Volume 6, Spring Issue, 1993

BOOK NOTE

THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER

By Bruce Sterling.
New York, New York: Bantam Books. 1992.
Pp. 328. $23.00 (hard).

In 1989 and 1990, federal and state agents across the United States cracked down on the nation's computer underground. The most ambitious offensive, Operation Sundevil, resulted in the seizure of forty-two computer systems and 23,000 floppy disks in cities from New York to Los Angeles (pp. 156-59). The Chicago Computer Fraud and Abuse Task Force conducted ten hacker raids in 1989 and 1990. These actions brought to the national spotlight numerous concerns about privacy and freedom in the electronic arena.

In *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*, Bruce Sterling colorfully describes the personalities and institutions behind the "great hacker dragnet of 1990" (p. 24). He approaches this subject by focusing on the four principal factions that participated in the crackdown: hackers, telecommunications companies ("telcos" like AT&T, MCI and Sprint), law enforcement officials, and civil libertarians (who rushed to the scene in the crackdown's wake). Relying on personal interviews and extensive field research, Sterling presents the problems and concerns faced by each group. He concludes with a glowing description of the First Conference on Computers, Freedom and Privacy, at which representatives from these mutually suspicious factions gathered and, in true League of Nations fashion, celebrated a newfound understanding.

Sterling's perspective as a science fiction writer gives him unique insight into the psyche of the computer hacker.[1] Unlike other popular accounts, Sterling's does not depict hackers as twisted geniuses bent on crashing telephone systems and stealing missile-launch sequences.[2]

---

1. Bruce Sterling has written four novels, co-authored a novel with William Gibson, the creator of the term "cyberspace," and has edited the science fiction anthology MIRRORSHADES (1990).

2. *See, e.g.*, KATIE HAFNER & JOHN MARKOFF, CYBERPUNK: OUTLAWS AND HACKERS ON THE COMPUTER FRONTIER, Pt. 1 (1991) (describing the exploits of a notorious band of

Rather, he divides hackers into essentially two camps: one good, the other bad. Good hackers are merely law-abiding citizens with a deep understanding of computers. "Hacking" to them comprises:

> the free-wheeling intellectual exploration of the highest and deepest potential of computer systems . . . the determination to make access to computers and information as free and open as possible . . . [and] the heartfelt conviction that beauty can be found in computers, that the fine aesthetic in a perfect program can liberate the mind and spirit (p. 53).

They are "the postmodern electronic equivalent of the cowboy and mountain man" (p. 54); and they "fiercely and publicly resist any besmirching of the noble title of hacker" (p. 55).

These upstanding citizens, unfortunately, have darker brothers—the "underground" hackers. Sterling traces the origin of underground hacking to the telephone fraud schemes of Abbie Hoffman and the Yippie movement of the 1960s. Many underground hackers retain this anti-establishment viewpoint. The majority of underground hackers, however, are not political ideologues. Primarily disaffected male teenagers, they are motivated, Sterling argues, by a need for technological empowerment (pp. 62-63). At the keyboard they consider themselves elite: capable of, and therefore justified in, "transcending" the oppressive rules of their intellectual inferiors (pp. 58, 62). Moreover, they are typically unconcerned with money. Their motivation, he contends, derives from the desire for technical mastery and peer recognition (p. 95).

People who steal credit card numbers and steal services from phone companies ("phreak") are not necessarily hackers. Fraud, the author contends, does not require the same level of computer expertise as hacking, even when the fraud is committed with computers via telephone lines. The bluntness and greed of phreaks, he argues, are looked down upon by the elite computer underground (p. 61). Of course, true hackers may need to crack private computer systems to quench their thirst for knowledge. Their harmless intellectual explorations, he argues, should not incur criminal penalties.[3]

---

computer criminals).

3. "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" (p. 63).

The real villains in Sterling's account are the myopic corporate behemoths who do not understand their own complex computer systems, but jealously guard every scrap of information hidden within them.[4] To Sterling and the hackers, ignorance appears to be the greatest crime of all.

Although Sterling's characterizations often ring true, his apologia for the hackers may go too far. He fails to address two major rationales for restricting hacker activity (the harm caused to and the invasion upon other computer users) while attributing the crackdown to something like a government-industry conspiracy against harmless teenagers.

Despite the author's sympathies, hackers have caused real harm to innocent people. Sterling pays insufficient attention to incidents such as the devastating "rtm" virus of 1988, which crippled civilian and government computers across the country,[5] and the computer espionage of a young German hacker popularized in Clifford Stoll's account *The Cuckoo's Egg*.[6] These events, as well as the recent "Michelangelo" virus[7] and a hacker-induced disruption of 911 service in Toronto,[8] suggest that the telcos were not merely paranoid when they demanded that police take action against computer intruders. Rather, they were responding to real threats of computer down-time, destruction or theft of valuable data, and interruption of essential services.

