UIC John Marshall Journal of Information Technology & Privacy Law

Volume 2
Issue 1 *Computer/Law Journal - 1980*

Article 21

1980

The Trial of a Computer Crime, 2 Computer L.J. 441 (1980)

Jay Becker

THE TRIAL OF A COMPUTER CRIME

By JAY BECKER*

INTRODUCTION

It was a sign of the times. In one issue of Computerworld was a feature called "Crime Wrap-up."[1] The article, which occupied a prominent spot in this major computer industry periodical, contained the news that Michigan had become the fifth state to pass legislation concerning computer crime.[2] Right beneath it were separate stories of three different computer crime cases, one involving an acquittal, one a plea and one an indictment.[3] Beneath these stories, at the bottom of the page, was an advertisement for a national management consultant specializing in computer security.[4] "There's always the chance something or someone can 'get to' your computer," the ad warned investigators of computer crime. The Law Enforcement Assistance Administration ("LEAA") recently awarded $400,000 for the training of prosecutors and investigators in computer crime. These unconnected, but related, items indicate that computer crime problems will arise more and more frequently in the criminal trial of the future.

Although computer crime is not the only area where lawyers must try to adapt pre-cybernetic laws to the realities of current information technology, this area is of growing significance in what has become the most information-oriented society ever to exist. Whether it is computer copyright, software taxation, issues of liability when computers are involved in industrial accidents, or clauses in purchase contracts for computer hardware, the law is being forced to recognize that the widespread use of computers is causing

* B.A. cum laude 1965, City College of New York; J.D. 1968, Harvard University Law School. Mr. Becker is a member of the bar of the State of California and Director of the National Center for Computer Crime Data. A former deputy district attorney, Mr. Becker is a sole practitioner specializing in computer crime law.

1. Computerworld, July 30, 1979, at 4, col. 1.

2. *Id.*

3. *Id., reporting* People v. Ristol, Crim. #A345083 (Los Angeles Super. Ct. 1978); United States v. Ferguson, Crim #79-105 (C.D. Cal. 1979); United States v. Herr, Crim. #79-538 (C.D. Cal. 1979).

4. *Id.*

changes in our society so different in degree as to be almost different in kind. Although some would suggest that the computer is no more than a big adding machine, it is impossible to look at the phenomenon of computer crime without considering the varied effects of computers on our legal consciousness.

On a physical level, the computer is staggering in its ability to concentrate and manipulate enormous quantities of information. The information may represent money, complex mathematical equations, physical goods, or repetitive tasks. All fit within the computer's grasp.

On an intellectual level, computers have changed vocabularies, and perhaps more importantly, concepts of how things get done. Whether one thinks about a word like "deprogramming," or asks someone for "feedback," systems and information science theories have caused everyone to talk and think in new ways. For instance, to date the law has no consistent answer to the demand to redefine "property" in view of the value of information in the computer environment.[5]

Finally, there is a third kind of reaction to the incursion of computers into our lives, a response on a mythical level. This reaction does not affect the way that we think, but shapes the stories we tell ourselves when we do not know what to think. Such unthinking reactions are responsible for some of the more colorful and interesting aspects of social behavior, as well as some of critical importance. For example, few criminal lawyers would deny the power of sexist mythology in the area of rape. Subconscious prejudices about men, women, sex, and other vague, far-reaching ideas color, if not dictate, decisions in many rape trials. In the same way, unarticulated feelings about computers affect the whole realm of computer crime. Publicity both creates and caters to computer myths, and computer crime sentencing often reflects that fact.

Inexplicably, none of these dramatic changes has brought forth a flood of legal literature about the trial of computer crimes,[6] and even less guidance is available in the case law. Consequently, much of the information presented herein is anecdotal, representing the responses to a survey of attorneys who tried (or plea-bargained)

---

5. *See* text accompanying notes 37-45.

