UIC John Marshall Journal of Information Technology & Privacy Law

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

Article 16

1980

Computer Abuse Research Update, 2 Computer L.J. 329 (1980)

Donn B. Parker

COMPUTER ABUSE RESEARCH UPDATE†

By DONN B. PARKER*

INTRODUCTION

The purpose of this update is to provide a brief explanation of the nature of the Computer Abuse Research Project conducted at SRI International for the past nine years and funded by a series of grants from the National Science Foundation ("NSF"). The charter and general purpose of the project both in relation to the data processing profession and society at large are explained. Computer abuse and crime are defined, and the working file of reported cases and its use are described. Finally, a survey of prosecutors' concepts of computer crime is reported. A bibliography of the SRI Computer Abuse Project in recent years is appended to the article.

With the ever-expanding coverage of computer abuse research in the mass media, in magazines and trade publications, in the law enforcement community, and among legislators, it becomes increasingly important to clarify the purposes, methods, and objectives of the SRI project. Interest in such research reflects the proliferation of computers in all segments of business, government, and society at large and increasing reports of computer crime. The United States Chamber of Commerce estimates that losses from business, economic, and white-collar crime may cost more than $40 billion per year. A central objective of the Computer Abuse Research Project was to begin to lay a foundation on which the relationship between the proliferation of computers and the increasing reports of computer crime could be studied. Methodologically, it was equally important to determine both the nature and the extent of their coincidence. SRI's working file of reported computer abuse cases reflects this exploratory approach—here, one of gathering relevant data.

The objectives of this approach are an awareness and under-

† This article was prepared by SRI International. Points of view, opinions and conclusions stated herein are those of the author and do not necessarily represent the official position or policies of SRI International.

* Senior management systems consultant, SRI International, Menlo Park, California 94025.

standing not only of computer crime but also of the means of deterrence, detection, and prevention of abuses that arise in the use of computers. The 1976 proposal abstract for the most recent three years of research under National Science Foundation Grant MCS-7601242 stated:

> The objectives of the research proposed by Stanford Research Institute (SRI) are to assess the problem of reported computer abuse and to devise control and prevention techniques. An initial phase (Phase I) of computer abuse research, recently completed by SRI under NSF Grant GI-37226, demonstrated the existence of the problem of computer abuse and gave an indication of its scope. Current research (Phase II), nearing completion under NSF Grant GJ-44313, is aimed at performing a problem assessment. The 3-year research program proposed herein carried forward the concerns of these earlier phases and emphasizes computer abuse prevention and control.
>
> The proposed research will continue the development and expansion of SRI's file of case histories (currently containing records for 350 cases) and will computerize the file. The research will also continue development of a taxonomy of threats, and examine the technical and operational prevention and control techniques for computer abuse, the effects of advancing computer technology on white collar crime, legal implications of computer abuse, the nature of computer abuse as white collar crime, social loss from computer abuse, privacy violations, bureaucratic computer problems, and future aspects of computer abuse.
>
> Two coordinated research efforts will be undertaken, one in law and the other in computer science, using field investigation, interviewing, case documentation, case analysis and application, and law and literature searching. A conference will be held, and progress reports and papers will be produced.

The Computer Abuse Project is *not* a rigorous, sociological, statistically based crime study. An abiding aim of the project is to develop a body of knowledge that will attract the interest of qualified sociologists, statisticians, computer scientists, criminologists, and criminal justice experts. The work is a new field of inquiry in a science (computers) that itself is not much more than thirty-five years old. The first proposal to the National Science Foundation in 1971 was correctly rejected as a crime or antisocial sociological study on the basis that the project staff was made up of computer management/technology researchers and an attorney. However, the project was funded by the Mathematical and Computer Sciences Division of NSF as an exploratory, and later, problem assessment empirical study. Its mandate was to collect and report on incidents of reported abuses involving computers, to explore the technological implications of such abuses, and to conduct legal research on the technical adequacy of the law.

This project is organized to explore and assess the new and changing problem of computer abuse on the basis of a limited, somewhat biased collection of reported cases. The project has shown the existence of a problem and some of its ramifications for computer technology, computer management, and the law.

Few researchers have attempted serious work on this subject because valid information is difficult and expensive to obtain. The principal source of information is from the cases that have been discovered *and* in many instances publicly reported. Such cases reveal little, however, about the most important cases—that is, those that have not been discovered because of the perpetrator's success—and about others that are not reported for various reasons. This is the nature of any research on abuse and on crime in particular. In this sense, therefore, the amount of business or white-collar crime that occurs is unknown. Unlike other areas of research, criminological research is usually performed empirically by using individual case studies and by studying limited, narrow aspects.

Computer abuse as defined in this project[1] is necessarily so broad and diverse as to cover any kind of crime, civil suit, or dispute between two or more parties that involved a computer. The possibility is thus remote that an exhaustive search across this spectrum could provide a statistically valid population that could be used to determine statistics such as mean, standard deviation, etc. Therefore, the project has been self-limited to recording all reported cases that can reasonably be found, and to verifying as many of them as possible to provide at least a lower bound on the number of accurately reported cases. From these cases, we may report on the nature of the perceived problem by case example. The results of this procedure have been most valuable in both improving computer security and in finding shortcomings in the law. It is a continuing study, and results change as more loss experience becomes known and technology and its applications change.