Sterling might counter that such harm is caused by malicious computer criminals and not "pure" hackers, who seek only to expand their knowledge and skill. Even if relevant, such is not always the case. Even

---

4. According to the author, the telcos, in conjunction with other corporate victims of computer fraud, were the primary movers behind the hacker crackdown. He explains that telephone fraud is not a new phenomenon, that "[e]ver since telephones began to make money, there have been people willing to rob and defraud phone companies" (p. 48). However, by the late 1980s the telcos were suffering from a host of internal and regulatory problems that decreased their already low tolerance for the theft of services by "phone phreaks" and intrusion into their systems by hackers (pp. 19-20, 23). The final straw for the telcos came on January 15, 1990. On that date, a software error (unrelated to hacker activity) caused a chain reaction in AT&T's nationwide switching circuitry. During the nine-hour crash, sixty-thousand people lost their phone service and seventy million calls went uncompleted (p. 1). Although the actual software problem was quickly identified, rumors of hacker tampering abounded (pp. 22-23). "It was easier to believe . . . that some evil person, or evil group had done this. . . ." (p. 39).

5. *See* HAFNER & MARKOFF, *supra* note 2, Pt. 2.

6. CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

7. *See* John Markoff, *Computer Users Plot To Evade Virus*, N.Y. TIMES, Mar. 6, 1993, at A14.

8. *See Teen Hacker Causes Havoc in 911 Service*, TORONTO STAR, Oct. 7, 1992, at A1.

the most elite hacker can make mistakes while exploring an alien system, and such mistakes can be as damaging to a computer system as deliberate malfeasance.[9] Moreover, even the most elite hacker can succumb to the temptations of stolen credit and free long distance service. For example, elite hacker Mark Abene, a.k.a. "Phiber Optik," whom Sterling describes as "unworldly and uncriminal" (p. 245) and "a splendid example of the computer intruder as committed dissident," (p. 244) was recently indicted, along with four fellow hackers, on charges including stealing credit card information and corrupting computer databases.[10]

The author also gives little weight to the privacy interests that are violated by hacker intrusions. Although he discusses at length the hackers' view that they should have unfettered freedom to explore the computer networks of the world,[11] he fails to mention that computer users have, by statute and common law, a right to some degree of privacy in their files and data.[12] Nor does this right to privacy seem unreasonable: computer users *should* have as much right to be secure in their electronic mail and personal files as in their homes and personal effects.[13] That is,

---

9. For example, Robert T. Morris, the son of a celebrated computer security expert, is reported to have intended no harm when he released a seemingly innocuous "worm" program into the national Internet computer network. *See* HAFNER & MARKOFF, *supra* note 2, Pt. 2. The "rtm" worm, however, proliferated at an unexpectedly high rate and ultimately brought computer systems across the country to a crashing halt. *Id.*

10. *See* Winn Schwartau, *Hackers Indicted for Infiltrating Corporate Network*, INFOWORLD, July 27, 1992, at 56.

11. He describes the philosophy of hacker guru "Emmanuel Goldstein" in stating that:

> [T]echnical 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 liberty and free initiative of the individual techno-rat (pp. 64-65).

This Nietzschean theme is repeated throughout hacker literature. *See, e.g.*, Philip Elmer-Dewitt, *Cyberpunk!*, TIME, Feb. 8, 1993, at 58 (noting that one of the central ideas of cyberpunk is that "[a] good piece of information-age technology will eventually get into the hands of those who can make the best use of it, despite the best efforts of the censors, copyright lawyers and datacops").

12. Thirty-eight states have criminal statutes prohibiting unauthorized access to a computer system. *See* 1 GUIDE TO COMPUTER LAW (CCH) ¶ 9420 (1989).

13. Privacy in the electronic arena has been the subject of much commentary. *See, e.g.*, Henry H. Perritt, Jr., *Tort Liability, The First Amendment, and Equal Access to Electronic Networks*, HARV. J.L. & TECH., Spring 1992, at 108-10; Terri A. Cutrera, *The Constitution in Cyberspace: The Fundamental Rights of Computer Users*, 60 UMKC L. REV. 139 (1991); Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal*

computers users should be free from intrusions either by the state or by the merely curious and bored.

This is not to say, however, that the 1990 hacker crackdown was conducted in an exemplary, or even acceptable, manner. Sterling should be congratulated for drawing attention to the methods used by the police and the Secret Service to achieve their goals. In particular, he describes at length the trial of Craig Neidorf, a hacker known in the underground as "Knight Lightning" (pp. 128-36, 250-53). Neidorf was arrested in 1990 for publishing an electronic "magazine" called *Phrack*, which he and a friend transmitted to electronic bulletin boards across the country. The February 25, 1989, issue of *Phrack* included an edited version of a document that an Atlanta hacker, Robert Johnson, a.k.a. "Prophet," had copied from confidential Bell South files (the "911 Document"). Prophet had transmitted the 911 Document to hackers across the country, including the editors of *Phrack*. The 911 Document, which Sterling reproduces in its tedious entirety (pp. 262-73), only contained administrative information that was commercially available from Bell South. Nevertheless, Neidorf was charged with computer fraud and abuse, wire fraud and interstate transportation of stolen property in connection with publishing the 911 Document in *Phrack*.[14]

Had *Phrack* been a "real" magazine printed on paper rather than electronic networks, such a prosecution against a member of the press would have been untenable. The First Amendment's protection of the press has insulated newspapers and magazines from criminal and civil liability in connection with numerous similar situations.[15] It has never been established, however, that the First Amendment protection of the press extends to electronic publications.[16] Until courts make this logical

---

Information, 65 TEX. L. REV. 1395 (1987); Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893 (1984); John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991 (1984).