6. *See* A. BEQUAI, COMPUTER CRIME (1978); Bequai, *Legal Problems in Prosecuting Computer Crime*, 21 SECURITY MANAGEMENT 26 (1977); COUGHRAN, COMPUTER ABUSE AND CRIMINAL LAW (1976); Coughran, *Outlook for Prosecution in Computer Abuse Cases*, 1 CRIM. JUSTICE J. 397 (1978); Hemphill & Hemphill, *Prosecuting Computer Criminals*, 14 SECURITY MANAGEMENT 62 (1978); Holman, *Computer Crime: A Prosecutor's Perspective*, in PROC. HONEYWELL COMPUTER SECURITY & PRIVACY SYMP. (1979). Notably absent are any studies of the defense of a computer crime case.

computer crime cases, investigators who contacted the National Center for Computer Crime Data (NCCCD),[7] and the case histories contained in NCCCD's files. Because of the few specifics available, all but the broadest generalizations seem premature.

I. SEARCH AND SEIZURE

One need only consider the requirements for a search warrant in light of the complexity of computer technology to begin to understand the search and seizure issues inherent in computer crimes. The enormity and complexity of the "scene of the crime" where computers are involved is demonstrated by the litigation involving Equity Funding Corporation.[8] There, thousands of fictitious insurance policies had been created and existed somewhere within a computer memory. At the same time, the computer was processing hundreds of thousands of valid insurance policies. According to Carl Pabst, a partner in the accounting firm of Touche Ross, appointed by the trustee in the Equity Funding bankruptcy proceedings, it was impossible to maintain adequate security over the computer site while allowing the business to continue to function.[9]

Both in drafting a warrant and serving it, problems can be severe. Simply by describing what is to be seized and how it can be recognized, so that a magistrate will find the particularity requirements of the Penal Code[10] satisfied, is a bit more difficult when premised on an understanding of computer language, and perhaps of computer operations as well.

For example, in the case of *People v. Ward*,[11] Municipal Court Judge Lewis Doll was asked to sign a search warrant authorizing the seizure of, among other things, "computer memory bank or other data storage devices magnetically imprinted with Information Systems Design (ISD) remote plotting computer programs."[12] Ward was believed to have stolen a program from ISD and to have made it available to University Computing Company, one of ISD's competitors.

Alameda County deputy district attorney Donald Ingraham at-

7. The National Center for Computer Crime Data data base is organized along the same lines as the SRI International data base, much of which has been graciously made available to the Center. Reference to materials in the Center's data base reflect this organization. Files can be viewed on arrangement with the Center's director.

8. *See* Report of the Trustee of Equity Funding Corporation of America in Proceedings for the Reorganization of a Corporation, #73-0346 (C.D. Cal. 1973).

9. Personal communications with Carl Pabst.

10. *See, e.g.*, CAL. PENAL CODE §§ 1525, 1529 (West).

11. *Reported at* 3 CLSR 206 (Cal. Super. Ct. 1972).

12. J. BECKER, THE INVESTIGATION OF COMPUTER CRIME, app. 5 (1980).

tempted to explain the specifics of Ward's theft, alleging that the stolen program was valuable because it was capable of "producing remote plotting."[13] Then, remote plotting had to be explained and the fact that it was designed and developed by ISD. This was a ticklish task since California law is still unclear as to whether the stealing of the information in a program is a crime.[14]

Another difficult problem was that the prosecutor did not know in what form the stolen program might be found at the scene of the search. The search warrant affidavit indicated that it might be found in the form of computer keypunch cards, computer printout sheets, or in an intangible form within the computer.[15] To locate the material to be seized, an expert from the victim company accompanied the officers serving the warrant.[16]

For the attorney drafting such a warrant, great care must be taken to learn enough about the computer operation involved to describe adequately those aspects which are relevant. Additionally, they must be described clearly enough to be understood by the magistrate. It goes without saying that, without a comparable knowledge on the part of the defense attorney, he or she will be in no position to contest the adequacy of the description of any item contained in the warrant.

There is considerable value in having an expert available when the warrant is served where neither the attorney nor the investigator serving the warrant has enough knowledge of the computer system to perform a search intelligently and completely. It may be that only the expert has a sufficient background in programming to query the computer, locate the relevant information stored in the system, retrieve it, and do all this without harming the operation of the computer system. Yet, until August 1979, it was unclear under California law whether an expert could be taken to the scene.[17]

Though difficulty in executing a search warrant represents the most visible form of the computer search and seizure problem, it is hardly the only one. Since the nature of computers involves numerous opportunities for electronic access, and many possible intruders, it should not be too surprising that different investigative tech-

13. *Id.* at 57, 59.

