If you have issues viewing or accessing this file contact us at NCJRS.gov.

153234

FEDERAL COMPUTER SYSTEMS PROTECTION ACT

HEARING

BEFORE THE

SUBCOMMITTEE ON
CIVIL AND CONSTITUTIONAL RIGHTS

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

NINETY-SEVENTH CONGRESS

SECOND SESSION

ON

H.R. 3970

FEDERAL COMPUTER SYSTEMS PROTECTION ACT

SEPTEMBER 23, 1982

Serial No. 109

NCJRS

MAR 8 1995

ACQUISITIONS

U.S. DEPT. OF JUSTICE
JUL 24 1984
MAIN LIBRARY

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
11-290 O WASHINGTON : 1984

COMMITTEE ON THE JUDICIARY

PETER W. RODINO, JR., New Jersey, *Chairman*

JACK BROOKS, Texas
ROBERT W. KASTENMEIER, Wisconsin
DON EDWARDS, California
JOHN CONYERS, JR., Michigan
JOHN F. SEIBERLING, Ohio
GEORGE E. DANIELSON, California
ROMANO L. MAZZOLI, Kentucky
WILLIAM J. HUGHES, New Jersey
SAM B. HALL, JR., Texas
MIKE SYNAR, Oklahoma
PATRICIA SCHROEDER, Colorado
BILLY LEE EVANS, Georgia
DAN GLICKMAN, Kansas
HAROLD WASHINGTON, Illinois
BARNEY FRANK, Massachusetts

ROBERT McCLORY, Illinois
TOM RAILSBACK, Illinois
HAMILTON FISH, JR., New York
M. CALDWELL BUTLER, Virginia
CARLOS J. MOORHEAD, California
HENRY J. HYDE, Illinois
THOMAS N. KINDNESS, Ohio
HAROLD S. SAWYER, Michigan
DAN LUNGREN, California
F. JAMES SENSENBRENNER, JR., Wisconsin
BILL McCOLLUM, Florida

ALAN A. PARKER, *General Counsel*
GARNER J. CLINE, *Staff Director*
FRANKLIN G. POLK, *Associate Counsel*

SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS

DON EDWARDS, California, *Chairman*

ROBERT W. KASTENMEIER, Wisconsin
PATRICIA SCHROEDER, Colorado
HAROLD WASHINGTON, Illinois

HENRY J. HYDE, Illinois
F. JAMES SENSENBRENNER, JR., Wisconsin
DAN LUNGREN, California

CATHERINE A. LEROY, *Counsel*
THOMAS M. BOYD, *Associate Counsel*

153234

U.S. Department of Justice
National Institute of Justice

This document has been reproduced exactly as received from the person or organization originating it. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official position or policies of the National Institute of Justice.

Permission to reproduce this [redacted] material has been granted by
Public Domain
U.S. House of Representatives

to the National Criminal Justice Reference Service (NCJRS).

Further reproduction outside of the NCJRS system requires permission of the [redacted] owner.

CONTENTS

WITNESSES

ADDITIONAL MATERIAL

APPENDIX

FEDERAL COMPUTER SYSTEMS PROTECTION ACT OF 1981

THURSDAY, SEPTEMBER 23, 1982

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CIVIL AND CONSTITUTIONAL RIGHTS
OF THE COMMITTEE ON THE JUDICIARY,
Washington, D.C.

The subcommittee met, pursuant to call, at 9:35 a.m., in room 2237, Rayburn House Office Building, Hon. Don Edwards (chairman of the subcommittee) presiding.

Present: Representative Edwards.

Also present: Representative Nelson.

Staff present: Catherine A. LeRoy, chief counsel, and Thomas M. Boyd, associate counsel.

Mr. EDWARDS. The subcommittee will come to order.

The subject of today's hearing is computer-related crime. There is legislation pending in the subcommittee on this subject, H.R. 3970, sponsored by our distinguished colleague from Florida, Congressman Bill Nelson, who I am honored to have here today.

Congressman Nelson is also the author of the Florida State statute on computer crime, enacted when he was a member of the Florida State Legislature.

As the use of computers expands in our society, the opportunity to use computers to enage in or assist in criminal activities also expands. In response to this perceived problem, a number of States has enacted legislation specifically aimed at computer fraud. The Federal Bureau of Investigation offers its agents specialized training in computer fraud. Private industry is attempting to enhance the security of its computer facilities.

In addition, various Federal agencies are responsible for overseeing the creation and maintenance of adequate security for the Federal Government's own farflung systems. Their success—or lack of it—has been discussed and criticized in a series of Government reports, including a GAO report published in April of this year.

