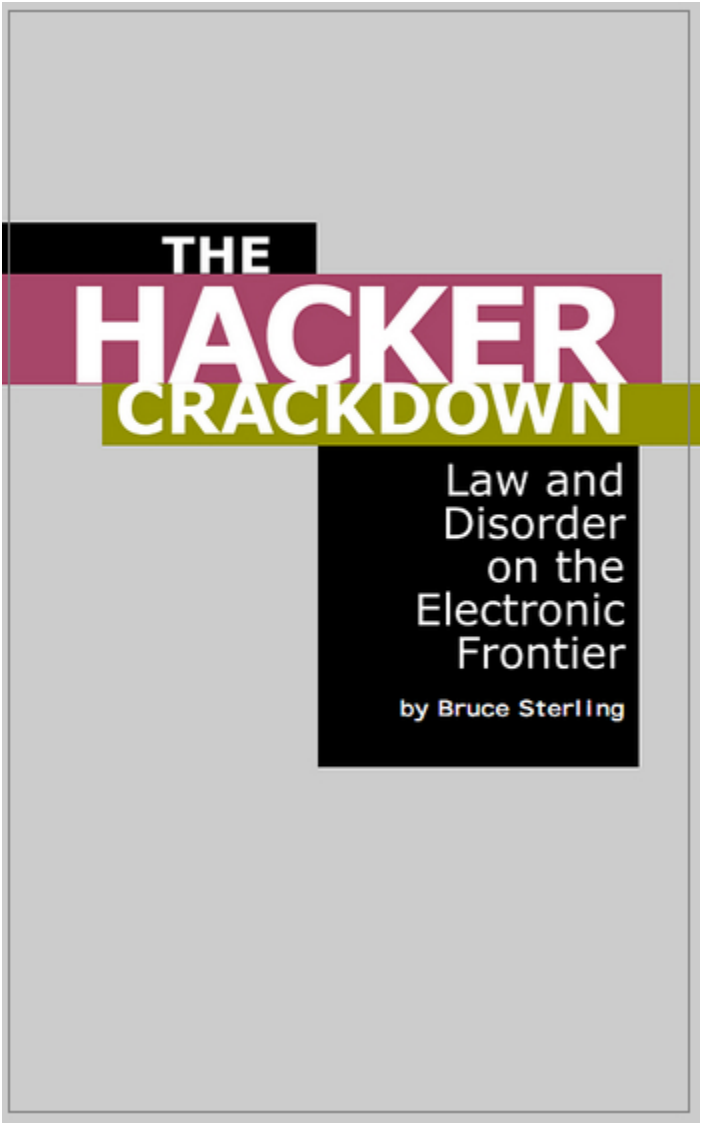
Club. Shadow Brotherhood. Sharp Inc. 65C02 Elite. Spectral Force. Star League. Stowaways. Strata-Crackers.

Team Hackers ‘86. Team Hackers ‘87. TeleComputist Newsletter Staff. Tribunal Of Knowledge. Triple Entente. Turn Over And Die Syndrome (TOADS). 300 Club. 1200 Club. 2300 Club. 2600 Club. 2601 Club. 2AF.

The United Soft WareZ Force. United Technical Underground.

Ware Brigade. The Warelords. WASP.

Contemplating this list is an impressive, almost humbling business. As a cultural artifact, the thing approaches poetry.



Part 4: The Civil Libretarians:

It has been my practice throughout this book to refer to hackers only by their "handles." There is little to gain by giving the real names of these people, many of whom are juveniles, many of whom have never been convicted of any crime, and many of whom had unsuspecting parents who have already suffered enough.

But the trial of Knight Lightning on July 24-27, 1990, made this particular "hacker" a nationally known public figure. It can do no particular harm to himself or his family if I repeat the long-established fact that his name is Craig Neidorf (pronounced NYE-dorf).

Neidorf's jury trial took place in the United States District Court, Northern District of Illinois, Eastern Division, with the Honorable Nicholas J. Bua presiding. The United States of America was the plaintiff, the defendant Mr. Neidorf. The defendant's attorney was Sheldon T. Zenner of the Chicago firm of Katten, Muchin and Zavis.

