Santa Clara University
School of Law

Santa Clara High Technology Law Journal

Volume 9 | Issue 2 Article 10

January 1993

Book Review

George J. Alexander

BOOK REVIEWS

INTELLECTUAL PROPERTY PROTECTION AND MANAGEMENT: LAW AND PRACTICE IN JAPAN, Teruo Doi.

George J. Alexander†

In the United States, a number of authors have produced comprehensive work on domestic intellectual property. A needy lawyer has alternatives to the electronic databases.

Customarily, United States treatises are concise and informative, weaving a myriad of specifics into a pattern of law. It may not be great literature but it is very useful law.

Many of the works produced in other countries are different and, I would be tempted to say, more verbose and less comfortable for case-hardened lawyers. That assumes it is written in English, the only language U.S. lawyers are likely to understand. The difference in expression may be a product of the differences between common law and code based systems.

Professor Doi has produced a masterful book in the American tradition. It is destined to hold the place of a Prosser on Torts in the field of Japanese intellectual property law. The book would be an outstanding addition to legal literature if many others had competing volumes. In a field in which English language information is very scarce, it is a unique contribution.

The book is comprehensive, with chapters on such traditional topics as employee inventions, regulation and copyright in cable television, performance rights, trade secrets, domestic trademark protection and protection against infringing importation and restrictive trade practices in patent and know-how licensing. It is extremely timely, reporting Japanese legislation concerning unfair competition, the Copyright Act, and the Trademark Act passed or modified in the 1990s.

Coverage is not tradition-bound, however. It has chapters on such evolving concepts as computer technology copyright and the

† Professor of Law and Director, Institute of International and Comparative Law, Santa Clara University.

copyright protection of videograms. It gives insights into Japanese organization. When describing government regulation and copyright protection of cable television, the author provides charts describing the growth of the industry and ownership of cable stations. When employee invention rights are discussed, the problems are fully explored, even reaching the question of taxation of compensation for employee inventions.

This book is indispensible for lawyers who have professional concerns about any of the issues covered. They will find it lucid, comprehensive and authoritative. More than that, they will find it of familiar style requiring no special knowledge of Japan or its legal system. The book is also clearly not transliterated. Professor Doi is an expert in his field not only as it applies to Japan but also in its American application. If it has a fault, it may be that its masterfully uncomplicated exposition may lead an novice attorney to believe that Japanese law is as similar to her own as the law of another state.

For those less interested in specific information concerning Japanese law, however, a close reading of the book can provide an insightful view of cultural differences between the United States and Japan. Here trade secrecy is a often a problem because employee mobility makes it difficult for employers to suppress the spread of secrets. Domestic law protects mobility by limiting the rights of employers to declare production methods secret thus allowing employees to market their skills elsewhere.

In Japan, the author notes, employees are reluctant to leave an employer. "Under such a system there is not much fear of trade secrets being stolen by employees," the author notes.[1]

Professor Doi has created a work no intellectual property lawyer affected by Japanese law should neglect. That probably includes almost all intellectual property lawyers.

1. T. Doi, Intellectual Property Protection and Management: Law and Practice in Japan (Waseda University 1992) at 35.

THE HACKER CRACKDOWN: LAW AND DISORDER IN THE ELECTRONIC FRONTIER. By Bruce Sterling. *Bantam Books*, 1992. 328 pages. $23.00

By Kenn Lara†

INTRODUCTION

The Hacker Crackdown: Law and Disorder on the Electronic Frontier, by Bruce Sterling, is a contextual account of the police raids against electronic bulletin boards that occurred in the early 1990s. Using these law enforcement hacker raids as the narrative watermark of the book, the author places the raids within the historical milieu of telephones and computers. He divides the book into four major chapters: Crashing the System, The Digital Underground, Law and Order, and The Civil Libertarians. Within each chapter, the technological concepts and their functions within the system or network are discussed. In addition, Crashing the System includes historical and social background on the telephone and the telephone companies. This chapter also describes the real life characters who played roles in using, and sometimes abusing, the technology and the system. The Digital Underground looks at the kinds of computer users that inhabit electronic bulletin boards, and gives characterizations of those users who were daring enough to exploit the openness of "cyberspace." Interjected between the technology and the human users are discussions of the conceptual frameworks, theories, and philosophies that guide the interaction between the people and the machines of the "electronic frontier." The chapters on Law and Order and The Civil Libertarians highlight, on a personal level, the conflict between the law and the hackers.