Although this subcommittee has been involved in a number of computer-related issues, including the exchange of computerized criminal justice information and the future direction of the FBI's NCIC system, the subject of the use of computers in the furtherance of criminal activity is a new one for us.

Accordingly, the purpose of this hearing is primarily educational. The witnesses have been asked to provide the subcommittee with information on the scope and nature of the problem, the existing tools or mechanisms used to deal with the problem, the adequacy

of those mechanisms, the need for additional tools or resources, and the like.

Before I introduce the witnesses I welcome on behalf of the subcommittee Congressman Bill Nelson. Do you have a statement, Mr. Nelson?

Mr. NELSON. Mr. Chairman, I thank you for this opportunity to explore this subject. I look forward to it as an educational opportunity to identify the problem, and to see what needs to be done about the problem, and I thank you for granting the opportunity of these hearings.

Mr. EDWARDS. Thank you.

Our first witnesses are representatives from the Department of Justice: Mr. Roger Olsen, Deputy Assistant Attorney General in the Criminal Division, and from the FBI, Floyd Clarke, Deputy Assistant Director in charge of the Criminal Investigation Division, and William A. Bayse, Assistant Director in charge of the Technical Services Division.

You may proceed.

Mr. NELSON. Mr. Chairman, I ask unanimous consent that the subcommittee permit the hearing, in whole or in part, to be covered this morning by television broadcasting, radio broadcasting by this still photography.

Mr. EDWARDS. Without objection, it is so ordered.

TESTIMONY OF ROGER M. OLSEN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE; FLOYD CLARKE, DEPUTY ASSISTANT DIRECTOR, CRIMINAL INVESTIGATIVE DIVISION, FEDERAL BUREAU OF INVESTIGATION; AND WILLIAM A. BAYSE, ASSISTANT DIRECTOR, TECHNICAL SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. OLSEN. Thank you, Mr. Chairman, I am pleased to be here representing the Department of Justice in order to respond to questions concerning the Department's views on computer-related crimes. All of us are aware of the constant and pervasive impact computers now make on our daily lives. In fact, their use in transactions of every description is so commonplace that even measuring the extent of their use, and the comparable potential for criminal misuse, is very difficult.

Nevertheless, in July of this year the Justice Department's Bureau of Justice Statistics published a report entitled "Electronic Fund Transfer Systems and Crime."

The authors suggested that by 1985 computer terminals either for electronic funds transfer or check verification will be used in at least 10 percent of all point-of-sale transactions such as those in stores and restaurants that there may be as many as 400 million computer-controlled automated teller machine transactions every month; and that the monthly volume of activity in computerized telephone bill paying accounts could be in excess of $50 million.

While these figures represent estimates, they strongly suggest a new vast potential for fraud and other criminal conduct.

The report is also significant for its discussion of the difficulty in defining and measuring the extent of computer crime. For exam-

ple, in describing the role of computers in electronic funds transfers or EFT's, the report noted that usually traditional legal descriptions of crime, for example, fraud or theft, can be used to describe EFT crime but such a term reveals little about how the computer was involved in the offense.

Moreover, while new classification systems could be developed based on the role of the computer in the crime, the report noted that there is little consensus as to what such classifications should be.

Thus, the report's authors decided that "any crime, whether prosecuted or not under traditional or special computer/EFT laws, that would not have occurred but for the presence of an EFT system is considered an EFT crime.

"A review of these and other sources led to the conclusion that there is no valid data for measuring and understanding the nature and extent of EFT crime."

Nevertheless, the sheer magnitude and dollar volume of the transactions handled by computers has caused significant discussion in the law enforcement community and in the data processing industry about computer security and the use or abuse of computers to perpetrate crime.

The Congress has also expressed an interest in devising a statute designed to safeguard the integrity of computer operations.

A bill to accomplish this, S. 240 was introduced by former Senator Ribicoff in the 96th Congress.

While the Department of Justice took an active role in helping to make this statute effective from the criminal prosecutor's standpoint, this administration does not endorse that particular bill.

At present, as you are aware, there is no sanction available specifically dealing with computer-related crime. Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" which somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets.

The crafting of such a theory can be awkward, and the results far from perfect. Even if a theory is devised which apparently covers the illegal acts, it still must be treated as an untested, untried basis of prosecution in the trial court. This can lead to the dismissal of a prosecution, notwithstanding the egregious nature of the crime or the extensiveness of trial preparation, because decades old statutory elements designed to deal with other crimes have been stretched too far to accommodate modern criminality.