14. *Compare* People v. Kunkin, 100 Cal. Rptr. 890 (1972), *vacated*, 9 Cal. 3d 245 (1973), *with* People v. Ward, 3 CLSR 206, 208 (Cal. Super. Ct. 1972). In vacating the appellate court's opinion in *Kunkin*, the California Supreme Court assumed, without deciding, that the documents containing the information were themselves property.

15. J. BECKER, *supra* note 12, at 58.

16. *Id.* at 61-62.

17. *Compare* People v. Superior Court (Williams), 77 Cal. App. 3d 69 (1978), *with* People v. Superior Court (Myers), 25 Cal. 3d 67 (1979).

niques may be necessary to detect computer criminals. Different investigation methods, however, may themselves trigger novel search and seizure arguments.

For example, in one case,[18] two employees of the New York Department of Motor Vehicles were collecting registration payments, then issuing orders to the DMV computer to cancel the transactions reflecting receipt of the registration fees. Once the transactions were cancelled, they felt safe in keeping the money. After the crime was discovered, considerable effort was required to reprogram the DMV system to, in effect, monitor the defendants and numerous other employees of the Department. Ultimately, surveillance led to the arrest of the two individuals, who pled guilty. In Los Angeles and Tokyo, computers were similarly programmed to detect when they were being used without permission, as well as the location of illicit users.[19]

These cases demonstrate some of the novel search-fact situations on which defense attorneys may meditate. To challenge searches as infringements of rights unanticipated by the founders of the constitution is not without rewards. History has shown that the novel theory of one era has become the dogma of the next. In the case of *United States v. Kelly*,[20] two employees of Univac used part of the company's computer to run their own business. The legality of the surveillance of the defendants was raised as a major, but unsuccessful, aspect of the defense case.[21]

II. CHARGING COMPUTER CRIMES

The most immediate and likely problem for an attorney reviewing a computer crime case is the applicability of state or federal legislation defining computer crime. The introduction of the Federal Computer Systems Protection Act (S. 240), has focused a considerable amount of attention on computer crime.[22] Senator Abraham Ribicoff, its main proponent, has traveled widely, talking about the problems that the federal government has faced in attempting to

18. People v. Buoniconti (unreported). Information on this case is on file with the National Center for Computer Crime Data.

19. People v. Maki, Crim. #A321762 (1975) [NCCCD file #7546]; D. PARKER, CRIME BY COMPUTER 80-84 (1976).

20. United States v. Kelly, Crim. #77-250 (E.D. Pa. 1977) [NCCCD file #7741].

21. Personal communication with assistant United States attorney Walter S. Batty.

22. *Legal Sanctions to Computer Abuse*, 2 ASSETS PROTECTION, Mar. 1977, at 27. *Federal Computer Systems Protection Act: Hearings Before the Subcomm. on Criminal Laws and Procedures, Senate Comm. on the Judiciary*, 95th Cong., 2d Sess. 207 (1978) [hereinafter cited as *Hearings*].

prosecute major computer crime cases without such enabling legislation. In introducing his bill in 1977, Ribicoff referred to several fact situations in which prosecution was difficult because no legislation specifically covered computer crimes.[23] Three such cases were *United States v. Kelly*,[24] *United States v. Sampson*,[25] and *United States v Kostoff*.[26]

In *United States v. Kelly*,[27] the defendants set up a computerized sheet music arranging and engraving company using their employer's computer. They were charged with using the mails to defraud,[28] because they sent out brochures which failed to state that they were using the employer's computer and not their own.

In *United States v. Sampson*,[29] the first case involving the theft of computer time was brought under 18 U.S.C. § 641, which makes theft of government property a crime.[30]

Finally, in *United States v. Kostoff*,[31] the prohibition against making false statements in loan applications[32] was used against a group which created false credit information for a fee.

