Masthead Logo

DePaul Law Review

Volume 26
Issue 1 *Fall 1976*

Article 14

Crime by Computer

James N. Rabjohn

CRIME BY COMPUTER by DONN B. PARKER. New York: Charles Scribner's Sons. Charts, tables, photographs, and index. 1976. Pp. xii + 308. $10.95 cloth.

*James N. Rabjohn**

Computers are the stuff of fantasy and mystery. The havoc they can cause, whether by accident or design, is very real. A skillful computer operator is armed with a weapon that can penetrate and compromise a bank or other financial institution without leaving a trace. The operator can cause the "crime" to lurk quietly inside the machine, waiting for days or years to be activated. The poison he has planted, in the form of a few lines of computer code, may act with or without notice, then eradicate itself leaving not even a telltale trace. Meanwhile, the perpetrator may long since have disappeared.

Instances in which the computer has been used to bilk the gullible and swindle the guileless are numerous. "Val Smith" siphoned assets from a computer for six years without detection. A bank teller, less interested in stealth than speed, extracted $1.4 million from a bank and observed "the computer didn't make it easier to steal, but it sure did make it faster."[1] Equity Funding succeeded, for a time, in creating and juggling 64,000 fake insurance policies before the eyes of investors who were all too willing to buy the trick. Obviously, the law must contend with the computer.

Crime by Computer by Donn B. Parker is an unexceptional compendium of newspaper clippings on this growing problem of "computer abuse." To one for whom the word "computer" causes cerebral paralysis, this book may be an informative, occasionally entertaining, introduction. To those who have preconceptions about the range and type of computer abuse, it may suggest additional forms. This is not a book for specialists; rather, it is geared to the general reading public. It is not heavy reading, nor is it peppered with needless computer-related cant. There are only the briefest of legal references.

The primary prescription for the problems it details is apparently better ethical standards, such as professionalization of computer-related jobs, or special licenses. Other preventive measures are suggested which already are well known and widely-applied security devices. The mes-

* Assistant Study Director, National Opinion Research Center at the University of Chicago. B.A., Williams College; Ph.D. candidate (Political Science), University of Chicago.

1. D. PARKER, CRIME BY COMPUTER 194 (1976).

sage that comes through the loudest and clearest, though, almost has become a cliche: the abuses, the crimes, are committed by individuals, not machines. Big Brother is flesh and blood; no amount of electronic hocus-pocus can change that.

Crime by Computer starts from the uncontested position that "[a]s computers and telecommunications are used to take over the storage, transporting, exchange, and accounting of assets, so crooks with new skills, knowledge, and access will replace the old-style criminals."[2] For example, negotiable instruments are being replaced by a new form of financial assets—a computer tape spotted with electronic pulses and magnetic patterns. Parker, in an anecdotal and non-technical presentation, indicates the range of problems which arise when computers enter the picture. He gives examples of four major areas of computer abuse.

First, the computer itself may be the object of attack. Irate victims and computer operators literally have shot at the menacing metallic boxes, usually without notable success. Terrorists have attempted to destroy them; enterprising personnel have stolen parts from them. In addition, computer programs are now subject to theft or malicious destruction. More interesting is the second area of computer abuse. The computer may passively assist in crime by creating a unique environment for unauthorized acts. The computer facilitates such familiar crimes as fraud, theft, larceny, embezzlement, extortion, sabotage, or espionage. The computer can also actively be used as the very instrument of an illegal act. Control and manipulation of a large number of assets with incredible speed is now possible. The final area of computer abuse, according to Parker, is symbolic. The computer may be used to intimidate, deceive, or defraud victims. How often do most people carefully check computer printed bills against original purchases? As another example, the presence of stacks of computer output in a courtroom or meeting have often been pointed to as attempts to intimidate a jury or impress members of a committee.

One crucial issue considered by Parker is the extent of computer abuse. He concludes that there have been only 374 reported cases of computer crimes since 1958. Considering that there are approximately 150,000 computers operating in the United States, the extent of the problem at first glance appears to be minimal. The losses from computer-related crimes, however, probably are higher than from their pre-computer equivalents, although the evidence is inconclusive. Headline cases such as Equity Funding, which may or may not be a computer crime, tend to obscure the true extent of abuse. Also, there may be much criminal activity that has gone undetected. The typical "white collar" nature of these crimes puts them into that category of sometimes-detected and rarely-prosecuted crimes.

2. *Id.* at 6.

Crime by Computer also discusses the public's attitude towards computers. Errors and omissions, which represent the most common causes of loss, probably contribute to a general sense of suspicion on the part of the public. Parker makes the point that the lack of fair treatment in correcting errors is often more a source of abuse than the original error. The public also has become increasingly concerned about the invasion of privacy and breach of confidentiality which computers make possible. Parker remarks that governments traditionally have been tolerable because of their inefficiency. Computers can improve efficiency, however, and at the same time, jeopardize personal security and freedom. In many cases, the danger may not be in the storage of personal data but in the storage of incorrect or incomplete data. Ironically, the potential for security is far greater in computerized systems; errors, once discovered, can be corrected more quickly and completely.

Computer abuse can be prevented. One intriguing method is to design the computer in such a way as to detect abuse. Abuse can be made more difficult and costly, but like a pick-proof lock, the cost and inconvenience of developing the system may make its use unattrative. Obviously, there are degrees of care that can be taken.

As the opportunities for criminal activities multiply, the increased sophistication and decreased costs of monitoring systems should serve as a check on abuse. Both individuals and firms may be able to make more frequent and less costly audits of their assets to forestall or detect fraud. Improvements are taking place in the industry. More secure computers and computer environments are appearing and auditors with knowledge of electronic data are being trained.

The public could protect itself by ceasing to be so trusting of computers. Advancing technology has been a devil and a deity. We come to accept its gimmicks, usually with only a rudimentary understanding of their workings. Recently, a manufacturer of integrated circuits (ICs), the guts of pocket calculators, released a batch of ICs with an error in the circuit logic. It only appeared when a complex function was performed. Most people would have blindly accepted the Arcsin of 42 degrees as 3.2689, or whatever, even though it was incorrect. Technologies are usually only approximations requiring continual refinement. Each new "advance" should be greeted with healthy skepticism, for all too soon, most of us willingly accept the "bottom line" without the faintest notion of how it got there.

Parker has removed some of the mystification surrounding computers, making it apparent that the legal profession is capable of dealing with the problem of computer crime. Certainly, lawyers and legislators will have to make adjustments, such as learning a new vocabulary, but a fourth year of law school in data processing will not be necessary. Unfor-

tunately, it seems that the de-mystification of computer crime is not welcomed in some quarters. In sitting in on a trial, Parker was dismayed seeing obfuscation pile upon inaccuracies. He approached one of the lawyers and explained that he could eliminate the confusion that must be developing in the jurors' minds if he were called to the witness stand. The attorney was obviously not interested in eliminating the confusion. The mystery of machines can be a useful courtroom tool, although the ethics of such tactics are questionable.

The examples presented by Parker are worth pondering, for behind them are important moral and legal quandaries. Very few of the abuses are truly unique, but that does not mitigate their importance. It is the perception that computer abuse is somehow "different" that has engendered public and legal concern. The legal profession should not be intimidated by computers or technology. If technicians are allowed to establish standards and precedents, legal as well as electronic, they will. Legislators and litigators must press for and expose the underlying issues, the real crimes, and deal with them rather than elaborating on the paraphernalia surrounding them.

Crime by Computer is not a book for scholars, legal or otherwise. It is an introduction to an area of life and the law of which we must become aware. For those with little background and some uncertainty, this book serves as a useful eye-opener.