The potential magnitude of the harm that could be done by misuse of a computer suggests that there is merit in legislation that would directly address computer crime, and the power to regulate commerce and the power of the Federal Government to punish crimes where the Government is itself the victim would provide a constitutional basis for such a stature.

A limited approach would be to reach computer crime involving Federal Government-owned computers, and those of financial institutions insured by the United States; if a broader approach were to

be favored, the statute could be expanded to reach computers operating in or affecting interstate commerce.

The types of conduct that would be proscribed would include: One, fraud in the use of a computer—where the computer is the vehicle much as the mails and wire communication are the vehicles in the mail and fraud statutes; two, theft of property, services or money through the use of or in the illegal access to these computers; and three, the illegal use, damage or destruction of such computers.

In our rendering assistance in the drafting of the Ribicoff bill to address these activities, classical fraud language was incorporated in order to suggest reliance on existing legal interpretations of mail and wire fraud cases.

This was done to assure that the computer fraud statute would have solid legal underpinning in serving to cover virtually any type of bogus scheme using the designated computers.

Further, an illegal access, damage, and destruction clause was incorporated because of the unusual nature and remarkable quantity and quality of harm a single unauthorized access or destructive act can wreak when a significant computer or system is the target.

As I indicated previously, statistics detailing the extent of computer crime are simply not available and, consequently, I cannot, in all candor, represent that legislation in this area is clearly needed.

Notwithstanding, the experience of law enforcement in the various instances of computer-related crime that have by their size or nature drawn notice, suggests that we may fail ourselves by not being forearmed with an appropriately drafted statute.

Two well-known examples present themselves. The Seidlitz case, tried in the district of Maryland, and the Rivkin case in the California State court system are examples of computer-related crime which, if perpetrated in a slightly different manner, might well have escaped even the possibility of Federal prosecution.

In Seidlitz, the owner of a computer company stole confidential software by tapping into the computer system of a previous employer from his own remote terminal. Had the defendant not made 2 of the 50 access calls across State lines, there would have been no basis whatsoever for Federal prosecution; only a statute on theft of trade secrets would have remained as a possible recourse.

In Rivkin, a computer expert fraudulently used a bank's in-house access codes to transfer millions of dollars to accounts he controlled in another bank.

If Federal jurisdiction had been sought and the wire communication transferring the funds had all been within the same State, we would have been hard-pressed to prosecute.

Such instances in which the use of interstate facilities is avoided by the perpetrator would leave Federal law enforcement without an appropriate weapon and effectively foreclosed from addressing what might be properly perceived as an area of significant Federal interest.

I might point out that in considering the question of appropriate Federal legislation we should at all times keep in mind the fact that those people who are most likely to be perpetrating these sophisticated fraud offenses are also the ones who are most knowl-

edgeable about how to avoid the applicable Federal statutes so that it is not going to be simply an inadvertent case but rather that those people who are going to be gaining millions of dollars from fraud would also be the same ones who would be more likely than not to be escaping present existing Federal statutes.

With that in mind I would like to invite the committee's attention to Mr. Clarke and to Mr. Bayse of the FBI who will address this matter from the investigative perspective.

[The prepared statement of Mr. Olsen follows:]

PREPARED STATEMENT OF ROGER M. OLSEN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION

I am pleased to be here today representing the Department of Justice in order to respond to questions concerning the Department's views on computer-related crime. With me representing the FBI are Floyd Clarke, Deputy Assistant Director, Criminal Investigative Division, and William A. Bayse, Assistant Director, Technical Services Division.

All of us are aware of the constant and pervasive impact computers now make on our daily lives. In fact, their use in transactions of every description is so commonplace that even measuring the extent of their use, and the comparable potential for criminal misuse, is very difficult. Nevertheless, in July of this year the Justice Department's Bureau of Justice Statistics published a report entitled "Electronic Fund Transfer Systems and Crime." The authors suggested that by 1985 computer terminals either for electronic funds transfer to check verification will be used in at least ten percent of all point of sale transactions such as those in stores and restaurants; that there may be as many as 400 million computer controlled automated teller machine transactions every month; and that the monthly volume of activity is computerized telephone bill-paying accounts could be in excess of $50 million. While these figures represent estimates, they strongly suggest a new vast potential for fraud and other criminal conduct.

The report is also significant for its discussion of the difficulty in defining and measuring the extent of computer crime. For example, in describing the role of computers in electronic funds transfers or EFT's, the report noted that usually traditional legal descriptions of crime—e.g. fraud or theft—can be used to describe EFT crime but such a term reveals little about how the computer was involved in the offense. Moreover, while new classification systems could be developed based on the role of the computer in the crime, the report noted that there is little consensus as to what such classifications should be. Thus, the report's authors decided that "any crime, whether prosecuted or not under traditional or special computer/EFT laws, that would not have occurred *but for* the presence of an EFT system is considered an EFT crime.

