1-1-1985

COMPUTER CRIME UPDATE: THE VIEW AS WE EXIT 1984

Jay BloomBecker

Follow this and additional works at: http://digitalcommons.law.wne.edu/lawreview

Recommended Citation
COMPUTER CRIME UPDATE: THE VIEW AS WE EXIT 1984†

JAY BLOOMBECKER*

TABLE OF CONTENTS

I. AN OVERVIEW ........................................ 628
   A. Historical Background .............................. 629
   B. Publicity Problems and Promises ................. 632
      1. When Should Counsel Open His or Her Mouth? 632
      2. When Should Counsel Shut His or Her Client’s
          Mouth? .................................... 634
      3. Can Counsel “Network”? .......................... 635
      4. Should Counsel “Cash in” on Publicity? ....... 635
   C. Law Enforcement Reactions to the “Hacking
      Epidemic” ..................................... 635
      1. Computer System Seizures ....................... 636
      2. “Stinging” Bulletin Boards ........................ 636
      3. Informants .................................. 637
   D. Legal Approaches to Computer Crime .............. 637
      1. Intent ...................................... 639
      2. Juvenile Law .................................. 640
   E. Business Perspectives on Computer Crime ........ 640
   F. “Hackers” as the Huckster’s Dream ................ 642
   G. Computer Crime in Court .......................... 645
      1. Dismissals .................................. 645
      2. Sentencing .................................. 647
II. CHALLENGES IN THE LAW ............................. 648
   A. A New De Minimus ................................. 648

† © 1985 Jay BloomBecker.
* Director, National Center for Computer Crime Data, a research institute affiliated with California State University, Los Angeles. Mr. BloomBecker is the editor of COMPUTER CRIME LAW REPORTER and CONSCIENCE IN COMPUTING. A 1968 graduate of Harvard Law School, Mr. BloomBecker was a deputy district attorney in Los Angeles County for ten years before becoming the director of the Center in 1980. He has published more than 100 articles on the topic of computer crime.

627
B. Challenging the Exercise of Investigatory and Prosecutorial Discretion ........................................... 648
C. Challenging Victims’ Business Methods ......................... 648

III. CONCLUSION ........................................................................ 649

I. AN OVERVIEW

These are heady but difficult times in which to discuss computer crime. Four years ago, I marveled at the prospect of a magazine entitled Computerworld devoting an entire column to three different news stories about computer crime. Those were simpler, if not happier days. Today news of computer crime is commonplace — a front page story about such activity in the New York Times would not even raise an eyebrow.

A confluence of media attention, law enforcement and legislative reactions to that attention, and computer security vendors' attempts to capitalize on the situation has created a new villain, the "malicious hacker." 1


3. "Hacker," in this context, means someone given to using computers to cause harm
The purpose of this article is to observe and comment on the reactions to the so-called "hacking" phenomenon, and to attempt to suggest some of the legal issues implicit in those reactions. It is based largely on the ongoing research conducted by the National Center for Computer Crime Data.4

The reactions to "hacking" are of particular interest for the attorney, as counsel for (or prosecutor of) future accused computer criminals, or as a representative of the interests of the state (or future accused clients) in the ongoing negotiation of social values that criminal law represents.

A. Historical Background

It all started when a NORAD system malfunctioned and "detected" an attack by Soviet weapons which in reality had not occurred.5 The wire services and the television news shows had a field

4. The National Center for Computer Crime Data has been collecting and disseminating information about computer crime and security since 1978. Its work includes the tracking of computer crime laws and cases. The analysis of computer crime law in this article derives from the COMPUTER CRIME LAW REPORTER (1984); those based on case studies are largely based on the Computer Crime Census which will be published as part of 416, the First Annual Statistical Report of the National Center for Computer Crime Data in August 1985. See infra notes 46-50, 71, 90, 100, 114.

day reporting the disquieting news. People began to ask themselves, if we are relying on computers, can a computer error plunge us into nuclear war? The story passed from the consciousness of all but a pair of writers who turned it into *WarGames*, a movie that changed the landscape of computer crime.

*WarGames* took the NORAD malfunction, added teenage sex and heroism, threw in the “everynerd” element of personal computing, the far-out possibility of artificial computer intelligence deciding whether a nation goes to war, and the spice of “hacking.” Voila, a palpable hit. A spate of news shows asked: *WarGames* — Could it Really Happen?

The time was perfect for the “414 gang” to capture the national media's fancy. They had “life imitating art” written all over them when these Milwaukee computer hobbyists were found to have gotten access to an intentionally low-security file at the Los Alamos National Research Center. Then, when their electronic joyriding was found to extend to a bank in Los Angeles, a cement company in Montreal, and a hospital in New York, their fame was assured. One New York Times reporter commented, “when I heard they had gotten into the hospital system I caught the next flight to Milwaukee.”

*WarGames* dramatized the ultimate dangers of computer crime and suggested the ease with which it could be committed; however, the “414 gang” suggested something even more terrifying. The computer criminal is the boy next door.