I. The Profession and Society

Data processors are in positions of high trust. If they were not an honest community, the use of and reliance on computers would already be slowed by an onslaught of abusive acts. Data processing people are well paid, in great demand, have invested much effort in achieving their technical capabilities, and have interesting and challenging work. All of these factors most likely contribute to a low incidence of abusive acts within the data processing profession.

1. *See* Section II *infra*.

Nevertheless, as in any occupation of large size and high mobility, a certain number of persons will be dishonest or become so under certain circumstances. There are others who have high ethical standards, but who have learned to ignore them in a technical environment that treats individuals equally regardless of their ethical standards and where abusive acts can be easily concealed. Documented experiences in this project have shown that such people do exist and that their potential for doing harm is growing as the percentage of assets and asset records processed by computers increase. The mass media has always given high visibility to computer crime. The public is fascinated with new, innovative criminal activities. This results at times in treating computer criminals as folk heroes rather than as the miscreants they really are.

Contact with the media is a part of computer abuse research. Information in the news media represents a significant source of computer abuse cases. This information varies considerably in accuracy, precision, and thoroughness. Cases reported in computer trade publications, such as *Computerworld*, tend to have relatively higher validity and are based on direct inquiries and information from technically knowledgeable persons. In the general press, more than one article by more than one reporter generally increases the accuracy and quantity of information. Problems arising from conflicting information are resolved by choosing the information point-by-point and rating it according to plausibility, reliability of source, and in-parallel coverage by the latest available, dated report.

Contact with the media represents a two-way street. The project staff and management have had continuing concern about distorted reporting of research results in dealing with journalists worldwide. At one time, all cooperation and all interviews with the media were brought to a halt. This resulted in even less accurate, more distorted reporting of the project's findings. It was then agreed that we would maintain a policy of no overt seeking of publicity, with the exception of press releases to announce the completion of studies. Full cooperation, including the reporting of positive as well as negative findings, is now given on the media's request. This seems to produce the most satisfactory results. Unfortunately, misquotes and distortions still occur, but with less frequency as journalists begin to become familiar with the technical problems at issue and to appreciate the positive aspects of computers. It is hoped that this will in turn raise the level of knowledge of those that report computer abuse cases.

The book, *Crime by Computer*,[2] written by the project leader

2. D. PARKER, CRIME BY COMPUTER (1976).

was published four years ago and is now out-of-date and out-of-print. This book presented a nontechnical perspective of computer abuse; it was prepared for lay persons and was intended to dispel the misinformation in the media and also to alert computer users to the nature of the problem in easily and interestingly readable form. The book was written and supported totally independent of SRI and research sponsors. Only the research working file and publications that are in the public domain (and therefore available to anybody) were used as sources.

II. Computer Abuse Definitions

A working definition of computer abuse was necessary from the outset of the project. Of itself, the definition became a working hypothesis. It also served as the basis for the exploratory selection and collection of unanticipated types of cases to be categorized and studied. An error or omission of a type of case could have, at some later date, severely restricted this exploratory nature of the project.

The necessarily broad definition of computer abuse used is: any intentional act associated in any way with computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made, a gain. "Malicious" or "with intent to harm," could have been added, but we believed that the terms "victim" and "perpetrator," in the context of the definition, were sufficient.

This definition relates to computers in the most general way possible. Even if a stronger relationship between computers and abuse were used—for example, "an incident in which a computer is directly and significantly instrumental in an abusive act"—the problem of specificity remains. This problem has been eased by refining the definition in several ways. Further generality is achieved by extending the definition to include any case from which there is something to be learned that directly aids in revealing vulnerabilities or legal shortcomings in computer use and that supports the use of computer security safeguards or new legislation on computers. Another refinement is the identification of the four roles that computers play in computer abuse:

- *Object*—Cases include destruction of computers or of data or programs contained in them or destruction of supportive facilities and resources, such as air-conditioning and electrical power, that allow computers to function.
- *Subject*—A computer can be the site or environment of a crime, or a computer can be the source of, or reason for, unique forms and kinds of assets, which can be manipulated in unique unauthorized ways.
- *Instrument*—Some types and methods of crime are complex

enough to require the use of a computer as a tool or instrument. A computer can be used actively, such as to automatically scan telephone codes for working combinations that can later be used to make unauthorized use of a telephone system. A computer can also be used passively, such as to simulate a general ledger in the planning and control of a continuing financial embezzlement or fraud.

- *Symbol*—A computer can be used as a symbol for intimidation or deception. This could involve the false advertising of nonexistent services, such as has been done by several computer dating bureaus.

A limitation on the broad definition is the rejection of a case, if the substitution of a device other than a computer or computer-related device would not materially change the nature of the incident or the nature of the skills and knowledge needed by the perpetrator. The theft of a terminal and the fencing of it for resale would not be a computer abuse case if substitution of, for example, a typewriter would have made no difference in the methods, motivations, skills, knowledge, or resources involved in the incident.

The application of this broad definition of computer abuse to specific cases is difficult. For example, most credit card fraud is excluded from the file because the perpetrator did not have direct contact with a computer and was not in collusion with someone who did, or because the perpetrator did not use a characteristic of the computer system to make the fraud workable. The difficulty of specific application makes considerable judgment and experience necessary for consistent classification. The need for sufficient information and the difficulty in obtaining it is also a motivation for classifying cases on a best-effort basis when initially obtained, with reclassification when more information is obtained.