A review of these and other sources led to the conclusion that there is no "valid data for measuring and understanding the nature and extent of EFT crime.

Nevertheless, the sheer magnitude and dollar volume of the transactions handled by computers has caused significant discussion in the law enforcement community and in the data processing industry about computer security and the use or abuse of computers to perpetrate crime. The Congress has also expressed an interest in devising a statute designed to safeguard the integrity of computer operations. A bill to accomplish this S. 240 was introduced by former Senator Ribicoff in the 96th Congress. While the Department of Justice took an active role in helping to make this statute effective from the criminal prosecutor's standpoint, this administration does not endorse that particular bill.

At present, as you are aware, there is no sanction available specifically dealing with computer-related crime. Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of presecution" which somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets. The crafting of such a theory can be awkward, and the results far from perfect. Even if a theory is devised which apparently covers the illegal acts, it still must be treated as an untested, untried basis of prosecution in the trial court. This can lead to the dismissal of a prosecution, notwithstanding the egregious nature of the crime or the extensiveness of trial preparation, because decades old statutory elements de-

signed to deal with other crimes have been stretched too far to accommodate modern criminality. The potential magnitude of the harm that could be done by misuse of a computer suggests that there is merit in legislation that would directly address computer crime, and the power to regulate commerce and the power of the federal government to punish crimes where the government is itself the victim would provide a constitutional basis for such a statute.

A limited approach would be to reach computer crime involving federal government-owned computers, and those of financial institutions insured by the United States; if a broader approach were to be favored, the statute could be expanded to reach computers operating in or affecting interstate commerce. The types of conduct that would be proscribed would include: (1) fraud in the use of a computer (where the computer is the vehicle much as the mails and wire communication are the vehicles in the mail and wire fraud statutes); (2) theft of property, services or money through the use of or in the illegal access to these computers; and (3) the illegal use, damage or destruction of such computers.

In our rendering assistance in the drafting of the Ribicoff bill to address these activities, classical fraud language was incorporated in order to suggest reliance on existing legal interpretations of mail and wire fraud cases. This was done to assure that the computer fraud statute would have solid legal underpinnings in serving to cover virtually any type of bogus scheme using the designated computers. Further, an illegal access, damage, and destruction clause was incorporated because of the unusual nature and remarkable quantity and quality of harm a single unauthorized access or destructive act can wreak when a significant computer or system is the target.

As I indicated previously, statistics detailing the extent of computer crime are simply not available and consequently, I cannot, in all candor, represent that legislation in this area is clearly needed. Notwithstanding, the experience of law enforcement in the various instances of computer-related crime that have by their size or nature drawn notice, suggests that we may fail ourselves by not being forearmed with a appropriately drafted statute. Two well known examples present themselves. The Seidlitz case, tried in the District of Maryland, and the Rivkin case in the California state court system are examples of computer-related crime which, if perpetrated in a slightly different manner, might well have escaped even the possibility of federal prosecution.

In Seidlitz, the owner of a computer company stole confidential software by tapping into the computer system of a previous employer from his own remote terminal. Had the defendant not made two of the fifty access calls across state lines, there would have been no basis whatsoever for federal prosecution; only a statute on theft of trade secrets would have remained as a possible recourse.

In Rivkin, a computer expert fraudulently used a bank's in-house access codes to transfer millions of dollars to accounts he controlled in another bank. If federal jurisdiction had been sought and the wire communication transferring the funds had all been within the same state, we would have been hard-pressed to prosecute.

Such instances in which the use of interstate facilities is avoided by the perpetrator would leave federal law enforcement without an appropriate weapon and effectively foreclosed from addressing what might be properly perceived as an area of significant federal interest.

Mr. EDWARDS. Thank you very much, Mr. Olsen.

Mr. Clarke.

Mr. CLARKE. Mr. Chairman and Congressman Nelson, I appreciate the opportunity to appear before the subcommittee today to discuss computer-related crime and the investigative role of the FBI regarding this type of criminal activity.

Computers are frequently used in the commission of white-collar crimes. The role of a computer in furtherance of an illegal scheme varies with the motive and intent of the perpetrator.

Some examples of the varied ways computers are involved include: The occasional use of computers to create an illusion of legitimacy, for instance, to produce output in a fraudulent investment scheme; the use of computers as a tool in illegal businesses, such as, bookmakers and drug dealers to maintain fiscal and/or inventory records; and in actual criminal acts like a gun in a homicide.