To deal with the problems posed by cases such as these, S. 240 would make it a federal crime to access, or in any way use, a computer for fraudulent purposes.[33] These purposes include theft, sabotage, and embezzlement. The bill also gives four examples of what access means: tampering with input data, using computer facilities for illegal purposes, altering or destroying data within a computer

---

23. *Id.* at 178.
24. *See* note 20 *supra.*
25. 6 CLSR 879 (N.D. Cal. 1978).
26. Crim. #76-1128 (N.D. Cal. 1976).
27. *See* note 20 *supra.*
28. 18 U.S.C. § 1341 (1976).
29. 6 CLSR 879 (N.D. Cal. 1978).
30. Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; or

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined or converted—

Shall be fined not more than $10,000 or imprisoned not more than ten years, or both; but if the value of such property does not exceed the sum of $100, he shall be fined not more than $1,000 or imprisoned not more than one year, or both.

The word "value" means face, par, or market value, or cost price, either wholesale or retail, whichever is greater.

18 U.S.C. § 641 (1976).
31. *See* note 26 *supra.*
32. 18 U.S.C. § 1014 (1976).
33. *See* the Appendix in the next issue for the text of this bill.

system, and stealing money, property, or confidential information through the manipulation of computer output.[34]

Despite the appeal of specific statutes against computer crime, the breadth of the Ribicoff bill and the resistance of some segments of the computer industry have slowed its progress in becoming law. As currently phrased, the bill would allow any computer misuse to be treated as a federal felony, despite the enormous number of innocent or marginally criminal misuses that currently occur.

A broader problem presented by the Ribicoff bill is whether it is appropriate to define such a broad variety of crimes as falling within the federal purview. Donald Ingraham, a deputy district attorney in Alameda County, speaking in a non-representative capacity, opposes the Ribicoff bill. He argues that:

> The enactment of S. 240 would permit defense counsel to argue preemption, the legal doctrine which precludes states from enforcing copyright, postal fraud, and some other laws, on the theory that the availability of a federal statute excludes state and local relief. Particularly in computer-related crime, my experience is that federal preemption would deny protection to the smaller victims, and that anything smaller than Rifkin would not be accepted for prosecution because of U.S. attorney budget restraints.[35]

Knowledge of these problems with the computer crime bill lends support for whatever arguments a defense attorney may make when faced with the task of avoiding the application of a state or federal computer crime law to a specific case.

Furthermore, the Ribicoff bill is significant in that it appears to have been the model for most, if not all, of the state laws relating to computer crime.[36] Its history and its drawbacks can provide some assistance in the interpretation of state computer crime legislation.

On the state level, there has also been some activity in the area of computer crime legislation. Several months ago, the NCCCD received a telephone call from the Madison branch of the Wisconsin attorney general's office. They wanted advice and models of existing computer crime legislation. A sophomore at the University of Wisconsin had made unauthorized use of a university computer over a six-month period, and the local district attorney could find no law with which to prosecute the student.

More recently, NCCCD received a call from another midwestern state in which an investigation was in process. In that state, the investigator did not know whether the malicious mischief statute was

34. 18 U.S.C. § 1028(c)(1).

35. Ingraham, *A District Attorney Responds to John Taber*, 4 DR. DOBBS J. OF COMPUTER CALISTHENICS & ORTHODONTIA, Nov.-Dec. 1979, at 18.

36. *See* the Appendix in the next issue.

applicable. As in California Penal Code, section 494, the statute required injury to "any real or personal property."[37] The individual being investigated had changed the contents of some files within a computer. The investigator worried that the change of information would not be considered damage to the tape upon which the information was coded, and thus, would not be the subject of malicious mischief.