Theoretically, all types of crimes such as fraud, theft, larceny, extortion, conspiracy, espionage, sabotage, burglary, embezzlement, and murder could involve the computer. However, the occupations of the perpetrators, the methods of the crime, its environment, the forms of assets involved, timing (milliseconds and less), and geography (long-distance computer communication) can differ markedly when computers are involved, and thus warrant special treatment.

Other expansions and refinements of the broad definition of computer abuse have been used by the project for other purposes. In a study for the criminal justice community, cases of computer abuse were limited to those involving crimes, that is, one or more of the individuals involved were convicted of violating a criminal law. On another occasion, a computer-related crime was defined to be any illegal act for which a knowledge of computer technology and

usage was essential for perpetration and successful prosecution. It is possible to choose a definition that would rule out all but a few reported cases or one that would include many irrelevant cases. The goal in choosing a definition and applying it is to include all cases that may be relevant to the end purpose.

III. The File of Reported Cases and Its Use

Central to the Computer Abuse Research Project, both in method and purpose, is the working case file of verified and unverified reported instances of computer abuse. The method of collection is to include data relevant not only to verified cases, but also to reported cases, verified or not, that are plausible, indicate possible forms of computer abuse, or suggest types of computer vulnerability. The file is indexed to reflect the varying status of each case. Periodically, we publish the number of cases in the working file by type of source and remind readers of the difficulties of case collection and the variable quality of the file's information sources. We assume that this is sufficient to put the general results derived from the file in their proper context.

For example, in testimony before the Senate Subcommittee on Criminal Law and Procedures in June, 1979, I stated that "about 75% of the cases have been verified. The remainder have not been investigated and include reports for which sufficient data . . . have not been reported. Sources of case information include newspapers . . . ." In an SRI Report, *Computer Abuse Assessment*, reprinted in the Encyclopedia of Computer Science and Technology, it was stated that:

> The value of the research results is limited by the extent to which the data base of reported cases represents all cases. Conclusions must be based on the universe of the [cases] rather than the total universe of experience. Applying the conclusions to [all] cases beyond those represented by the [data base] is subject to statistical uncertainty. . . . Two instances have occurred where verified cases were subsequently found to be fictional, or at least not to contain sufficient basis in fact. Several unverified reported cases in the file are suspected of being without basis of fact, but remain in the file as real cases until proven otherwise. A number of cases were removed from the data base after discovery that they either did not occur, or occurred in ways that did not meet the requirements of the data base definition.[3]

A complete bibliography of project publications is included at the end of this paper.

The most basic difficulty in collecting and reporting case infor-

3. D. Parker, Computer Abuse Assessment 3, 10 (Stan. Research Inst. 1975).

mation is that the results can be based only on discovered and reported cases. Therefore, even though the number of reported cases per year appears to be growing at an exponential rate, the real or total number may be growing more slowly or even declining in number. We believe, however, that there is greater value in taking action to make computer use safer based on known reported cases and good judgment than in ignoring cases for lack of complete knowledge. We must accept that this may preclude protection from repetition of unknown loss experiences. In addition, we believe that reporting as much as is known of reported cases has a beneficial effect in motivating management to take prudent action and in aiding the criminal justice community.

The greatest value of the case file is in the application of example cases to computer security and criminal law research. Regardless of its stage of verification (including even fictitious cases), each case is valuable for determining the feasibility of its occurrence, computer security controls effectiveness, and the adequacy of the law to deal with it. For example, a project finding is that most cases involving the use of magnets to erase magnetically recorded data are fictitious. This discovery generated enough interest, however, that SRI and the United States National Bureau of Standards conducted laboratory tests to determine the feasibility of this practice. These tests demonstrated a low potential threat from the intentional use of magnets, resulting in appropriate modifications of security.

Another example of the file's value is the reporting of a series of incidents, some real and others possibly fictitious, of offenders replacing the blank deposit slips that the bank places on customer convenience tables with their own MICR codes preprinted by the bank. This resulted in deposits being credited to the offender's account. The reporting of these cases caused many financial institutions to change their deposit procedures, thereby ending this type of fraud.

The working file contains cases that have occurred since 1958. These cases include news clippings, excerpts from magazines and books, court proceedings, reports of law enforcement agencies, interviews with individuals involved, questionnaires from computer users, and documentation from everyone willing to report a case.

The collection of cases from news clippings is accomplished by project staff members scanning local news media, receiving clips sent to the project by interested parties, and by engaging a newsclipping service to collect all United States clips reporting nonviolent crime, suspected fraud, and civil suits. This results in about fifty clips per week that are scanned for involvement, or likely involvement, of computers.

During the nine years of monitoring news reporting and verifying reported information, the quality and accuracy of the reports have improved as reporters have become more knowledgeable about computer technology. Off-beat and human-interest news is often unreliable, but general news about an abusive act is usually sufficiently accurate for concluding that an act occurred if the names of participants and their quotes are used, and if it is from a reliable quality publication (*i.e.*, one that other research organizations use as a source). Parallel articles on the same case by different reporters are cross-checked. Even when technical facts are inaccurate, the text of the report will usually reveal whether or not computer technology played a role. The project currently has hundreds of news articles in a separate file pending examination to determine if they qualify for unverified status in the working file.