This is a story of the breakthroughs, events, and people that created the electronic frontier. It is also a story of the legal and theoretical implications of this new time and space frontier, a frontier the author terms as "cyberspace." The book is a fascinating introduction to the technology, lingo, and people of cyberspace, which is all told in easy-to-read and -understand language.

---

† J.D. Santa Clara School of Law, 1993.

CRASHING THE SYSTEM

This section begins by highlighting the crash of AT&T's long-distance telephone switching system on January 15, 1990. The author considers this event the catalyst for the eventual hacker crackdown. The crash, which left 60,000 people without service and took nine hours to repair, convinced politicians and law enforcement agencies to regard computer hackers seriously as national security threats. After much investigation, it was found that the AT&T crash of January 15, 1990, was caused by a software defect ("bug") and not by hacker interference. However, forces were set in motion that placed indirect, if not direct, blame upon computer hackers as a potential threat which could result in such mishaps in the nation's telephone system.

In a flashback, the author reviews the birth and development of the Bell System, and its holding company, AT&T. From Alexander Graham Bell to the breakup of "Ma Bell," the reader is given an overview of the symbiotic growth and expansion of the telephone and Ma Bell. There is also an overview of Ma Bell's guiding philosophy of public service and intensive research and development — "One Policy, One System, Universal Service." A brief account is given of the special relationship between Ma Bell and the government; this relationship often was intimate enough to almost be illegal. It was a relationship that ended in 1983, when the Bell System was ordered by a federal court to dismantle itself. From this breakup, there resulted the Regional Bell Operating Companies, the RBOCs (pronounced "arbocks"), which would play significant roles in the hacker crackdown, both as victims of hackers and as their eventual pursuers.

The author gives the reader an adequate foundation for comprehending the impact of hackers on the telephone company establishment. The concept of secrecy and the means of maintaining it are also discussed in this chapter. Telephone companies, or "telcos," wanted to maintain the security of their property and services, both tangible and intangible, but their systems were susceptible to electronic break-ins. Property security in cyberspace was a difficult matter because "theft" of telco services and electronic documents often left no physical evidence. The only evidence was the appearance of classified documents on numerous electronic bulletin boards, or long-distance service used but for which no payment was made. To the telcos, security meant preventing the misuse of their services and electronic documents. Only in the '90s have security

concerns realistically focused on potential threats to the entire telephone system.

THE DIGITAL UNDERGROUND

This chapter is very effective at pulling the reader into the world of semi-clandestine electronic bulletin boards (BBs) and their users. Sterling presents the relationships clearly and convincingly, leaving the reader with a good understanding of the users' mentality, the impact on the telcos, the RBOCs, the government, and cyberspace. This is by far the best chapter in the book.

As related by Sterling a fascinating world of code names, "techno-lingo," "handles," and bravado fills cyberspace. For example, the philosophy of a "phone phreak" is markedly different from that of a computer hacker. The latter does not even consider the former to be a member of cyberspace, but many people, including those in law enforcement agencies, regard both as "cyberpunks."

Phone phreaks, the author attests, are mainly concerned with the misappropriation of phone service. Their activities range from breaking into phone booths and stealing the change to using black boxes to discover long-distance access codes. The author believes their activities are both destructive and criminally reprehensible.

In contrast, computer hackers also like to break into telco systems, but are less destructive and less criminally reprehensible in their actions, as they usually leave the system intact. The challenge of navigating through supposedly secure telco systems is what drives these cyberpunks. They only copy a document as proof of their hacking skills; it is a trophy to show off to their friends and the rest of the world. Because they leave the original where they found it, they do not consider copying a file to be stealing. They do not use the copied document for financial gain, only for personal bragging rights, which they employ against other telco bandits and the telcos themselves.