In *People v. Ward*,[38] ISD, a computer company in Oakland, had developed a program called "Plot/Trans." Ward, while an employee of University Computing Company (UCC), one of ISD's competitors, obtained access to the ISD computer. He instructed the computer to produce a copy of the Plot/Trans program on a printer at his office. In reality, Ward directed the ISD computer to send a series of electronic impulses over the telephone lines to the UCC computer, where the impulses were used to create a physical embodiment of the information they contained—a printout which showed the Plot/Trans program. Ward was charged with a violation of California Penal Code, section 499C.[39]

Section 499C(b) provides, *inter alia*, that "[e]very person is guilty of theft who, with intent to deprive or withhold from another thereof the control of a trade secret . . . does any of the following . . . (4) steals, takes, or carries away any article representing a trade secret."[40]

A demurrer posed the question of whether the impulses Ward caused to be transmitted from ISD's computer to UCC's were an "article," as that term is used in § 499C(b)(1). The court held that they were not, since they were not "tangible."[41]

This ruling was dictum, however, since the court found that the printout of the Plot/Trans program was an "article."[42] Ward's transportation of the printout was found to satisfy the asportation requirement of this section. Further, the court found that making a copy of the program constituted a violation of 499C(b)(3) which makes it illegal if one "[h]aving unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret."[43]

The implications of the judge's dictum came home to roost in

37. CAL. PENAL CODE § 494 (West).
38. 3 CLSR 206 (Cal. Super. Ct. 1972).
39. CAL. PENAL CODE § 499(C) (West).
40. *Id.*
41. 3 CLSR at 208.
42. *Id.*
43. CAL. PENAL CODE § 499(C)(b)(3)(West).

Colorado. In the case of *People v. Home Insurance Company*,[44] the defendants were charged with grand theft. They had arranged to copy confidential information contained in the files of hospitals treating claimants against the insurance company. Though there was no question as to what the defendants had done, there was a question as to whether acquiring the information contained in the files constituted theft under Colorado law. The Colorado Supreme Court ruled that the information was not subject to theft, and dismissed the case. In response, the Denver District Attorney's office successfully urged the Colorado legislature to include a sweeping definition of "property" in that state's new computer crime law.[45]

III. PUBLICITY

From the time that a computer crime case is filed, if not before, it is far more likely to receive publicity than a comparable, noncomputer crime situation. Obviously, a case such as the multi-million dollar theft at Security Pacific Bank by the bank's former consultant, Stanley Mark Rifkin, is not easily ignored.[46] But even when the amount taken is not overwhelming, and the method not particularly novel, newspapers are likely to pick up a case if it is a "computer" crime.

The mass media seems quite willing to play a role in the creation of a myth. This myth sees computer criminals as weird geniuses, who in some way beat the system, and thus deserve both criticism and acclaim. In the Security Pacific Bank case, Rifkin penetrated a computer system to transfer $10.2 million of the bank's money to an account in Switzerland. Stories in the Los Angeles Times focused on the fact that bank officials were unaware of Rifkin's theft until the FBI reported it to them, and on what the Times called the government's loss of "key evidence."[47] However, this loss was not a crucial blow to the prosecution, since a tape of the criminal act was not suppressed.

It should not be surprising that the press chose to challenge the

---

44. 591 P.2d 1036 (Colo. 1979).

45. The Colorado Computer Crime Law defines "property" as "including but not limited to, financial instruments, information, including electronically produced data and computer software and programs in either machine or human readable form and any other tangible or intangible items of value." COLO. CRIM. JUST. CODE § 18-5.5-101, -102.

46. *See, e.g.*, Mankin, *Dialing for Dollars*, NEW WEST, Dec. 18, 1978, at 15; *$10.2 Million Theft May Yield Profit for Victim*, EDPACS, Jan. 1979, at 11; EFT REPORT, Nov. 15, 1978; *Hearings, supra* note 22, at 209.

47. *Key Evidence Ruled Invalid in $10.2 Million Bank Theft*, Los Angeles Times, Feb. 7, 1979, at 1.

competence of the prosecution rather than the thought processes of Mr. Rifkin, since more people seemed to view the case more as one in which the bank got what it deserved, than one in which a petty criminal stole an enormous amount of money. Computer myths mean that cases which otherwise would be left in relative obscurity are publicized. And they also mean that many of these cases will be reported badly.