The prosecution was led by the stalwarts of the Chicago Computer Fraud and Abuse Task Force: William J. Cook, Colleen D. Coughlin, and David A. Glockner, all Assistant United States Attorneys. The Secret Service Case Agent was Timothy M. Foley.

It will be recalled that Neidorf was the co-editor of an underground hacker "magazine" called *Phrack*. *Phrack* was an entirely electronic publication, distributed through bulletin boards and over electronic networks. It was amateur publication given away for free. Neidorf had never made any money for his work in *Phrack*. Neither had his unindicted co-editor "Taran King" or any of the numerous *Phrack* contributors. The Chicago Computer Fraud and Abuse Task Force, however, had decided to prosecute Neidorf as a fraudster. To formally admit that *Phrack* was a "magazine" and Neidorf a "publisher" was to open a prosecutorial Pandora's Box of First Amendment issues.

Neidorf had been urged to plead guilty. But Neidorf was a political science major and was disinclined to go to jail for "fraud" when he had not made any money, had not broken into any computer, and had been publishing a magazine that he considered protected under the First Amendment.

Neidorf's trial was the *only* legal action of the entire Crackdown that

actually involved bringing the issues at hand out for a public test in front of a jury of American citizens.

Neidorf, too, had cooperated with investigators. He had voluntarily handed over much of the evidence that had led to his own indictment. He had already admitted in writing that he knew that the E911 Document had been stolen before he had "published" it in *Phrack* -- or, from the prosecution's point of view, illegally transported stolen property by wire in something purporting to be a "publication."

But even if the "publication" of the E911 Document was not held to be a crime, that wouldn't let Neidorf off the hook. Neidorf had still received the E911 Document when Prophet had transferred it to him from Rich Andrews' Jolnet node. On that occasion, it certainly hadn't been "published" -- it was hacker booty, pure and simple, transported across state lines.

The Chicago Task Force led a Chicago grand jury to indict Neidorf on a set of charges that could have put him in jail for thirty years. When some of these charges were successfully challenged before Neidorf actually went to trial, the Chicago Task Force rearranged his indictment so that he faced a possible jail term of over sixty years! As a first offender, it was very unlikely that Neidorf would in fact receive a sentence so drastic; but the Chicago Task Force clearly intended to see Neidorf put in prison, and his conspiratorial "magazine" put permanently out of commission. This was a federal case, and Neidorf was charged with the fraudulent theft of property worth almost eighty thousand dollars.

With the Document itself to hand, however, exactly as it was published (in its six-page edited form) in *Phrack*, the reader may be able to verify a few statements of fact about its nature. First, there is no software, no computer code, in the Document. It is not computer-programming language like FORTRAN or C++, it is English; all the sentences have nouns and verbs and punctuation. It does not explain how to break into the E911 system. It does not suggest ways to destroy or damage the E911 system.

There are no access codes in the Document. There are no computer passwords. It does not explain how to steal long distance service. It does not explain how to break in to telco switching stations. There is nothing

in it about using a personal computer or a modem for any purpose at all, good or bad.

Close study will reveal that this document is not about machinery. The E911 Document is about *administration*. It describes how one creates and administers certain units of telco bureaucracy: Special Service Centers and Major Account Centers (SSC/MAC). It describes how these centers should distribute responsibility for the E911 service, to other units of telco bureaucracy, in a chain of command, a formal hierarchy. It describes who answers customer complaints, who screens calls, who reports equipment failures, who answers those reports, who handles maintenance, who chairs subcommittees, who gives orders, who follows orders, who tells *whom* what to do. The Document is not a "roadmap" to computers. The Document is a roadmap to *people*.

As an aid to breaking into computer systems, the Document is *useless*. As an aid to harassing and deceiving telco people, however, the Document might prove handy (especially with its Glossary, which I have not included). An intense and protracted study of this Document and its Glossary, combined with many other such documents, might teach one to speak like a telco employee. And telco people live by *speech* -- they live by phone communication. If you can mimic their language over the phone, you can "social-engineer" them. If you can con telco people, you can wreak havoc among them. You can force them to no longer trust one another; you can break the telephonic ties that bind their community; you can make them paranoid. And people will fight harder to defend their community than they will fight to defend their individual selves.