7. See, e.g., “*WarGames*” Scenario: Could it Really Happen?, NIGHTLINE, ABC NEWS, July 8, 1983, Show No. 565 (Transcript on file at National Center for Computer Crime Data, 4053 JFK Library, California State University, Los Angeles, California 90032); Preventing “*WarGames.***” NEWSWEEK, Sept. 5, 1983, at 48. The lasting influence of “WarGames” can be seen in the following headline: *Film Provided Model for Nasa Security Breach, Teen Says*, COMPUTERWORLD, Aug. 27, 1984, at 19. See infra note 16.
9. Id.
10. Id.
12. It may take another generation of women’s liberation before women are equally represented among the ranks of “computer hobbyists.” Despite a great historic tradition spanning from Ada, Countess of Lovelace, to Capt. Grace Hopper, computing has yet to eliminate sexism. See, e.g. Project on Equal Education Rights, *Sex Bias at the Computer*
In the media, Neal Patrick assumed the “Aw shucks, I only did it because you made it so easy” posture. He was moderately convincing, it appears, as editorials in a number of publications suggested that

---

Terminal-How Schools Program Girls (Jan. 1985)(available from PEER, 1413 K. St. N.W. Washington, D.C. 20005); D. Heller & J. Bower, COMPUTER CONFIDENCE - A WOMAN'S GUIDE (1983); Van Nuys, Why Is the World of Computers Dominated by Males?, 5 INFOWORLD, 35, at 8, 10; Larkin, Women in Computer Services, COMPUTERWORLD, Nov. 12, 1984, at 8, 10; but see Laberis, DP Less Sexist Than Other Fields, Women Say, COMPUTERWORLD, May 23, 1983, at 18; Henley, Mom Replies, CREATIVE COMPUTING 6 (Dec. 1984) (This somewhat tongue in cheek letter to the editor by the Director of UCLA's Women's Studies Program suggests that a software program for ditherheaded men called Jockware would be a fitting complement for the program called Women's Ware. Within the ranks of well-publicized “hackers,” Susan Headley, (also known as Susan Thunder) stands alone. A small but not insignificant number of women have been convicted of computer crimes. Perhaps reflecting the economic position of women in our society, the computer crimes involving women have involved input clerks accused of falsifying input at the computer terminals where they worked. See, e.g. U.S. v. Jones, 414 F. Supp. 964 (D. Md. 1976), rev'd, 553 F.2d 351 (4th Cir. 1977); Patricia Ferguson, Stanley Rifkin's female accomplice in his abortive attempt to commit a second wire transfer crime is discussed in Becker, Rifkin, A Documentary History, 2 COMPUTER/L. J. 471, 481-82 (Summer 1980).

13. It is hard to overemphasize the extent to which the “414 gang” was a media event. Neal Patrick was featured on the cover of NEWSWEEK, on Donahue, America's most respected talk show, on Good Morning America, in PEOPLE magazine, and in numerous lesser circulation publications. See supra note 8. A participant at the hearings where Patrick spoke wrote:

The first day of the hearings was a circus. The first two witnesses were Neal Patrick, one of the Milwaukee 414s, and Jim McClary, Division Leader of the Operational Security and Safeguards Division at Los Alamos. As a potential confrontation between victim and attacker it provided a great deal of drama, and it was truly a media event. Approximately 20 television cameras filmed the proceedings, and the clicking of the still cameras was occasionally so loud that the speakers could not be heard.


Articles and correspondence in both the general circulation and trade press focused on the kid who "did it," alternately applauding and condemning him. But what are we to make of the committee that made him into a national hero for having embarked on nothing more or less than a criminal path of electronic intrusion? And how do we explain to our kids that crime doesn't pay when, upon completing this simpleminded, pompous lecture before a group of credulous poli-
better security, and not punishing the bearer of bad news, was the answer to “hacking.”

B. Publicity Problems and Promises

“The hits just keep on coming,” an oft-heard disc-jockeys’ slogan, is true of computer crime as well. As this article is written in the early days of 1985, several significant cases await trial, and the newspapers are full of accounts of others not yet in the judicial stream.

Thus, it is clear that publicity continues to be a major factor in the computer crime world. Since Equity Funding’s “Billion Dollar Bubble” burst, the media has reported computer crime with great vigor. But counsel in recent computer crime cases have had to react to new and difficult problems. The tactics adopted in response present interesting practical and legal questions:

1. When Should Counsel Open His or Her Mouth?

Counsel handling a widely publicized case may quickly be inundated with requests for interviews, information, and leads. All of these requests require careful attention and planning, since they are likely to come quickly while other problems are vying for counsel’s

---


attention. The beginning of any such decision should be the common sense approach promulgated by the ABA Model Rules of Professional Conduct: "A lawyer shall not make an extra-judicial statement that a reasonable person would expect to be disseminated by means of public communication if the lawyer knows or reasonably should know it will have a substantial likelihood of materially prejudicing an adjudicative proceeding."\(^\text{18}\)