In the case *United States v. Sampson*,[48] the early newspaper stories spoke of the crime as involving "possibly millions of dollars worth of time and data storage."[49] A story in Computerworld indicated that "[t]hose reports were vastly exaggerated."[50] The value at the time was instead put "at about $2,000 at commercial rates."[51]

One consequence of having the media pander to the computer mythology is that a client charged with a computer crime must be warned to avoid adverse publicity more carefully than might be the case in most other crimes. For whatever reason, several defendants in computer crime cases have failed to observe what would appear to be a common sense approach for defendants awaiting trial. Rifkin's subsequent attempt to steal an additional $50 million from Union Bank was widely reported, and not very favorably. It seems quite likely that the amount of publicity and attention drawn to the case made it impossible for Judge Byrne to sentence Rifkin in a more lenient manner, as was suggested by his attorney.

Jack Polak, who was accused of theft from San Diego County by computer, threatened witnesses in the prosecution against him immediately after publicity about the case was circulated.[52] William Holman, the San Diego deputy district attorney who prosecuted the case, believes that this witness intimidation led to a much more severe sentence for Polak.[53]

Despite the problems resulting from greater media interest in computer crime cases, few successful techniques have been devised to cope with the effects of this publicity. The NCCCD survey replies indicate few attempts to counteract it. Some motions for change of venue were considered and not filed, and some were filed without success. Philip Cohen, the defense attorney in the Polak case, at-

48. 6 CLSR 879 (N.D. Cal. 1978).

49. *See, e.g.*, San Francisco Chronicle, Jan. 21, 1978, at 1.

50. French, *Two Charged in Theft of Nasa System Time*, Computerworld, Feb. 6, 1978, at 6, col. 1.

51. *Id.*

52. Personal communications with the prosecutor. *See* notes in NCCCD file #77341.

53. *Id.*

tempted to counteract the adverse effects of publicity through *voir dire* after his motion for a change of venue was denied.

To date, NCCCD has not seen documents of any sophisticated, publicity-limiting measures, such as gag orders or the like. Nonetheless, one can only assume that in the right case, the same considerations which have been listed by other authors[54] would be applicable to the trial of a highly publicized computer crime case. In the Rifkin case, Rifkin pled guilty and was sentenced, but had the case gone to trial, there might well have been the need for some consideration of protective measures against continuing publicity.

IV. DISCOVERY

The complexity of computer crime cases and their potential worldwide scope have already brought about problems in discovery which criminal law practitioners might find surprising. In the case of *People v. Lyle*,[55] the defendants were accused of erasing information maintained on the California Law Enforcement Telecommunications System (CLETS) and the Criminal Justice Information System (CJIS) computers at the Department of Justice. A defendant's request for specific information as to how these computer systems were maintained was based on the theory that disclosure would assist in preparing a defense by allowing a test of the accuracy and reliability of the computer's record-keeping ability. The nub of the problem posed by this request for discovery, at least according to a prosecution witness, can be found in the affidavit filed in opposition to the request:

> The CLETS, CJIS, and CHS [Criminal History System] involves the use of hundreds of thousands of computer instructions which comprise the most complex storage and retrieval system in the country. It would take a highly trained computer and communications expert at least one year to become familiar with all of the requested information and to check the accuracy and reliability of the system and its parts.[56]

The same expert also testified that the only way to give the discovery sought by the defendants would be to disclose the entire con-

54. *See* Best, *The Trial Lawyer's Role in the Sensational Case*, in PLI, ADVANCED CRIMINAL TRIAL TACTICS 221 (1978); Ferber, *Beating Bad Press: Protecting the California Criminal Defendant from Adverse Publicity*, 10 U.S.F.L. REV. 391 (1976); Hurson, *The Trial of a Highly Publicized Case: A Prosecutor's View*, 16 AM. CRIM. L. REV. 473 (1979); Younger, *Some Thoughts on the Defense of Publicity Cases*, 29 STAN. L. REV. 591 (1977); Jones, *Handling the High Publicity Case*, in PLI, ADVANCED CRIMINAL TRIAL TACTICS 153 (1978); Isaac, *The Psychology of Trying the Publicized Case*, *id.* at 175.

55. Unreported decision, Sacramento Mun. Ct. #38990 (1977) [NCCCD file #77110].

56. *Id.*

tents of both of the systems. Further problems would then arise since much of the information contained in these systems is confidential criminal history information, the disclosure of which is prohibited by law.