14. The government ultimately dropped its prosecution against Neidorf. *See* Mike Godwin, *Some "Property" Problems in Computer Crime Prosecution*, CARDOZO L.F., Aug. 24, 1992, at 24, 25.

15. Sterling notes that Emmanuel Goldstein's infamous underground hacker magazine *2600: The Hacker Quarterly*, which regularly included features on stealing telephone service and perpetrating computer intrusion, repeatedly escaped direct repression because it was printed on paper and recognized as subject to the First Amendment's freedom of the press (pp. 63-68).

16. *See* Rosalind Resnick, *The Outer Limits*, NAT'L L.J., Sept. 16, 1991, at 1, 32. Recently, the federal district court in Austin held that information contained on floppy disks, including an electronic bulletin board and its contents, constituted "work product materials"

extension of First Amendment principles, cases like Neidorf's may continue to arise.[17]

Sterling also describes the Operation Sundevil raid of an Austin, Texas, game designer: Steve Jackson Games, Inc. ("SJG"). The raid and subsequent confiscation of equipment occurred because the responsible law enforcement officials understood neither the technology they seized nor its users. In particular, Lloyd Blankenship of Austin, a.k.a. "Mentor," operated an underground electronic bulletin board called the "Phoenix" Board, a clearinghouse for hacker information. Blankenship was also an employee of SJG and a member of SJG's "Illuminati" bulletin board, which posted information and messages relating to SJG's popular "Illuminati" game. When a law enforcement officer suspected that Mentor's Phoenix Board had a copy of the illegal 911 Document, he also assumed that the Illuminati board was part of the 911 Document conspiracy. Despite the extremely tenuous connection between the 911 Document and SJG and numerous factual errors in the officers' search warrant affidavit, a search warrant issued for the offices of SJG.[18]

On March 1, 1990, the Secret Service raided the offices of SJG and confiscated every piece of electronic equipment there including modems, telephones, three computers, and over 300 disks containing business and personnel records, manuscripts of SJG publications, and correspondence (pp. 138-46). The Secret Service did not return the majority of SJG's equipment until June 1990,[19] causing the company to sustain over $40,000 in damages,[20] even though criminal charges in connection with the 911 Document were never brought against Blankenship or any other SJG employee.[21] The SJG raid was based on nothing more substantial than a

---

protected under the Privacy Protection Act, 42 U.S.C. § 2000aa(7)(b) (1988). *See* Steve Jackson Games, Inc. v. United States, No. A 91 CA 346 SS, slip op. at 16 (W.D. Tex. Mar. 12, 1993).

17. See Laurence H. Tribe's discussion of his axiom that "Constitutional principles should not vary with accidents of technology" in Laurence H. Tribe, The Constitution in Cyberspace: Law and Liberty beyond the Electronic Frontier 17-22 (prepared remarks for the First Conference on Computers, Freedom & Privacy, Mar. 26, 1991) (copy on file with the author).

18. Steve Jackson Games, Inc. v. United States, No. A 91 CA 346 SS, slip op. at 8-9 (W.D. Tex. Mar. 12, 1993).

19. *Id.* at 10.

20. *Id.* at 13.

21. *Id.* at 10. In response to the confiscation of its computer equipment, SJG brought a civil action against the Secret Service alleging, in part, violations of the Privacy Protection Act, 42 U.S.C. § 2000aa (1988), and the Stored Wire and Electronic Communications and Transactional Records Access Act, 18 U.S.C. §§ 2701-2711 (1988). The United States District Court for the Western District of Texas held that the Privacy Act was violated by

misunderstanding.

Although one may not agree that all laws prohibiting computer intrusion are unjust, it is hard to deny that the recent enforcement of those laws has at times been unsatisfactory. Abuses such as the Neidorf trial and the SJG raid stem from fundamental misunderstandings between the computer community, law enforcement officials, and society. In a world where privacy is increasingly compromised via electronic means, one can only hope, as Bruce Sterling does, that the principal players are finally beginning to hear one another.

Jorge L. Contreras, Jr.

---

the Service's refusal to return the confiscated materials within a reasonable amount of time and that the Stored Wire Act was violated because the Service failed to notify SJG of its rights under the statute and failed to make back-up copies of the materials it seized. Steve Jackson Games, Inc. v. United States, No. A 91 CA 346 SS, slip op. at 19, 25 (W.D. Tex. Mar. 12, 1993).