The reported-case file is not a statistical sample and is not intended to be statistically based because the total population of actual cases cannot be known. The file is biased in some known and probably some unknown ways, but this has been carefully stated in most of the recently published project research papers. However, this point is usually omitted in news and magazine articles written by others who reference the project's work. We have loosely called the computer abuse file of reported cases a computer crime file when to take the time to explain and define our precise meanings for a general audience would be secondary to another theme.

The specific results of the research are not based on the entire reported-case file, except for gross characterizations to show how the reported cases have grown and how trends have developed in the types of cases reported. Rather, the specific research results are based on subsets of applicable cases. For example, computer abuse perpetrators were characterized on the basis of information in twenty-six interviews with such persons, and the average reported gross loss per case in a subset of forty-two cases of banking-related abuse was found to be $430,000. Therefore, it is incorrect to assume that the research results are based on the entire file, which is known to contain unverified cases. The number and type of cases used have been stated in definitive project findings and are usually limited to those investigated by the project. As resources allow, from five to ten cases per year are investigated in the field.

By mid-1979, 669 cases had been reported.[4] Approximately sixty new cases have been collected since then, but have not yet been categorized and entered in the working file. In addition, news clippings

4. This number was subsequently reduced to 668 when field investigation revealed that the Penn Central boxcar theft case did not involve computers.

collected in the last eight months have not yet been examined for computer abuse incidents. The degree of case verification is established by using the eight rating code levels described below. The first character is alphabetic and is used as follows:

Y = The case has been verified.
N = The case has not been verified.
D = It is not certain that a computer was involved.

The second character of the rating code is numeric and orders the level of verification from high (for example, 1) to low (for example, 4). The full set of codes used and numbers of cases by level are:

No. of Cases	Code	Verification
147	Y1	Legal or law enforcement agency documentation sufficient to identify an act and the role of a computer.
141	Y2	Description of the act obtained directly from at least one reliable source or case participant or other reliable person if that person has supplied names of case participants.
246	Y3	Reliable public media reports identifying victim and quoting named investigating officials describing an accomplished act or stating official disposition of the case.
20	Y4	Description of the act obtained directly from at least one reliable case participant or other reliable person in which names of case participants have not been revealed.
554	Total verified cases	
45	N1	Reliable public media reports identifying a victim, but quoting no investigating officials or agencies.
59	N2	Reliable public media reports with no identification of participants.
7	N3	Other.
3	D1	Not certain that a computer was involved.
114	Total unverified and uncertain cases.	
668	Toltal cases (80% verified)	

The level N3 cases are documented in letters; one was documented orally. These include five cases personally investigated and described in a memorandum by Stanley Rifkin, who is now serving a federal prison term.

The application of the definition of what constitutes an unverified or verified computer abuse case has been under periodic study and change. The goal is to include all types of cases in anticipation that ultimate research purposes are not predictable as computer technology and its uses change. Published gross tabulations are derived from the entire reported-case file, including unverified, partially verified, and possibly a few fictitious cases. Recent cases too late for inclusion are always omitted.

There is value in collecting and studying reported cases that may be fictitious in order to discover new abuse methods being discussed publicly and to anticipate possible abuses in the future. This anticipatory awareness is necessary in the development of computer security because long lead times are needed to install controls in systems. Potential threats and potential vulnerabilities must be anticipated.

Data are tabulated by levels of confidence in case validity and by types of cases. As more cases are collected and future experience in cataloguing cases is gained, studies naturally have more meaning. That meaning will in turn motivate increased sophistication of the data tabulating. The project has never achieved one-hundred percent agreement among all staff members in categorizing all cases. Such is the nature of measuring and cataloguing human activities. This problem was partly overcome in the most recent vulnerability analysis (not yet published) performed by two people independently using a single set of rules and tabulating for each of several confidence levels of case validation.

It is expensive to validate and research cases. The increasing number of cases reduces the proportion of cases that can be adequately treated under fixed levels of project funding. Fortunately, increased funding is now anticipated, and a greater part of the project resources will be used to improve the quality of the case file.

The presentation of data has been limited to selected tabulations. Cross-tabulations and other statistical analysis have not yet been attempted because of the limited quality, quantity, and accuracy of the case data. The working file of reported cases has never been published for reasons of privacy and copyright protection and because it is a working, changing file. The file is available for others to examine at SRI's facilities in Menlo Park, California. Copies of the file have been made available to several serious researchers.

Data from the case file are now in a computer-stored data base accessible from SRI terminals. A computer program is in production use that provides twelve reports with data tabulated as follows:

(1) Incidence and loss by year and type of abuse (1958-1978 and four types).
(2) Identification and tabulation of cases by size of loss (twenty-one ranges).
(3) Identification and tabulation of cases by type of abuse (forty-seven types).
(4) On-line case descriptions by source of information received.
(5) Identification and tabulation of cases by state and country geographic location and type (four types).
(6) Case identification by victim name (private).
(7) Identification of cases by perpetrator or defendant name and occupation.
(8) Identification of cases by employee status, class of victim, number of perpetrators and collusion (yes or no).
(9) Identification of cases by perpetrator or defendant occupation.
(10) On-line case descriptions by keywords.
(11) On-line case description by case number.

A manual describing the data base and access systems has been prepared for project use.