This was the genuine, gut-level threat posed by *Phrack* magazine. The real struggle was over the control of telco language, the control of telco knowledge. It was a struggle to defend the social "membrane of differentiation" that forms the walls of the telco community's ivory tower -- the special jargon that allows telco professionals to recognize one another, and to exclude charlatans, thieves, and upstarts. And the prosecution brought out this fact. They repeatedly made reference to the threat posed to telco professionals by hackers using "social engineering."

However, Craig Neidorf was not on trial for learning to speak like a professional telecommunications expert. Craig Neidorf was on trial for

access device fraud and transportation of stolen property. He was on trial for stealing a document that was purportedly highly sensitive and purportedly worth tens of thousands of dollars.

Zenner, half-a-dozen other attorneys, Nagle, Neidorf, and computer-security expert Dorothy Denning, all pored over the E911 Document line-by-line.

On the afternoon of July 25, 1990, Zenner began to cross-examine a woman named Billie Williams, a service manager for Southern Bell in Atlanta. Ms. Williams had been responsible for the E911 Document.

Ms. Williams had been called as a witness for the prosecution, and had gamely tried to explain the basic technical structure of the E911 system, aided by charts.

Zenner now asked whether the charts she had been using to explain the mechanics of E911 system were "proprietary," too. Were they *public information*, these charts, all about PSAPs, ALIs, nodes, local end switches? Could he take the charts out in the street and show them to anybody, "without violating some proprietary notion that BellSouth has?"

Ms Williams showed some confusion, but finally agreed that the charts were, in fact, public.

"But isn't this what you said was basically what appeared in *Phrack*?"

Ms. Williams denied this.

Zenner now pointed out that the E911 Document as published in Phrack was only half the size of the original E911 Document (as Prophet had purloined it). Half of it had been deleted -- edited by Neidorf.

Ms. Williams countered that "Most of the information that is in the text file is redundant."

Zenner continued to probe. Exactly what bits of knowledge in the Document were, in fact, unknown to the public? Locations of E911 computers? Phone numbers for telco personnel? Ongoing maintenance

subcommittees? Hadn't Neidorf removed much of this?

Then he pounced. "Are you familiar with Bellcore Technical Reference Document TR-TSY-000350?" It was, Zenner explained, officially titled "E911 Public Safety Answering Point Interface Between 1-1AESS Switch and Customer Premises Equipment." It contained highly detailed and specific technical information about the E911 System. It was published by Bellcore and publicly available for about $20.

He showed the witness a Bellcore catalog which listed thousands of documents from Bellcore and from all the Baby Bells, BellSouth included. The catalog, Zenner pointed out, was free. Anyone with a credit card could call the Bellcore toll-free 800 number and simply order any of these documents, which would be shipped to any customer without question. Including, for instance, "BellSouth E911 Service Interfaces to Customer Premises Equipment at a Public Safety Answering Point."

Zenner gave the witness a copy of "BellSouth E911 Service Interfaces," which cost, as he pointed out, $13, straight from the catalog. "Look at it carefully," he urged Ms. Williams, "and tell me if it doesn't contain about twice as much detailed information about the E911 system of BellSouth than appeared anywhere in *Phrack*."

...[T]he "value" of the Document had been blown to smithereens. It wasn't worth eighty grand. According to Bellcore it was worth thirteen bucks. And the looming menace that it supposedly posed had been reduced in instants to a scarecrow. Bellcore itself was selling material far more detailed and "dangerous," to anybody with a credit card and a phone.

Neidorf had never urged Prophet to defraud anyone, or to steal anything. Prophet also admitted that he had never known Neidorf to break in to any computer. Prophet said that no one in the Legion of Doom considered Craig Neidorf a "hacker" at all. Neidorf was not a UNIX maven, and simply lacked the necessary skill and ability to break into computers. Neidorf just published a magazine.