H. William Allen, chairman of the ABA Committee on Ethics and Professional Responsibility, suggests a possible exception to this rule which is of significance in computer crime litigation: "A lawyer might be justified in seeking publicity on behalf of a client, especially in a criminal case where a prosecutor has released information about the alleged offense and the accused offender."\(^\text{19}\)

Such a situation arose in the case of Ronald Mark Austin, and an aggressive media counter-attack ensued. Austin is currently awaiting trial in California,\(^\text{20}\) charged with a number of counts of computer crime based on his alleged "capture" of computer files in systems in the United States and Norway.\(^\text{21}\) To "capture" a file need mean nothing more than changing the password to the file, which can easily defeat its use by most unsophisticated users. Occasionally "capture" may also mean erasing the contents of a file. Robert Philibosian, the Los Angeles District Attorney at the time of Austin's arrest, immediately called a press conference. He claimed that Austin had gained access to sensitive data, damaged files, and caused "hundreds of thousands of dollars damage" to the computer systems he penetrated with his $200 home computer.\(^\text{22}\) California Assemblyman Tom Hayden visited Austin and took the opportunity to castigate the Los Angeles District Attorney for overstating the nature of Austin's crimes, trying the case in the media, and prejudicing Austin's rights.\(^\text{23}\)

\(\text{18. ABA MODEL RULES OF PROFESSIONAL CONDUCT Rule 3.6(a).}\)
\(\text{19. Front Page, supra note 3, at 82.}\)
\(\text{21. Id.}\)
\(\text{22. Student Accused of Plugging Into Pentagon Computer Link, Los Angeles Times, Nov. 3, 1983, at 5. This account of a news conference held by then Los Angeles District Attorney Robert Philibosian contains the following quotation: "This is not some childish prank. . . . We’re talking about something that damaged data, blocked use and has cost hundreds of thousands of dollars, so in that sense you’re talking about a theft from those companies and the federal government of hundreds of thousands of dollars." Id. But see Austin’s Accusers Cite Minor Overall Damage Done, UCLA Daily Bruin, Nov. 16, 1983, at 4.}\)
\(\text{23. Hayden Calls Austin Case “Whipped Up Emotionalism.” UCLA Daily Bruin,}\)
Common sense also dictates that counsel must not make any statement which might hurt the case or the client. However, applying this dictum is not always obvious. For instance, attorney Paul Piaskowski demonstrated two seemingly different views of his client’s interests in statements made to different media representatives. Piaskowski was quoted in a news story in the Milwaukee Sentinel and in a United Press release to the effect that the “414 gang,” of which his client was a member, had plugged into many more computers than the youngsters had been willing to admit. “This is just the tip of the iceberg,” he said, referring to published reports of a dozen violated computers.24 “You wouldn’t be far wrong if you took six times a dozen.”25 Yet his efforts were described in a subsequent article as designed “to portray the young men as computer hobbyists who were merely doing intellectual gymnastics; they had not meant to do any harm and certainly they were not criminals.”26

2. When Should Counsel Shut His or Her Client’s Mouth?

Another aspect of the high-publicity nature of computer crime is the possibility that a client will begin to like the sound of his or her own voice, particularly when it is amplified by media exposure. Ronald Mark Austin himself was besieged with phone calls from newspapers and television stations requesting interviews. His responses, contained in exclusive interviews for various local publications, included statements of trial strategy of questionable value to Austin’s cause. One needed only to read the newspapers to learn his defense. “The whole case centers around one word, ‘malicious,’” he said. “They have to prove that I was malicious and they won’t be able to do that.”27

Perhaps even more obviously in need of counsel was Steven Rhoades. Rhoades, already convicted of a computer crime in Los Angeles and on parole, agreed to be interviewed on a Los Angeles television news program about “hacking.” In a segment aired on Monday, November 26, 1984, he claimed that given a few days time he could “break into the Defense Department’s computers.” The following day

---

25. Id.
26. Front Page, supra note 13, at 79; See infra text accompanying notes 30 and 31 for a possible explanation of the apparent disparity.
it was reported that he was in Los Angeles County jail, having been arrested for a violation of his parole.\textsuperscript{28}

3. Can Counsel “Network’’?

In one of the most widely publicized computer-related misdemeanor prosecutions ever, a bulletin board operator was charged with publishing a telephone credit card number in violation of California law.\textsuperscript{29} Capitalizing on the widespread interest in the case generated by its apparent first amendment implications, Chicago attorney Paul Bernstein organized on-line legal assistance for Tcimpidis. The assistance was provided by attorneys and others who have access to computer bulletin boards.\textsuperscript{30}

4. Should Counsel “Cash in’’ on Publicity?

In response to the media’s interest in his client’s case, Paul Piaskowski, attorney for Neal Patrick, the Newsweek cover boy, was offering the rights to his client’s story and that of the other “414 gang” members for $20,000.\textsuperscript{31} He was reportedly unsuccessful with the American media, but garnered about $5,000 from European sources.\textsuperscript{32} Patrick had received a grant of immunity in return for agreeing to become the U. S. Attorney’s main source of information about the methods and activities of the “414 gang.”