IV. Computer-Related Crime

A questionnaire was developed by SRI International in 1979 under a grant[5] from the National Criminal Justice and Information Statistics Service, the Law Enforcement Assistance Administration (LEAA), United States Department of Justice, and sent to seventy-two district attorneys who participate in the Economic Crime Project of the National District Attorneys Association funded by the LEAA. The purpose of the questionnaire was to determine the degree and nature of experience with computer-related crime among offices that are focusing on economic crime programs. Responses numbered forty-six.[6]

Within the past five years, forty district attorney offices reported a total of 244 cases of respondent-defined, computer-related crime brought to their attention. Of these cases, 191 were prosecuted and

5. This report was prepared under Grant No. 78-SS-AX-0031 awarded to SRI International. Points of view or opinions stated herein are those of the author and do not necessarily represent the official position or policies of the United States Department of Justice or of SRI International.

6. A copy of the questionnaire with numeric tabulations of answers set forth in italics is reprinted at the end of this article.

157 convictions were obtained by plea and 10 by trial. Many more cases of fraud have been handled that involved data in computer-readable form: 311 reported, 215 prosecuted, and 158 convictions obtained by plea and 20 by trial. Averages of both types of cases are in the range of five to eight per office. Foremost in the number of cases reported are the offices in Nassau, New York with more than 100; Cook County, Illinois with 30; and Baltimore, Maryland with 20. Other offices reported ten or less. Clearly, there is significant experience and a proliferation of computer-related crime, but they are concentrated in only a few offices probably because of the localization of computers and of prosecutors who have taken an interest in and have knowledge of this type of case.

In regard to prosecutors, a significant number of them are gaining capabilities to deal effectively with computer-related crime. Of the individual prosecutors responding, sixty percent have read a book or manual on computers and have attended one or more courses or seminars on computers.

To determine the level of technical knowledge of respondents, the questionnaire asked whether they could explain to juries various technical concepts of computers. Over one-half said that they could explain the components of a computer, how a computer program functions, and what a programmer does. A few less could explain the source and object code forms of a program and on-line computer terminal protocol. However, few could explain a program branch function, distributed processing, multiprogramming, computer crime methods (such as "Trojan horse" and "salami"), and the meaning of DBMS (data base management system). Only one knew the meaning of ROM (read-only memory). The conclusion is that many prosecutors have more computer-related knowledge than would be expected, but it is relatively shallow and limited. Only one individual responded positively to all of the above subjects, and ten were knowledgeable on at least one-half of the subjects.

There is little agreement on what constitutes computer-related crime. Ten examples of computer-related crime as defined in the study were described on the questionnaire. Only one prosecutor agreed that all cases qualified as computer-related crime. All agreed that welfare payment fraud using a computer terminal and computer to create falsified inventory data qualified as computer fraud. All but five and eight respondents respectively also agreed that theft of a computer program from a computer and falsification of computer input forms for payroll processing are computer-related crimes. Only six voted for falsely claiming the use of a computer in an advertised service, about twelve voted for theft of a computer or

computer terminal, and one-half agreed that theft of a program from an office and use of a computer to plan and manage a fraud were computer-related crimes. This lack of concurrence on what is considered a computer-related crime could partly explain the disparities in the number of cases reported. Additional analyses that have not yet been performed could confirm this.

District attorney offices (number in parentheses) reported dealing with alleged crimes in which a computer or program played the following role in illegal acts (from most frequent to least frequent roles): contained evidence (28), used as an instrument (24), produced output material (19), was the site (14), was the object of theft (11), was the object of sabotage (5) and falsely claimed use to deceive or intimidate a victim (5). Several offices reported ten to thirty instances involving the more frequent roles. The reason for so few cases of sabotage and theft may be that the questionnaire respondents deal more with fraud, and therefore, may be unaware of the more common cases of damage and theft.

The number of offices that reported using various computer-related items for evidence varied from a few to one-half of the offices. Computer output listings have been used by twenty-eight of the forty-six offices including twenty-one that requested specialized output reports. Computer programs were used by fifteen in output listing form, eleven on printed paper, seven in punch cards, and six on handwritten forms. Only six used programs or data as evidence on magnetic tape, and two used them on disk packs. Computer media used in the order of most to least include output listings, punch cards, magnetic tape, punch paper tape, and disk packs. The use of disk packs will probably increase, and punch cards and paper tape will probably decrease as technology changes. Westchester County, New York reported the use of output listings more than five hundred times each for data and programs.

About one-half of the offices indicated experience in interrogating computer employees and computer terminal users. Several offices reported ten to thirty such interrogations.

To a question asked about best evidence forms of data, twenty-seven respondents chose handwritten pages, only four chose magnetic tape, and seven would not favor one over the other. Factors considered included "understandability, mistrust, and precedence." One respondent indicated that the issue of fraud may lie in the difference between handwritten material and data on tape.

Respondents to the SRI questionnaire were asked to rank the quality of four different draftings of a search warrant to search the contents of a computer and adjacent rooms for evidence of an al-

leged theft of a computer program. The best search warrant draft by a large margin was:

> Search for personal property consisting of remote plotting programs, specifications, and user documents in the form of: key punch computer cards, reels of magnetic tape, magnetic disks or packs, computer printout sheets, computer printout sheets you are to have produced by execution of computer output programs from the computer storage.