On Friday, July 27, 1990, the case against Neidorf collapsed. Cook moved to dismiss the indictment, citing "information currently available to us that was not available to us at the inception of the trial." Judge Bua praised the

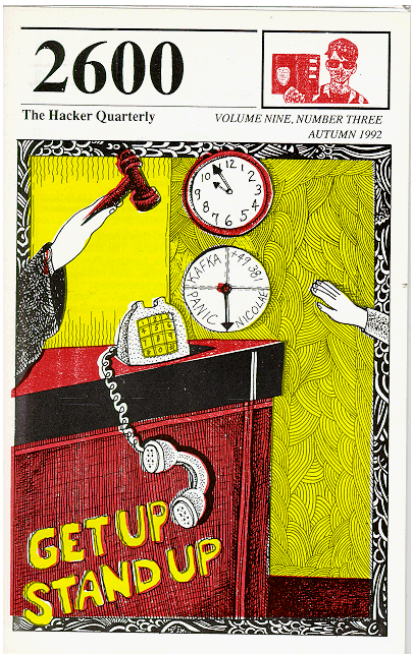
prosecution for this action, which he described as “very responsible,” then dismissed a juror and declared a mistrial.

Neidorf was a free man. His defense, however, had cost himself and his family dearly. Months of his life had been consumed in anguish; he had seen his closest friends shun him as a federal criminal. He owed his lawyers over a hundred thousand dollars, despite a generous payment to the defense by Mitch Kapor.

Neidorf was not found innocent. The trial was simply dropped. Nevertheless, on September 9, 1991, Judge Bua granted Neidorf’s motion for the “expungement and sealing” of his indictment record. The United States Secret Service was ordered to delete and destroy all fingerprints, photographs, and other records of arrest or processing relating to Neidorf’s indictment, including their paper documents and their computer records.

Legally speaking, the Neidorf case was not a sweeping triumph for anyone concerned. No constitutional principles had been established. The issues of “freedom of the press” for electronic publishers remained in legal limbo.

Excerpt From:



BOOK REVIEW

Hacker Crackdown: Law and Disorder on the Electronic Frontier
by Bruce Sterling
$23.00, Bantam Books, 313 pages
Review by The Devil's Advocate

The denizens of cyberspace have long revered Bruce Sterling as one of cyberfiction's earliest pioneers. Now, Sterling has removed his steel-edged mirrorshades to cast a deep probing look into the heart of our modern-day electronic frontier. The result is *The Hacker Crackdown*, the latest account of the hacker culture and Sterling's first foray into non-fiction.

At first glance, *Crackdown* would appear to follow in the narrative footsteps of *The Cuckoo's Egg* and *Cyberpunk*. The setting is cyberspace, 1990: year of the AT&T crash and the aftermath of Ma Bell's fragmentation; year of Operation Sundevil, the Atlanta raids, and the Legion of Doom breakup; year of the E911 document and the trial of Knight Lightning; year of the hacker crackdown, and the formation of that bastion of computer civil liberties, the Electronic Frontier Foundation. Unlike *Cuckoo* and *Cyberpunk*, however, Sterling's work does not center around characters and events so much as the parallels he draws between them. Crackdown is far less story and far more analysis. Crackdown is also personal. Missing is the detached and unbiased aloofness expected of a journalist. Intermingled with the factual accounts, for instance, are Sterling's keen wit and insight:

"In my opinion, any teenager enthralled by computers, fascinated by the ins and outs of computer security, and attracted by the lure of specialized forms of knowledge and power, would do well to forget all about hacking and set his (or her) sights on becoming a Fed. Feds can trump hackers at almost every single thing hackers do, including gathering intelligence, undercover disguise, trashing, phone-tapping, building dossiers, networking, and infiltrating computer systems...."

Sterling is fair. He effectively gets into the psyche of hacker and enforcer alike, oftentimes poking fun at the absurdity in both lines of reasoning. To hackers he is honest and brutal: "Phone phreaks pick on the weak." Before the advent of ANI, hackers exploited AT&T. Then they drifted to the Baby Bells where security was less than stellar. From there it was a gradual regression all the way down to local PBX's, the weakest kids on the block, and certainly not the megacorporate entities that give rise to "steal from the rich" Robin Hood excuses. To enforcers he is equally brutal, charting a chronicle of civil liberty abuses by the FBI, Secret Service, and local law enforcement agencies.