Though hardly your everyday discovery problem, the Rifkin case involved transactions in Switzerland. Prosecution requests for a procedure for taking depositions in Switzerland developed into a voluminous legal file. For attorneys used to nothing more complex than an extradition from Puerto Rico, venturing into the civil law system of much of the non-Commonwealth world can provide fascinating, though thorny, legal, economic, and practical problems.

V. TRIAL

Computer crime cases are tried even less frequently than most criminal matters. In several instances, respondents to NCCCD's computer crime survey indicated surprise that more computer crime cases were not tried. Most of those expressing surprise were prosecutors who apparently saw more potential weaknesses in their own cases than the attorneys working on the defense side. However, in view of the generally light sentences which accompanied many guilty pleas, this defense strategy is perhaps understandable.

As a consequence of the apparent disinclination to go to trial, getting evidence admitted at trial and convincing the trier of fact are issues about which little can be said based on actual case experience. Those attorneys who actually have tried computer crime cases did not experience great difficulty in communicating with the jury, according to their reports. Each stressed the need to spend a considerable time in self-education. To accomplish this goal, some read standard, general-information books[57]; some attended a course in computer crime; and just about all had lengthy discussions with experts who explained to them the nature of the underlying computer system.

None of the prosecutors involved in the survey experienced any difficulty in finding experts. Victimized companies provided expertise when needed. Those defense attorneys who hired independent experts indicated no unusual difficulties in getting them, understanding them, or examining them. One general warning, applied to the area of computer crime, is the need to remember that computer experts are not necessarily accounting or security experts, and that their testimony should be carefully focused within the realm of their expertise.

57. *E.g.*, D. PARKER, CRIME BY COMPUTER (1976); T. WHITESIDE, COMPUTER CAPERS (1978).

The admissibility of computerized evidence has been extensively discussed in cases and legal periodicals.[58] Again, surprisingly little of this discussion has been relevant in any of those computer crime cases actually tried. The theoretical problems that face the proponent of computer-based evidence are staggering. To establish completely the reliability of a computer system that produces a document or some other form of information would entail establishing that the system was adequately secured against intentional abuse or negligent harm.[59] This is a task that few computer owners would relish undertaking.

To explain fully the reliability of a computer system to a judge would require a rather extensive and painstaking course in computer programming, systems design, and many other subspecialities of the computer field. The enormity of the task may even work against the defense attorney seeking to put the prosecution to this burden of proof. George Monaco, chief of the Cook County District Atorney's Fraud Bureau, responded to a defense motion asking him to produce proof of a computer system's reliability, by saying, "Judge, if the court has no objection to clearing its calendar for the next year, I will be delighted to bring the experts necessary to explain to the court everything it could possibly want to know about how this computer works." "Motion denied," the judge responded.[60]

VI. SENTENCING

In light of the scarcity of computer crime trials, the importance of the sentencing phase cannot be overstated. A number of factors contribute to making this one of the most challenging aspects of computer crime cases. Though specific fact situations vary, the typical computer crime presents a sentencing judge with a very difficult decision. In the cases that have come to the attention of NCCCD, no defendant has had any serious prior contacts with the law. In most cases, the individual was white, middle class, gainfully employed, and well regarded in the community.

Where a loss was sustained, often the victim was a business that pursued the defendant or defendants civilly and obtained a judgment for the total loss, or obtained the defendant's promise of

58. Johnston, *A Guide for the Proponent and Opponent of Computer-Based Evidence*, 1 COMPUTER/L.J. 667 (1979); Bender, *Computer Evidence Law: Scope and Structure*, *id.* at 699. For additional articles on computer-related evidence law, *see* Schulte, *Bibliography [Computer-Related Evidence Law]*, *id.* at 781.

59. The best summary of these problems is found in Note, *A Reconsideration of the Admissibility of Computer-Generated Evidence*, 126 U. PA. L. REV. 425 (1977).

60. Personal conversation with district attorney.

restitution. Often the defendant's actions were not far from common practice in the computer industry. In some of the cases, novel theories of law were used, and the defendants were the first individuals ever convicted of computer crime under the statutes pled by the prosecutors.