Ranked second of moderate quality was the text used in an actual search warrant in *People v. Ward*[7]:

> Search for personal property in the form of keypunch computer cards punched with the remote plotting programs, computer printout sheets with printouts of remote plotting programs, computer memory bank or other data storage devices magnetically imprinted with remote plotting computer programs, related documentation.

Ranked next of poor quality was:

> Search for personal property consisting of remote plotting programs and documented specifications and user documents in printed, punch card, magnetic media, or computer stored forms.

The draft ranked last appeared to be generally unacceptable:

> Search for personal property consisting of remote plotting programs and related documentation.

Respondents suggested the following variation as an alternative for the search warrant drafts:

> Search for: (1) user source documents; (2) user source deck (cards or other formats); (3) object decks (cards or other formats); (4) printouts of questioned program in action; (5) copies of computer logs, journals, etc. for time period in question.

Drafting this variation requires a person familiar with "source deck," "object deck" and "source documents." Another respondent pointed out that wording must not only be understandable by laymen, judges, and executing officers, but must also be technically precise and inclusive. Item (5) above, requiring copies of computer logs and journals for the time in question is an important inclusion.

Another variation suggested is as follows:

> To search for evidence or fruits of a crime in the form of data or information contained in or recorded upon computer-related devices and mechanisms included but not limited to computer cards, computer cards punched with the remote plotting programs, computer print out sheets, computer tape, magnetic disks or packs, or other computer printed or encoded devices or mechanisms, and data and information contained within the magnetic or electronic data stor-

7. A California Superior Court opinion in this case is reported at 3 CLSR 206 (Cal. Super. Ct. 1972).

age capacity of the computer or computers at said location; you are commanded to use the facilities of the computer or computers of said location to produce said aforementioned data or information in printed and legible form.

This variation is the most comprehensive except it lacks Item (5) of the previous variation. It may be too comprehensive, however, because it provides for seizing any materials or information whether or not related to remote plotting computer programs. These examples display some of the problems associated with legal definitions of computer-related crime.

This above-mentioned survey was conducted as a part of a larger project to develop a manual on investigation and prosecution of computer crime and not to characterize the computer crime activities of the thousands of prosecutor's offices. The questionnaire was not pretested, and follow-up sampling has not yet been done. Additional support will be sought for a statistical analysis of this survey's data based on cross-tabulation and further sampling to answer the following questions:

- What characterizes the offices that did not return the questionnaire?
- What characterizes the offices at the extremes of the data ranges?
- What factors explain the disparate number of cases reported and prosecutors' concepts of computer crime?
- What are the differences in responses by office based on the number of crimes reported by each office?
- What methods were used by the offices to produce the data they reported?

The most surprising result from this questionnaire is the large number of prosecutors gaining or having technical knowledge about computers. There are numerous opportunities available today to do this through books and seminars. On the basis of the frequent inquiries that SRI receives from an increasing number of law students, they are not only learning about, but also specializing in, computer technology.

More advanced computer training is now needed for investigators and prosecutors who have some familiarity with computer technology. The forms of such programs should be to make them fully capable of dealing effectively with computer-related crime.

V. Conclusion

Other research efforts are starting to expand the work of the computer abuse project. The National Computer Centre in Manchester, England is developing a similar case file. The Caulfield

Institute of Technology has a computer abuse project in Australia; its data on cases collected bear a marked similarity to the characteristics of SRI project data, but there are also some significant differences.

The United States General Accounting Office, with SRI assistance, performed a study of sixty-nine computer crime cases in the federal government in 1976. The original manager of the project, John R. Schultz, indicated that thousands of cases of fraud were reported in large payment systems, such as welfare and Social Security, where evidence resides in computer media. In the GAO study, an appropriate narrowing of the definition of computer abuse resulted in a more pertinent (to their purposes) and manageable number of cases. As computer abuse studies expand, the researchers will choose definitions and apply them in ways relevant to their end purposes and with methods suited to their field of endeavor. Finally, Jay Becker has started a collection of cases in his National Center for Computer Crime Data in Los Angeles.

The SRI project does not claim that the results of its research are representative of all abusive computer acts. As in all empirical research, there are partially supported hypotheses to be further supported or not, as experience and knowledge dictate. In the meantime, this project remains the only serious, comprehensive, ongoing study on this subject matter. It is hoped that efforts to support or improve upon the results will be based on new, more valid, and more accurate information.

SRI QUESTIONNAIRE (WITH TABULATED RESULTS)

Return to: Donn B. Parker
SRI International
333 Ravenswood Avenue
Menlo Park, CA 94025

From:

NDAA QUESTIONNAIRE

1. Have you or your office had any of the following experiences:

Yes and approximate number of times			
(No *6*	*27*)	A.	Used or obtained a magnetic tape for evidence?
(No *10*	*28+*)	B.	Used or obtained punch cards for evidence?
(No *2*	*2*)	C.	Used or obtained a magnetic disk or disk pack for evidence?
(No *28*	*708+*)	D.	Used or obtained a computer listing of data for evidence?
(No	)	E.	Used or obtained a computer program for evidence in the form of
(No *15*	*534+*)		1. computer output sheets?
(No *11*	*227+*)		2. printed sheets of paper?
(No *6*	*21+*)		3. handwritten sheets?
(No *7*	*23+*)		4. punch cards?
(No *2*	*2*)		5. punched paper tape?
(No *3*	*5*)		6. magnetic tape?
(No *2*	*2*)		7. magnetic disk or disk pack?
(No *12*	*73+*)	F.	Requested and obtained a computer output report that was generated especially for you from a computer?
(No *10*	*30*)	G.	Used a log or journal of usage of a computer or computer terminal?
(No *20*	*92+*)	H.	Interrogated a computer employee concerning his work (operator, programmer, etc.)?
(No *19*	*93*)	I.	Interrogated an employee about his preparation of data for use in computers?
(No *14*	*64+*)	J.	Interrogated any person about his use of a computer terminal?