Perhaps the best reason to read *Crackdown* is to learn what other books have neglected to focus on: the abuses of power by law enforcement. Indeed, it is these abuses that are the main focus of Sterling's work. One by one he gives a grim account of the raids of 1990, the Crackdown or cultural genocide that was to have as its goal the complete and absolute extinction of hacking in all of its manifestations.

On February 21, 1990, Robert Izenberg was raided by the Secret Service. They shut down his UUCP site, seized twenty thousand dollars' worth of professional equipment as "evidence," including some 140 megabytes of files, mail, and data belonging

to himself and his users. Izenberg was neither arrested nor charged with any crime. Two years later he would still be trying to get his equipment back.

On March 1, 1990, twenty-one-year- old Erlk Bloodaxe was awakened by a revolver pointed at his head. Secret Service agents seized everything even remotely electronic, including his telephone. Bloodaxe was neither arrested nor charged with any crime. Two years later he would still be wondering where all his equipment went.

Mentor was yet another victim of the Crackdown. Secret Service agents "rousted him and his wife from bed in their underwear," and proceeded to seize thousands of dollars' worth of work-related computer equipment, including his wife's incomplete academic thesis stored on a hard disk. Two years later and Mentor would still be waiting for the return of his equipment.

Then came the infamous Steve Jackson Games raid. Again, no one was arrested and no charges were filed. "Everything appropriated was officially kept as 'evidence' of crimes never specified."

Bruce Sterling explains (in an unusual first-person shift in the narrative) that it was this raid above all else which compelled him to "put science fiction aside until l had discovered what had happened and where this trouble had come from."

Crackdown culminates with what is perhaps the most stunning example of injustice outside of the Steve Jackson raid. Although the trial of Knight Lightning is over, its bittersweet memories still linger in the collective mind of cyberspace. This, after all, was the trial in which William Cook maliciously tried (and failed) to convict a fledgling teenage journalist for printing a worthless garble of bureaucratic dreck by claiming that it was in fact a $79,449 piece of "proprietary" code. In an effort to demonstrate the sheer boredom and tediousness of the E911 document, and the absurdity of Cook's prosecution, *Crackdown* includes a hefty sampling of this document (at a savings of over $79,449 by Cook's standards).

More than any other book to date, *Crackdown* concentrates on the political grit and grime of computer law enforcement, answering such perennial favorites as why does the Secret Service have anything to do with hackers anyway? In Crackdown we learn that something of a contest exists between the Secret Service and the FBI when it comes to busting hackers. Also touched upon are the "waffling" First Amendment issues that have sprung forth from cyberspace.

Crackdown is a year in the life of the electronic frontier. For some, a forgotten mote of antiquity; for others, a spectral preamble of darker things to come. But for those who thrive at the cutting edge of cyberspace, Crackdown is certain to bridge those distant points of light with its account of a year that will not be forgotten.

Excerpt From:

==Phrack Inc.==

Volume Four, Issue Forty-One, File 2 of 13

[-=:< Phrack Loopback >:=-]