C. Law Enforcement Reactions to the “Hacking Epidemic.”\textsuperscript{33}

Since the “414 gang” became news, “hacking” has been the


\textsuperscript{29} People v. Tcimpidis, Los Angeles Municipal Court, San Fernando Branch, No. 900532 (1984). Tcimpidis’ case was dismissed in 1985 based on a lack of evidence to substantiate the charges that he intentionally published the telephone credit card numbers in question.

\textsuperscript{30} Watt, Innocent Plea in On-Line Case, INFOWORLD, Dec. 3, 1984, at 17. A computer “bulletin board” bears only a functional resemblance to “bulletin boards” as they are commonly conceived. There is no board on which messages are posted. Instead, a computer system stores and displays messages to remote callers who read the messages on their own video display terminals, and sometimes make copies of the messages. Id.

\textsuperscript{31} See supra note 14; see also Raiders of Los Alamos Seek $20,000 for TV Rights, Milwaukee J., Aug. 17, 1983, at 1,6.

\textsuperscript{32} Front Page, supra note 13, at 80.

\textsuperscript{33} If any further proof of the sensationalistic nature of media coverage of “hacking” were needed, the use of the word “epidemic” to describe “hacking” should suffice. See Shea, The FBI Goes After Hackers, INFOWORLD, March 26, 1984 at 38-43, (hereinafter FBI). See also id. at 41 (quoting Gerald Schmidt: “It’s an epidemic. In practically every upper-middle class high school this is going on”). “Schmidt” identifies himself as John
"squeaky wheel" of computer crime. In response, law enforcement attention has grown considerably, as have private security initiatives:

1. Computer System Seizures

Faced with growing demand for protection from "hackers," federal law enforcement officials have had to operate with the considerable handicap of having neither legal tools nor up-to-date training sufficient for the job.\(^{34}\) Perhaps the most significant handicap is the difficulty federal law presents to the prosecution of juveniles.\(^{35}\)

A deterrent strategy seems to have surfaced in response to these problems. A justice official was quoted explaining the rationale of a "tough" public stance against youthful computer enthusiasts in order to "end the national craze of breaking into private computer systems."\(^{36}\) The federal government does not put juveniles in jail, according to an unnamed Justice Department official quoted in the *San Jose Mercury News*.\(^{37}\) "But there are a lot of other possibilities: some kind of commitment on the part of the parents, maybe a monetary penalty. Heck, just our keeping the equipment has got to be a hardship."\(^{38}\) At another point, unnamed officials were quoted to the effect that "search warrants allowing them to confiscate the computers will be their ultimate weapon. 'Some of these kids must miss their computers terribly,' said one agent."\(^{39}\)

2. "Stinging" Bulletin Boards


34. See *FBI*, supra note 33.
35. See infra note 60 and accompanying text.
37. *Id.*
38. *Id.*
39. Emmons, *FBI Pulls Plug on Boys' Game of Computer Tap*, Los Angeles Times, Oct. 14, 1983, at 1, col. 2. This account includes the well publicized detail of an FBI agent climbing through a teenager's bedroom window and declaring, "Hold it right there; that computer is mine!" *Id.*
40. For a discussion of the operation of electronic bulletin board systems, see Soma,
Arizona, a sheriff's office bulletin board set up to facilitate contact with the public led to an unanticipated prosecution. A sixteen year old posted a message offering to install a device on television sets which would allow customers to access pay-TV stations without payment. The youth was arrested after the message was investigated.41

In a similar effort purposely set up to "sting" hackers, the United States Air Force allowed the circulation of AUTOVON dialup numbers on a "hacker bulletin board." Several months lapsed before the Air Force announced that it had been recording the numbers of those who had called the AUTOVON number.42

3. Informants

As indicated above,43 informants have become a necessary feature of hacking investigations. As in other criminal situations, arrested suspects have, on occasion, become police informants in "hacking" cases.44

D. Legal Approaches to Computer Crime

Calls for legislation at both the federal45 and state46 levels have increased in volume and intensity since the advent of "hacking." These calls are a response to the increased public visibility of computer crime since the "hackers" have become big news. This is not surprising, given the prominence played by Neal Patrick and other self-styled "hackers" who testified to their ability to enter a variety of computer systems quite simply with the technology available to most computer users.47

42. FBI, supra note 33, at 44. AUTOVON is a private telephone system connecting computers on every Air Force Installation in the world. Id.
43. See supra note 33.
44. See, e.g. Police Use Teen Computer Whiz to Track Hackers, San Diego Evening Tribune, Sept. 1, 1984, at 1.
47. See supra note 13 and accompanying text.
State legislatures are considering and enacting computer crime legislation with increasing frequency. Currently, thirty-eight states have computer crime laws. The odds are strong that this figure will increase by the time this article reaches publication.

On the Federal level, two bills have already been passed. The number of proposed laws has grown dramatically, and with them the breadth of solutions offered. They range from the simple to the remote.