(No) K. Investigated an alleged crime where a computer or computer program played one or more of the following roles:

(No *5* *17*) 1. object of sabotage?

(No *11* *40*) 2. object of theft?

(No *14* *42+*) 3. site of an illegal act?

(No *28* *95+*) 4. contained evidence of an illegal act?

(No *19* *50+*) 5. produced output material in an illegal act?

(No *24* *52+*) 6. used as the tool or instrument in an illegal act?

(No *5* *5+*) 7. falsely claimed use to deceive or intimidate a victim?

2. If you had evidence in a financial fraud case in the form of accounts payable records on (1) handwritten pages and (2) magnetic tape where it is available on a computer output report, in which form would you introduce it? Why?

(1) –27 (2) –4 Either (1) or (2) –7

3. A search warrant is to be prepared to search the contents of a computer and adjacent rooms for evidence of an alleged theft of a computer program. Rank the following search instruction examples from best to worst (1 best, 4 worst) by circling the appropriate digit in each example. (If none of these appeal to you, you are welcome to suggest a different form below).

Total Reponses = 31

(1 2 3 4) *4 17 8 0* A. Search for personal property in the form of key punch computer cards punched with the remote plotting programs, computer printout sheets with printouts of remote plotting programs, computer memory bank or other data storage devices magnetically imprinted with remote plotting computer programs, related documentation.

(1 2 3 4) *2 8 17 2* B. Search for personal property consisting of remote plotting programs and documented specifications and user documents in printed, punch card, magnetic media, or computer stored forms.

(1 2 3 4) *0 2 1 26* C. Search for personal property consisting of remote plotting programs and related documentation.

(1 2 3 4) *22 3 4 1* D. Search for personal property consisting of remote plotting programs, specifications and user documents in the form of (1) key punch computer cards, (2) reels of magnetic tape, (3) magnetic disks or packs, (4) computer printout sheets, (5) computer printout sheets you are to have produced by execution of computer output programs from the computer storage, (6) reels of magnetic tape you are to have produced by execution of computer output programs from the computer storage.

(suggested form) E. _____

_____

_____

4. We wish to determine your level of knowledge of computer technology. Please indicate whether you could explain the following concepts to a jury. (We would not expect you to know most of these).
Total Responses = 42

(Yes *27* No *15*) A. Parts of a computer (storage, processor, input, output).

(Yes *21* No *21*) B. How a computer program functions in a computer.

(Yes *7* No *34*) C. Program branch function.

(Yes *17* No *25*) D. Source and object code forms of a program.

(Yes *22* No *20*) E. Job description of a programmer analyst.

(Yes *5* No *36*) F. Distributed processing.

(Yes *9* No *33*) G. Multiprogramming.

(Yes *6* No *36*) H. DBMS

(Yes *12* No *30*) I. EFTS

(Yes *1* No *41*) J. ROM

(Yes *17* No *25*) K. On-line computer terminal protocol.

(Yes *7* No *35*) L. Computer crime methods (Trojan horse, salami, round down).

5. Have you read a book or manual on computers?

(Yes No)
26 *17*

6. Have you attended one or more seminars or courses on computers?
(Yes No)
24 *21*

7. Indicate which of the following acts you would consider to be a computer related crime.

Number Answering:

All: 1
8 or 9: 6
6 or 7: 19

Computer Related Crime (Check)		
(*11*)	A.	Theft of a computer.
(*13*)	B.	Theft of a computer terminal.
(*27*)	C.	Theft of a computer program from an office desk.
(*37*)	D.	Theft of a computer program from the storage device in a computer system.
(*41*)	E.	Welfare payment fraud by a welfare office clerk who changed the address of a deceased client to her own and reactivated the case through a computer terminal.
(*34*)	F.	Payroll fraud by a timekeeper who entered false overtime data for workers by pencil into data forms used for a computer input.
(*6*)	G.	False advertising by a dating service claiming they use a nonexistant computer to match people for dates.
(*17*)	H.	A national ring of homosexuals who legitimately buy computer time-sharing services to maintain and communicate lists of young boys transported from one member to another for immoral purposes.
(*42*)	I.	The president of a company who uses his computer to create false data about inventory levels of products.
(*24*)	J.	An accountant who engages in an accounts payable fraud not involving computers but buys computer time to use in the planning and management of his fraud.