By Dispater & Mind Mage

Two New Hardcovers November 24, 1992

~~~~~~~~~~~~~~~~~~

by Alan J. Rothman (New York Law Journal)(Page 5)

During the opening sequence of the classic English television series “The Prisoner,” the lead character known only as Number 6 (brilliantly played by Patrick McGoohan) is abducted and taken to a secret location called “The Village.” He desperately pleads with his captors “What do you want?” Their grim response is “Information.” Through 17 thrilling episodes, his kidnappers staged elaborate high-tech ruses to find out why he quit work as a spy.

Had this story been set in the 1990s rather than the 1960s, all The Village’s proprietors would have needed was a PC and a modem. They could have assembled a composite of Number 6’s movements by cross-referencing records from any of the commercial data bases containing the details of nearly everyone’s daily activities. Then with a bit of ingenuity, they could have tried to steal even more information by hacking into other restricted data systems.

No longer fiction, but common fact, the billowing growth in the computers and telecommunications networks everywhere is generating urgent legal issues regarding the content, usage and ownership of the data coursing through them. Dilemmas have also surfaced concerning the responsibilities of the businesses which gather, sift and repackage such information. Indeed, a critical juncture has now been reached where the basic constitutional rights of privacy and expression are colliding with the ever-expanding reach of modern technology.

Two well-crafted books have recently been published which together frame the spectrum of relevant individual rights issues in these areas with uncanny symmetry. Fortunately, neither degenerates into a “computers are bad” jeremiad. Rather, they portray an appropriate balance between the virtues of computerization and disturbing cases of technological misuse for wrongful commercial and governmental ends.

Presenting array of new forms of electronic encroachment on personal privacy is Jeffrey Rothfeder’s alarming new book, “Privacy
~~~~~~~~~~~~~~~~~~

for Sale: How Computerization Has Made Everyone's Private Life an Open Secret" (Simon & Schuster, 224 pages, $22). He offers the chilling thesis that anyone can find out nearly anything regarding anybody and there is nowhere left to hide. He convincingly states his case in a concise and insightful exploration of the trends and abuses in the mass processing of personal data.

The fascinating mechanics of how and where information about virtually every aspect of our lives is gathered and then computerized are extensively described. The most productive fonts include medical records, credit histories, mortgage applications, subscription lists, phone records, driver's licenses and insurance forms. Yet notwithstanding the legitimate commercial and regulatory reasons for providing these facts, the author carefully documents another more deeply hidden and troubling consequence of volunteering such information: It is constantly resold, combined with other sources and reused without your knowledge or permission for purposes entirely different from those you first intended.

Mr. Rothfeder alleges the most perilous result of these activities is the growing and highly organized sales, integration and cross-matching of databases. Businesses and government entities now have sophisticated software to generate complex demographic profiles about individuals, populations and geographic areas. In turn, these computer-generated syntheses are increasingly used for invasive and discriminatory purposes.

Numerous examples of such misuse are cited, ranging from slightly annoying to purely horrifying. The astonishing breadth of this roster includes the sale of driver's license information with height weight specifications to clothes marketers for tall men and thin women, purchases of credit histories and workmen's compensation claims reports by prospective employers who believe this material is indicative of a job applicant's character, and the creation of "propensity files" by federal agencies to identify people who have not committed any offense but might likely be criminals.

Two additional problems pervade the trafficking of intimate information. First, there is little or no federal legislation to effectively protect people from certain problems presented in the book. For example, the release of medical records thought to be "confidential" is virtually unprotected.

Second, it can be extremely difficult to have false entries corrected before they have a ripple effect on your other data. Beyond the common tales of frustration at clearing up a faulty credit report, Mr. Rothfeder relates the case of a man denied any health insurance because his medical records contained an erroneous report he was HIV positive.

JOURNEY IN CYBERSPACE

Turning to a much more accurate account, author Bruce Sterling takes readers into the ethereal realm of "cyberspace" where computers, networks, and electronic bulletin boards systems (BBS) are linked together by phone. In his first non-fiction work, "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" (Bantam, 328 pages, $23), he chronicles the U.S. government's highly visible efforts in 1990 to prosecute "hackers" it suspected of committing crimes by PC and modem. However, Mr. Sterling distinguishes this term as being more about active computer enthusiasts, most of whom have never committed any wrongdoing. The writer's other credits include some highly regarded "cyberpunk" science fiction, where computer technology is central to the plots and characters.

The "crackdown" detailed by the author began with the crash of AT&T's long-distance phone system on January 15, 1990. Although it has never been proven that hackers were responsible, this event served as the final catalyst to spur federal law enforcement agencies into concerted action against a suspected underground of computer criminals. A variety of counter-operations were executed. Most notable was Operation Sundevil the following May when agents around the country seized 42 computer systems, 23,000 diskettes, and halted 25 BBS's where the government believed hackers were exchanging tips of the trade.