A number of novel approaches to computer crime have accompanied this new legislation. Of particular importance are new protections of the right to privacy, civil remedies for victims of computer


50. All the following bills are from the 98th Congress, 2d Sess., and can be found at pp. II-1 through II-61 in BloomBecker, (ed.) Computer Crime Law Reporter. The Hughes bill, H.R. 5116, parts of which became law, incorporated much of the Nelson bill, H.R. 1092, as well as providing for punishment of credit card crimes. Rep. Mica's bill, H.R. 4384 would set up a commission to study computer crime, and Sen. Cohen's and Congressman Coughlin's, H.R. 4301 would offer alternatives to the definition and punishment scheme of Rep. Nelson. See Bortnick at 5-8, L. Becker at 7-10.

51. See, e.g., CONN. GEN. STAT. § 20-175 (1981); VA. CODE §§ 18.2-152.1 - 18.2-
Two areas of the law most immediately called into question by "hacking" deserve further comment:

1. Intent

When Ronald Mark Austin noted that the success of his prosecution would depend on proof that he had acted maliciously, he raised an important issue. One of the key legal questions posed by "hacking" is the issue of intent. In many cases, the systems accessed by "hackers" document the unauthorized entries made. The identity of the person making the access usually requires independent evidence, but often it can be established by admissions or testimony of admissions to others.

Thus, the question of the intent with which a computer system is accessed is of considerable importance. At the time of the alleged crimes by Austin, there were two relevant paragraphs defining computer crime in the California Penal Code:

Any person who intentionally accesses or causes to be accessed any computer system or computer network for the purpose of (1) devising or executing any scheme or artifice to defraud or extort or (2) obtaining money, property, or services with false or fraudulent intent, representations, or promises, shall be guilty of a public offense . . .

and

Any person who maliciously accesses, alters, deletes, damages, or destroys any computer system, computer network, computer program, or data shall be guilty of a public offense.

Subsequently, a California legislator introduced a bill to add a paragraph to the Penal Code defining non-malicious access to a com-
puter system as a misdemeanor. This paragraph adds a section (2) to 502 (d), renumbering the former 502(d) as 502(d)(1).

Section 502(d)(2) reads:

Any person who intentionally accesses any computer system, computer network, computer program, or data, knowing that the access is prohibited by the owner or lessee, is guilty of a misdemeanor. This paragraph shall not apply to any person acting within the scope of his or her employment. 59

2. Juvenile Law

One of the major unresolved problems in the prosecution of "hackers" is the fact that federal law and practice virtually guarantees that all but the most significant computer crimes perpetrated by juveniles will not be prosecuted under federal law. A provision in the United States Code requires that before a juvenile is tried in a United States federal court the Attorney General, after investigation, certify that "the juvenile court or other appropriate court of a State (1) does not have jurisdiction or refuses to assume jurisdiction . . . or (2) does not have available programs and services adequate for the needs of juveniles."60

E. Business Perspectives on Computer Crime

The change in attitudes toward computer crime in the past three years is not limited to the public. The business community, partly because it is made up of the general public, and partly because it is in the business of agreeing with the general public, has seen fit to develop a number of levels of response to computer crime.

GTE Telenet, a victim of unauthorized access by the "414 gang"61 and the owners of the computers confiscated by the FBI, pub-

59. Id. 502(d)(2); Computer Crime Law Reporter, II-63 - II-67 (BloomBecker ed.).
60. 18 U.S.C. § 5032 (1985). As a matter of practice, the U.S. Attorneys' office seldom attempts to fulfill the requirements of this section, choosing not to prosecute juveniles instead. In conversation with members of the U.S. Attorney's office in Detroit, I was told that juveniles accused of hacking in the raids referred to supra, at note 33 were not prosecuted. The representative of the U.S. Attorney's office in Detroit decided that the case against the juveniles should be prosecuted by the state authorities, if anyone, and assumed that the priorities of the Wayne County District Attorney's office were such that there was no point in referring the juveniles in question. (Personal conversation with U.S. Attorney). This assumption was challenged by the Wayne County prosecutor when I asked about it. (Personal conversation with prosecutor).
61. See supra text accompanying notes 8-11.
licized its view in a full page advertisement in the *Los Angeles Times* and elsewhere:

Today there’s a new breed of criminal. His weapon is the personal computer. His target: the corporate computer. Unfortunately, this criminal is unwittingly assisted by hackers who make computer trespassing seem innocent. It is not. Computer crime is costing business millions of dollars a year. And the problem is growing.62

IBM, in equally impressive ads, places its emphasis elsewhere: “There are rules for driving a computer, too. . . . when it comes to keeping information secure, each one of us is in the driver’s seat.”63

Living up to its own theory, IBM has demonstrated that it is clearly in the driver’s seat where its own information is concerned. An increasingly high posture has marked IBM’s efforts to protect proprietary information about its products. Most notable of its efforts was the “sting operation” performed by IBM-trained FBI agents after IBM was made aware of the theft of ten notebooks said to contain highly valuable information relating to its introduction of a new generation of computers.64