8. Approximately how many computer related crime cases in the last 5 years

	Respondents	*Number*	
...have been reported to your office?	*40*	*244*	
...have been prosecuted by your office?	*42*	*191*	
...have resulted in conviction by plea?	*34*	*157*	...by trial? *29* *10*

9. Approximately how many fraud cases in the last 5 years that have involved data in computer readable form

...have been reported to your office?	*38*	*311+*	
...have been prosecuted by your office?	*34*	*215+*	
...have resulted in conviction by plea?	*26*	*158*	...by trial? *22* *20*

10. Have you used experts in computer technology as witnesses or consultants?

(Yes	No)
8	*34*

Witnesses? Names:_____ _____

Consultants? Names:_____ _____

Where did you seek assistance? _____

11. If you have any requests or advice concerning the Manual for Investigation and Prosecution of Computer Related Crime, please use the remainder of this page and back of this form, and mark this box ☐.

1975-1980 BIBLIOGRAPHY OF THE SRI COMPUTER ABUSE PROJECT

1975

Parker, Donn B., "Computer Abuse Assessment," SRI Report and *Encyclopedia of Computer Science and Techology*, 22 pp (Marcel Dekker, New York).

Parker, Donn B., "Computer Abuse Perpetrators and Vulnerabilities of Computer Systems," SRI Report and *AFIPS Conference Proceedings, 1976 National Computer Conference*, 18 pp.

1976

Nycum, Susan H., "The Criminal Law Aspects of Computer Abuse: Federal Criminal Code," 26 pp, SRI International, Menlo Park, California.

Nycum, Susan H., "The Criminal Law Aspects of Computer Abuse: State Penal Laws," 35 pp, SRI International, Menlo Park, California.

"Criminal Sanctions Under the Privacy Act of 1974," 20 pp, SRI International, Menlo Park, California.

"Testimony of Donn B. Parker for the U.S. National Commission on Electronic Fund Transfers," 24 pp, SRI International, Menlo Park, California.

Nycum, Susan H. "Legal Protection of Proprietary Rights in Software," 129 pp, SRI International, Menlo Park, California.

1978

Parker, Donn B. and Russell Dewey, "EFTS, A Guide to EDP and EFT Security Based on Occupations," 81 pp, report for Federal Deposit Insurance Corporation, SRI International, Menlo Park, California.

Parker, Donn B. and Susan H. Nycum, "Programmer Criminality," 27 pp, SRI International, Menlo Park, California.

Parker, Donn B. and Susan H. Nycum, "Computer Crimes: Case Histories and Proposed Legislation," *Proceedings of the DHEW Secretary's Conference on Fraud, Error, and Abuse*, 24 pp.

Nycum, Susan H., "Trade Secret Protection for Proprietary Interests in Software," *AFIPS Personal Computing Digest, 1978 National Computer Conference Proceedings*, 3 pp.

Parker, Donn B., "Computer Security Differences for Accidental and Intentionally Caused Losses," *AFIPS Conference Proceedings, 1978 National Computer Conference*, 5 pp.

"Testimony of Donn B. Parker and Susan H. Nycum for the U.S. Senate Subcommittee on Criminal Law," 29 pp, Federal Computer Systems Protection Act Hearings before the Subcommittee on Criminal Law and Procedures of the Committee of the Judiciary U.S. Senate, June 21, 22, 1978.

Parker, Donn B., "New Approaches to EDP Security," *American Bankers Association Automation Conference Proceedings* (May 1978).

Parker, Donn B., and J. Don Madden, "ADP Occupational Vulnerabilities," 39 pp, SRI International, Menlo Park, California.

Parker, Donn B., "Computer Misuse," 3 pp, *Information Privacy* (IPC Science and Technology Press, London, November 1978).
Parker, Donn B., "Ethics and Computers," 3 pp, *Information Privacy* (IPC Science and Technology Press, London, September 1978).
Parker, Donn B., "Computer Crime Can Spell Doomsday," 1 p, *Los Angeles Times*, January 10, 1978.

1979

Parker, Donn B., "Computer-Related Management Misdeeds," 9 pp in Robert K. Elliott and John J. Wellingham, *Management Fraud: Detection and Deterrence* (Petrocelli Books, Inc.).
Parker, Donn B., *Ethical Conflicts in Computer Science and Technology*, 277 pp (AFIPS Press, New Jersey, 1979).
Parker, Donn B., "Vulnerabilities of EFTS to Intentionally Causes Losses," 20 pp, *ACM Communication*, December 1979, pp 654-660, Association for Computing Machinery.
Parker, Donn B., "The Race To Prevent Major Computer Attack," 17 pp, *Reader's Digest* (to be published).
Parker, Donn B., "Computer Abuse in White Collar Crime," *Sage Criminal Justice Systems Annuals*, Vol. 13, Gilbert Geis, Ezra Stotland, Editors.
Nycum, Susan H., "Security in EFTS," 25 pp, *University of San Francisco Law Review* (to be published).
Nycum, Sysan H., "Liability for Malfunctioning Computer Programs," 30 pp, *Rutgers Journal of Computers and Law* (to be published).
Nycum, Susan H., "Product Liability Exposure for Computer Programs," to be prepared for *Trial*, Monthly Journal of the American Academy of Trial Lawyers.
"Computer Abuse Assessment and Control Study," SRI Final Report under NSF Grant MCS7601242, SRI International, Menlo Park, California (March, 1979).
"Computer Crime," Criminal Justice Brochure for Executives, U.S. Department of Justice LEAA, 17 pp, 1979.
"Criminal Justice Resource Manual on Computer Crime," U.S. Department of Justice LEAA, 438 pp (1979).