The electronic bulletin boards are considered neo-speakeasies for computer users. They have names such as "The Administration," "ALIAS," "Anarchy Inc.," "Apple Mafia," "Black Bag," "Elite Phreakers and Hackers Club," "Legion of Doom," "The Phirm," "The Punk Mafia," "Neon Knights," and "Nihilist Order," to name a few. Members link up with the BB and begin communications, most of which involve the uploading and downloading of various and sundry items such as pirated software, copied confidential documents, credit card numbers, long-distance access codes, and text files for manuals. It was a gathering place where your

"handle" hid your true identity and your infiltration skills spoke for you. Users with handles such as "Carrier Culprit," "The Executioner," "Black Majik," "Solid State," and "Mr. Icon" would electronically congregate and exchange news of their exploits. It was an electronic underground that changed often, as users logged in and logged out and the BBs went online and offline. User access to and within the numerous boards was often secretive and elitist. Only those "in the know" were allowed the greatest access. To be "in the know" meant knowing the lingo, "the rap," and the action. As the boards and users become bolder, they attracted the attention of law enforcement agencies.

LAW AND ORDER

As boards became more blatant in their neo-criminal "phreaking" activities and because communications often crossed state lines, the federal government, especially the Secret Service and the FBI, began to take an interest. With the help of the Secret Service and FBI, regional law enforcement agencies mounted sting operations and investigations of crooked boards. They sometimes put up their own board to catch crooked users. Or, they would send in an undercover officer as a user on a suspect board.

This kind of covert action scared many a BB system operator ("sysop") and user. Some BBs took themselves offline and laid low for a while, but would eventually go back online. Users began to distrust other users, especially new ones. But few were ever to discover the undercover officer users. These agencies and officers, termed by the author as "Cyberspace Rangers," became well known within cyberspace. With the cooperation of the telcos, they successfully infiltrated the boards and began arresting and prosecuting individuals connected with boards involved in illegal activities.

A major issue discussed by the author is that during the raids, all the equipment was seized. Even in cases where no charges were pressed, the authorities have continued to keep the equipment, to the financial detriment of the owners.

Unfortunately, the author does not delve into other possible Fourth Amendment problems and evidentiary questions. The dummy BBs set up by law enforcement agencies and undercover users bring up entrapment and wiretapping issues, as well as problems involving search warrants and resonableness. The author, however, does give some attention to first amendment concerns in the next chapter.

THE CIVIL LIBERTARIANS

The actions by law enforcement agencies, described in the previous chapter, triggered a counterreaction from computer civil libertarians. Hacker raids in 1990 and 1991 by the Secret Service, Chicago Task Force, and the Arizona Organized Crime and Racketeering Unit were highly publicized in the media. This attracted the attention of computer entrepreneurs such as Mitch Kapor, of Lotus 1-2-3 fame, who founded the Electronic Frontier Foundation, a civil liberties organization, in reaction to the hacker crackdown. These computer civil libertarians seek to defend those who were the targets of the hacker crackdown. They believe that the raids and seizures are constitutionally unsound. To these civil libertarians, the First and Fourth Amendments are being compromised in cyberspace for so-called "national security reasons."

The author gives background on some of these entrepreneurial civil libertarians who brought publicity to bear against the law enforcement operations. For example, the reader is given an account of the well-publicized trial of Craig Neidorf, who was charged with wire fraud and transportation of stolen property. Neidorf ran a board that, through a circuitous route, obtained a confidential Southern Bell document. Neidorf was apparently the unfortunate recipient of the pirated document through users who uploaded and downloaded the document.

CONCLUSIONS

This book guides the reader through the stories of the hacker crackdown, via a narrative, story-telling format which prohibits the excessive use of technical language. This is both a strength and weakness. It is a weakness because it does not go into much legal or technical depth of the subject matter. It does not purport to be a manual on cyberspace, hacking, phone phreaking, or the telcos and their systems. It is, however, broad in its treatment of the recent interactions between citizens and the law in cyberspace wherein lies the book's strength.

It gives an overview of the electronic frontier and its potential legal implications. For some readers the lack of in-depth discussion and/or analysis on the first and fourth amendment ramifications of the hacker crackdown may be troublesome. However, it appears that constitutional lawyers were not the targeted audience of this book. Thus, the legal analyses may be sufficient for the lay reader who simply wants to learn more about computer hackers and electronic bulletin boards.

There are places in the narrative where the author seems to go off on philosophical tangents that tend to lose the reader. The relevancy of the tangent to the story matter is often questionable. It seems that the author sometimes gets lost between the narrative as a story and the narrative as a philosophical monologue of free thought. But in these instances, the author does eventually extricate himself, and the narrative continues.

In general, this book makes for a good introduction for lawyers who may want to enter the legal cyberspace. It is a timely and easy-to-read work that introduces the reader to the contextual background of cyberspace, where the constitutional battles of tomorrow will soon be fought.