Hitachi, a leading Japanese producer of IBM-compatible computer components, knew that the information would offer it considerable competitive advantage by allowing it to introduce its products before others. Therefore, Hitachi was willing to pay for the notebooks, for samples of the equipment itself, and for other documents and information.65

A computer consulting firm in Silicon Valley had been established before Hitachi’s interest was made known to the FBI.66 Although the FBI initially intended to use the firm as a front to catch people sending high technology to Russia, it was used in the Hitachi case as well.67 An FBI agent was introduced to the Hitachi representative, Kenji Hiyashi, as the main contact from within IBM. To assure that no

66. *Id.*
67. *Id.*
charge of entrapment be later made, the agent communicated to Hiyashi that the information Hitachi sought could be gotten only illegally, and that whoever did it could be prosecuted if caught, as well as shamed.  

Complete with damning video and audiotapes of conversations establishing the entire enterprise, the government and IBM were able to convince Hitachi to plead guilty, and pay a sizeable amount to IBM.

In other cases, IBM and a growing number of other victims have engaged undercover investigators to make cases of theft of corporate information, violation of copyright in the copying of computer games, theft of computer components, and theft of telephone and computer services. To date no successful challenges to these undercover operations have been reported to the Center. The author, however, has little doubt that they will follow the same general pattern as other challenges based on entrapment.

F. "Hackers" as the Huckster's Dream

One might have expected that some enterprising computer security vendor would eventually attempt to exploit the attention paid to the "414 gang." Sure enough. A San Francisco Bay area company selling access control software produced a button saying "We're the 415's." Normally off the record, or among their own, computer security specialists are often heard to voice thanks for the "hacker phenomenon." Nothing has been as good for the computer security business

68. Id.
70. For a discussion of entrapment in the context of non-computer crime cases, see Mascolo, Due Process, Fundamental Fairness, and Conduct that Shocks the Conscience: The Right Not to be Enticed or Induced to Crime by Government and its Agents, 7 W. NEW ENG. L. REV. 1 (1985).
71. A button measuring 5 inches in diameter was distributed to attendees at the 1983 Computer Security Institute Conference. It read: "Computer Security? We're the 415's." (Button on file at National Center for Computer Crime Data). And in what could be the continuation (or the fitting end) of the trend, the National Center for Computer Crime Data will call its First Annual Statistical Report on Computer Crime "416." See supra note 4.
as hackers. And with millions of dollars being invested weekly in new computer systems, the belief in the need for increased computer security carries with it the potential of a new and relatively untapped market for security devices.

These products provide all sorts of security, including better personal recognition through retinal patterns,73 or fingerprints;74 fewer unauthorized telephone accesses by the installation of call-back systems on remote access computer systems75 or more sophisticated access control systems;76 encryption of data kept in computer systems;77 special keys without which one cannot operate certain programs;78 programs to prevent software copying;79 and programs to disable programs to prevent software copying.80 They also suggest a number of questions for defense counsel to raise when a victim has failed to buy them,81 and a wealth of information for the investigator of a computer

73. "The Solution is Eyedentify" (promotional flyer from Eyedentify, 1225 Northwest Murray Rd., Portland, Oregon 97229, on file at the National Center for Computer Crime Data).
77. Kirchner, Encryption Endorsed as Way to End Hacking Plan, COMPUTERWORLD, Nov. 21, 1983, at 13; Why Not DES? (promotional flyer from Integrated Applications Inc., 8600, Harvard Ave., Cleveland, Ohio 44105, on file at the National Center for Computer Crime Data); Phasor (promotional flyer from International Phasor Telecom Ltd., 134 Abbot St. Vancouver, British Columbia V6B 2K6, on file at the National Center for Computer Crime Data); Teneron Solutions (promotional flyer from Teneron, 6700 S.W. Beaverton, Oregon 97005 on file at the National Center for Computer Crime Data).
80. "Backup Protected Software with Copy II PC" (advertisement in INFOWORLD, Dec. 3, 1984, at 80). The last sentence of the advertisement states: "This product is provided for the purpose of enabling you to make archival copies only." A similar advertisement on the preceding page offers the same type of product for Apple computer software. Id. at 79.
81. Grenier Jr., Martin, & Winkler, Liability for Breaches of Data Security—How Courts Consider Standards of Care and Technological Feasibility (Presentation at 2d International Conference on Communications, Stockholm, Aug. 8-12, 1974) (On file at Criminal
crime case.

In addition, the new interest in computer security has created a market for a variety of computer security information services not previously available. For instance, the attorney seeking a consultant in computer security can first consider the spotty but unique Computer Crime Expert Witness Manual. Furthermore, the Computer Security Institute, EDP Auditor’s Association, Information System Security Association, ACM Special Interest Group on Security Audit and Control, and the American Society for Industrial Security National Computer Security Committee represent several reliable referral sources for individual consultants.