In the Rifkin case, Judge Byrne was asked to fashion an innovative punishment uniquely designed for Rifkin. Attorney Robert Talcott quoted an article that Judge Byrne had written, which argued that alternatives should be considered in the sentencing of white-collar criminals. Byrne, acknowledging some possible shortsightedness in that article, was unmoved by defense arguments that Rifkin's intelligence in the computer field should justify his receiving a sentence other than incarceration in federal prison. Rifkin proposed that, instead of being put behind bars, he serve society by lecturing on how computer crimes are perpetrated and how they can be prevented. Apparently influenced heavily by Rifkin's attempted second computer crime, Byrne responded "[h]ow can Mr. Rifkin help others avoid computer crime when he can't keep himself from committing it?" Rifkin was sentenced to eight years in federal prison.[61]

Lest one draw too many conclusions from the Rifkin case, the case of Jerry Schneider in 1971, gained almost as much notoriety.[62] Widespread media reports of Schneider's theft estimated his "take" at anywhere from a quarter of a million dollars to a million and a half dollars in telephone equipment belonging to the Pacific Telephone Company. Schneider pled guilty in Los Angeles and received a forty-day county jail sentence. Like Rifkin, he was a highly intelligent individual and has no serious criminal history. Parenthetically, Schneider did pay back $9,000 over a period of five years as a result of a settlement of Pacific Telephone Company's civil suit against him.

Raymond Ressin, a "margin clerk" for a small brokerage company in Denver, abused his position in a variety of ways and bilked the firm of $170,000 through changes in the account of an accomplice.[63] After his trial and conviction, deputy district attorney Jeffrey Bayless argued that Ressin should be sentenced to ten years. He calculated that the average worker in Denver would have to spend this long to make as much as Ressin stole, and suggested that

61. Author's notes of hearing on Mar. 26, 1979 [NCCCD file #78313].

62. *See* D. PARKER, *supra* note 57, at 59-60.

63. People v. Ressin, Case #122398, Super. Ct. for the Second Jud. Dist., City and Cty. of Denver, Colo. (1977) [NCCCD file #77331].

a ten-year sentence would not be punitive, but would simply keep Ressin from turning a profit. The court was totally unsympathetic to the prosecution argument and claimed that since the brokerage firm was bonded, and the bonding company had a $169,000 judgment against Ressin, it was unrealistic to argue that Ressin was ahead $170,000. Bayless countered that a judgment is not the same as money in the bank, but that argument was lost on the judge. As of August 1979, Bayless reported that the bonding company had not collected any money from Ressin, who had gambled away much of his take before the trial began. Ressin received a suspended sentence and a $1,000 fine.

Bayless used one tactic that prosecutors may want to keep in mind, and about which defense attorneys will doubtless want to warn their clients. Through happenstance, Bayless learned that Ressin had been picked up for possession of a small amount of cocaine. Bayless held what he called one of the most extensive probation revocation hearings in the history of Denver, and he was able to get Ressin's probation revoked and replaced with a ten-year prison sentence.[64]

Like Ressin, Jack Polak abused his position as an employee to steal from his employer.[65] He created false billings to the County of San Diego, fed them into the county's computerized bill payment system, and created fictitious companies for receipt of the payments he procured. After successfully stealing $50,000, Polak made the mistake of nagging the county when it was slow in paying a second invoice for $70,000 that he fabricated. This began a series of events which led to his ultimate discovery and conviction. Perhaps as a result of his threatening witnesses, Polak received two to four years in state prison, a sentence more common in crimes of violence than computer crimes.

VII. CONCLUSION

It is difficult to know what conclusions an attorney can draw from these four examples of computer crime sentences. In general, it is well to keep in mind that, historically, chances have been great that computer criminals will receive minimal sentences. Whether the Rifkin case represents a change remains to be seen.

It should be quite clear that much of the excitement in anticipating computer crime issues comes from their highly speculative

64. Personal conversation with Jeffrey Bayless. *See* notes in NCCCD file #77331.
65. Personal conversation with prosecutor. *See* notes in NCCCD file #77341.

nature. The suggestions and observations in this article should be viewed as an opening volley in a discussion that interested readers can continue. This is not a field in which one rushes to speak the last word.