Some of the government's resulting prosecutions through their nationwide efforts were moderately successful. However, the book's dramatic centerpiece is the trial of Craig Neidorf (a.k.a. Knight Lightning). Mr. Neidorf was a contributor to Phrack, an electronic magazine catering to hackers, available on various BBS's.

In January 1989, another hacker named "Prophet" transmitted a document he pilfered from BellSouth's computers regarding the 911 emergency system to Neidorf. Together they edited the text, which Neidorf then published in Phrack. In July 1990, he was placed on trial for federal charges of entering a fraudulent scheme with Prophet to steal this document. The government alleged it was worth $79,499 and that its publication threatened emergency operations. To the prosecutor's dismay, the case was dropped when the defense proved the same material was publicly available for only $13.

With insight and style, Mr. Sterling uses this and other events to cast intriguing new spins on applicable civil liberties issues.

Are the constitutional guarantees of freedom of expression and assembly fully extended to BBS dialogs and gatherings? What degree of privacy can be expected for personal data on systems

which may be subject to surreptitious entry? Are hackers really breaking any laws when merely exploring new systems? Is posting a message or document on a BBS considered a “publication”? Should all BBS’s be monitored just because of their potential for illegal activity? What are the responsibilities of BBS operators for the contents of, and access to, their systems?

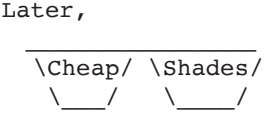
The efforts of Mitchell Kapor, the co-developer of Lotus 123 and now chairman of ONtechnology, are depicted as a direct response to such issues raised by the crackdown. Mr. Kapor assembled a prominent group of fellow computer professionals to establish the Electronic Frontier Foundation (EFF), dedicated to education and lobbying for free speech and expression in electronic media. As well, EFF has provided support to Craig Neidorf and others they consider wrongly charged with computer crime.

Weighty legal matters aside, the author also embellishes his story with some colorful hacker lore. These denizens of cyberspace are mostly young men in their late teens or early twenties, often fueled by junk food and propelled by macho. Perhaps their most amusing trait is the monikers they adopt -- Bloodaxe, Shadowhawk, and of course, Phiber Optik.

Someone else, a non-hacker involuntary given the pseudonym “Number 6,” knew his every act was continually being monitored and recorded against his will. As a manifestation of resistance to this relentless surveillance, he often bid farewell to other citizens of the Village with a sarcastic “Be seeing you.” Today, the offerings of authors Rothfeder and Sterling provide a resounding “And you” as a form of rejoinder (often uttered by The Village’s citizens as well), to publicize the ironic diversity threats wrought by information technology.

Number 6 cleverly managed to escape his fictional captivity in The Village during the final (and mind-boggling) episode of The Prisoner. However, based on the compelling evidence presented in these two books, the protection of individual rights in the reality of today’s evolving “global village” of computer networks and telecommunications may not be so neatly resolved.

Later,



Works excerpted:

* Advocate, The Devil's. "Book Review." Review of The Hacker Crackdown Law and Disorder on the Electronic Frontier, by Bruce Sterling. 2600: The Hacker Quarterly, 9, no. 3 (Autumn 1992): 67.225.133.110/~gbpprorg/2600/crackdown.txt

* Cowboy, Datastream. Phrack World News. Part 3 of 3. PWN Quicknotes, no. 10. Phrack, 4, no. 41 (December 31, 1992): http://phrack.org/issues/41/13.html#article

* Rothman, Alan J. "Two New Hardcovers." Phrack Loopback. Review of The Hacker Crackdown Law and Disorder on the Electronic Frontier, by Bruce Sterling. Phrack, 4, no.41 (December 31, 1992): http://phrack.org/issues/41/2.html#article

* Sterling, Bruce. "The Hackers Who Came In From The Cold" June 21–23, 1991. Phrack World News Special Edition IV (CyberView 91). Phrack, 3, no. 33 (September 15, 1991): http://phrack.org/issues/33/10.html#article

* Sterling, Bruce. 1992. The Hacker Crackdown: Law and Disorder on the Electronic Frontier, trans. Bryan O'Sullivan (Literary Freeware, 1994): www.mit.edu/hacker/hacker.html