83. Information about the Computer Security Institute is available from 43 Boston Post Road, Northborough, Massachusetts 01532. See infra note 96 and accompanying text.
84. Information about the EDP Auditor’s Association is available from P.O. Box 2051, Winter Park, Florida 32789.
85. Information about the Information System Security Association is available from P.O. Box 71926, Los Angeles, California 90071.
86. Information about the ACM Special Interest Group on Security Audit and Control is available from ACM, 11 W. 42 St., New York, New York 10036. See infra note 93 and accompanying text.
88. Information about COMPUTER FRAUD AND SECURITY BULLETIN is available from Elsevier International Bulletins, 52 Vanderbilt Ave., New York, New York 10017.
89. Information about COMPUTER CRIME DIGEST is available from the National Center for Computer Crime Data, 4053 JFK Library, California State University, 5151 State University Dr., Los Angeles, California 90032.
90. Information about COMPUTER CRIME LAW REPORTER is available from the National Center for Computer Crime Data, 4053 JFK Library, California State University, 5151 State University Dr., Los Angeles, California 90032.
91. Information about DATA PROCESSING AUDITING REPORT is available from Box 85 Middleville, New Jersey 07855.
92. Information about COMPUTER SECURITY DIGEST is available from 711 W. Ann Arbor Trail, Suite 4, Plymouth, Michigan 48170.

Thus, we can see that the effect of capitalism has been mixed. The marketers have certainly contributed to the publicity surrounding the issue by reproducing the stories and feeding the media with additional examples and readily available experts to decry the increasing incidence of computer crime. They have also invested in some of the informational resources like the publications mentioned above.99

G. Computer Crime in Court

The author has not placed the analysis of computer crime in the courts last to build suspense, but rather to place it in relation to its significance. Compared to all the activity reported, the number of computer crime cases actually tried is alarmingly small.100 Alarming, that is, to someone attempting to fill an article like this with useful advice for litigators, or impatiently trying to divine the implications of the many computer crime laws now in place. Nonetheless, a brief survey of unsuccessful computer crime prosecutions may be a useful foretaste of future developments:

1. Dismissals

In perhaps the most widely reported computer crime dismissal, a

93. Information about SECURITY AUDIT AND CONTROL REVIEW is available from ACM, 11 W. 42 St., New York, New York 10036.

94. Information about EDPACS is available from 11250 Roger Bacon Dr., Reston, Virginia 22090.

95. Information about COMPUTER SECURITY ALERT is available from 500 N.E. Spanish River Blvd. No. 8, Boca Raton, Florida 33431.

96. Information about COMPUTER SECURITY is available from 43 Boston Post Road, Northborough, Massachusetts 01532.

97. Information about CONSCIENCE IN COMPUTING is available from the National Center for Computer Crime Data, 4053 JFK Library, California State University, 5151 State University Drive, Los Angeles, California 90032.


99. See supra notes 88-98 and accompanying text.

100. It appears, based on preliminary results of the National Center for Computer Crime Data's survey, that since 1976, when the first computer crime law passed, less than 200 cases of computer crime have been prosecuted in all the jurisdictions which have such laws. Of a sample of 52 cases reviewed by the National Center for Computer Crime Data in a preliminary report on its Computer Crime Census, 2 had gone to trial, and 13 were still pending. See BloomBecker, Preliminary Results: NCCCD Computer Crime Census, A Presentation to the National Association of Attorneys General, May 15, 1985 (on file at the National Center for Computer Crime Data).
trial judge virtually invited the state legislature of New York to supplement its theft of services laws with a computer crime statute. An employee of the New York City Board of Education was charged with theft of services based on his use of the board's computer for personal and small business purposes. The media made much of his use of the computer for horse genealogy records, suggesting in some reports that the computer was being used in horse-race handicapping or the running of betting pools. The case was dismissed when the court found that services could be the subject of theft of services law in New York only if they are offered for sale. Thus, since the board of education was not in the business of selling computer time, its employee could not be prosecuted for using that time.

Another county employee was less successful in his attempt to fight a charge of moonlighting involving the use of computer services. Michael McGraw, while a computer programmer for the Indianapolis Department of Planning and Zoning, was charged with theft based on his use of the city's computer to keep records of his sales of weight-loss products. After a jury found him guilty, the trial judge overrode the verdict, ruling that the Indiana theft law was not specific enough to cover the theft of computer time. On appeal the trial judge was reversed. The McGraw case received considerable publicity, even though the value of the computer time taken was calculated by the prosecution as being an almost trivial amount.

The following cases may help to demonstrate some of the difficulties of prosecution even when there is a computer crime law in effect. For instance, a Michigan computer crime law was held not to cover an alleged extortion when a programmer refused to tell his former employer how a program he had written worked. He argued that the employer owed him $19,500 for the programming work he had done. The court found no criminal intent in the programmer's actions, noting that the employer could have gotten access to the pro-

102. Id. at 1017, 450 N.Y.S.2d at 958.
103. Even a scholarly monthly fell prey to the media hype of this case. The Winter 1984 issue of ABACUS asked “Would you like to use your company’s computer to play the horses?” ABACUS, at 66 (1984). Commendably, computer law expert Michael Gemignani noted in the text: “He [Weg] was not accused of using the computer to place wagers . . . as some stories suggested.” Id.
104. Weg, 113 Misc.2d at 1021-23, 450 N.Y.S.2d at 960-61.
105. Id.
107. Id.
109. Id.
gram while it was being developed, and its failure precluded a finding of criminal intent on the part of the programmer.110

In California, an argument aimed more at the gut than the head seems to have carried the day for one defendant accused of computer crime for fooling a computerized ticket machine used by the Bay Area Rapid Transit System.111 Despite successful prosecutions of other such crimes, one judge dismissed a case based on the argument that the ticket machine was nothing more than a big “Coke” machine.112

Analogously, a flaw in the Utah computer crime law noted by the Utah Law Review113 may explain why that jurisdiction has had no computer crime prosecutions in the five years its statute has been on the books.

2. Sentencing

As with most white collar crime, and most cases where both sides see the possibility of greater losses in trial than in negotiation, most of the computer crime cases studied by the National Center have been resolved by plea-bargaining.114 Very few of those in which prosecution was initiated resulted in dismissals, making the sample above more significant than would otherwise be the case. Despite continued requests for such information from parties interested in the Federal Computer Systems Protection Act,115 there is still no body of cases demonstrating the difficulties experienced by federal investigators of computer crime.

The “414 gang,” the cause of much of the interest in computer crime in October of 1983, was resolved with more of a whimper than a bang. Two twenty-two year olds, Gerald Wondra and Thomas Winslow, plead guilty to two counts of making abusive interstate phone calls, and each was fined $1,000 and placed on probation.116

110. Id.
111. People v. Moore, Alameda County Superior Court (California) No. 71976 (1981).
112. Id.
114. Thirty of the thirty-two guilty findings in the National Center for Computer Crime Data’s Computer Crime Census were the results of pleas. See supra note 100.
116. United States v. Wondra, 84-Cr 42 United States District Court, Eastern District of Wisconsin; United States v. Winslow, 84-Cr 41 United States District Court, Eastern District of Wisconsin.
One of the individuals arrested as part of an FBI raid\textsuperscript{117} was given two concurrent sentences of one year's probation after he had cooperated with prosecutors and recommended stricter security procedures for GTE, the victim of his computer abuse.\textsuperscript{118}

II. CHALLENGES IN THE LAW

A. \textit{A New De Minimus}

At the heart of much wrangling about "hacking," and implicit in many other theft of computer time cases, is the question of the valuation of computer time and services. Both prosecution and defense will benefit from an agreement as to what amount of computer use is too trivial to justify criminal treatment. A trivial amount of computer use, although illegal, will not warrant prosecution, just as the possession of small quantities of drugs does not warrant prosecution. Since computer time is much more complex and variable in nature than a relative fungible like marijuana, the effort is likely to be more challenging.

B. \textit{Challenging the Exercise of Investigatory and Prosecutorial Discretion}

As suggested above,\textsuperscript{119} the use of federal power to arrest juveniles and seize their computer equipment without the apparent ability or intent to try those arrested for any crime is a questionable tactic that may be current in law enforcement reactions to "hackers." Although discriminatory prosecution arguments have been raised in a few adult computer crime defenses, none has been successful, as far as the National Center has been able to ascertain.

C. \textit{Challenging Victims' Business Methods}

The "414 gang" was praised in some circles for performing the invaluable service of demonstrating the pitiful state of some businesses' computer security precautions. Particularly alarming were their entries into computer systems in which the passwords had never been changed, and could be ascertained in general documentation for those systems. Often arguments in defense of the "hackers" stress the fact that but for this negligence, many of the crimes committed would not have been possible. These arguments, while possibly persuasive on

\textsuperscript{117} See supra note 33.


\textsuperscript{119} See supra notes 32-35 and accompanying text.
a common sense basis, have received no legal recognition. With the growing focus on intent with which access is made, it seems clear, however, that security features which communicate that a system is private and, therefore, not open to outsiders' use, will help establish the element of knowing lack of authorization to use a computer system which must often be proven to establish the commission of a computer crime.  

III. CONCLUSION

The "hacker phenomenon" has significantly increased the likelihood that an accused computer criminal will enter the office within the next couple of years. To help the attorney avoid the feeling of being left behind by the revolution (and because it will help him or her run the law business), this author suggests that the reader acquaint his or herself with the nearest personal computer store. Why should others be the only ones half scared and half delighted to be joining the computer generation?

The media has discovered the computer crime problem and labeled it "hacking." In this atmosphere, as this article suggests, there have been flurries of activity by law enforcement, legislatures, computer security vendors, and even attorneys. What significance and what value these activities have in terms of reducing computer crime is yet to be seen, given the paucity of reliable statistics on the topic. The words of the doctor in *Portnoy's Complaint* provide an apt conclusion to this article: "Now vee may perhaps to begin. Yes?"