Examples of the latter and most common occurrence include the use of a computer to: Gain access to communications networks and, thereafter, steal information from someone else's computer; and placing a subroutine in an existing program to divert funds to another account or inflate billing charges.

Banking institutions are especially vulnerable to this form of computer-related crime since many employees of banking institutions use computer terminals in the normal course of business. Tellers could juggle deposits or shift money from dormant accounts to their own and managers could create fictitious loan accounts or investments.

In these cases, the computer system is either directly or indirectly involved in the conversion of something of value. The methods used by criminals of today have changed substantially with the increased reliance on computer systems in our society.

This has been and will continue to be especially true where fraud, deceit, and embezzlement are involved since the schemes are being continuously modified to fit our changing environment.

The investigator, to be successful, has had to anticipate and adjust to environmentally imposed changes in criminal methodology. The advent of automation is no exception to this rule and the FBI has taken steps to prepare for computer-related crime investigations.

Since 1976, the FBI has conducted a 3- to 4-week training course which has been attended by 166 FBI agents and 83 non-FBI law enforcement officers.

This course requires no prior knowledge of computers, yet, at the conclusion of the training all students are able to operate and program a computer. Students access a data base consisting of records which would be found in a real banking environment and are involved in the execution of a mock search warrant. This course is currently scheduled three times each year.

The FBI has also provided a 1-week condensed version of the above-described course to 203 non-FBI personnel at the FBI Academy and an additional 568 law enforcement officers have been trained onsite at 22 schools. These road schools are conducted three to six times each year.

The Training Divison of the FBI is currently in the process of obtaining a state-of-the-art system to supplement the current training that is provided.

To augment the trained agent force assigned throughout the United States, as the needs arise, our Technical Services Division provides telephonic or onsite technical assistance and conducts complex analyses of seized magnetic media evidence on the FBI's computer equipment.

Another facet of computer-related crime involves Federal jurisdiction. This is true irrespective of the violation or the method involved. The authority on issues of jurisdiction is the Department of Justice and the U.S. attorneys' offices.

Therefore, when information is received regarding a possible violation, including those that are computer-related, all jurisdictional questions are decided through consultation with the Department of Justice and/or the appropriate U.S. attorney.

Evaluations are made as to the appropriate statute vis-a-vis the violation and the prospective merits of the particular case.

The FBI is often asked to statistically summarize its computer-related crime investigations. This has not been possible, since the FBI collects only certain management-oriented statistics on its investigative activities on a statute-by-statute basis. In the absence of a computer crime statute these investigations are categorized or classified according to the statute that will most probably be utilized in the prosecution.

Therefore, no system nor facility exists which differentiates between computer-related and noncomputer-related crimes.

Informal discussions and surveys of white-collar crime squad supervisors in our 59 field offices yielded a conservative estimate that less than 100 cases involving computers were opened between April 1, 1981, and March 31, 1982.

It might be argued by some experts that this figure supports a popular theory that less than 20 percent of the detected computer-related crimes are reported. These same experts may well argue that the apparent aversion to reporting computer-related crimes is an underlying problem facing the investigator.

We have observed that the traditional approach of using informants and sources is relatively ineffective in developing information to initiate investigations of computer-related crimes. We rely on referrals and the reporting of possible violations in the computer area.

The FBI's in-house seminars with our experienced investigators, discussions with academic and private-sector experts on computer-related crimes, and informal internal surveys, provide a means to evaluate our own effectiveness and ability to successfully meet the challenges of investigating computer-related crimes.

We find that, given the current reporting environment, we are fully capable of meeting these challenges effectively and efficiently; however, we believe the criminal justice system would be better served by appropriately drafted Federal computer crime legislation.

Thank you.

[The prepared statement of Mr. Clarke follows:]

STATEMENT OF DEPUTY ASSISTANT DIRECTOR FLOYD CLARKE

I appreciate the opportunity to appear before the Subcommittee today to discuss computer-related crime and the investigative role of the FBI regarding this type of criminal activity.

Computers are frequently used in the commission of White Collar Crimes. The role of a computer in furtherance of an illegal scheme varies with the motive and intent of the perpetrator. Some examples of the varied ways computers are involved include: The occasional use of computers to create an illusion of legitimacy, for instance, to produce output in a fraudulent investment scheme; the use of computers as a tool in illegal businesses, such as, bookies and drug dealers to maintain fiscal and/or inventory records; and in actual criminal acts like a gun in a homicide.

Examples of the latter and most common occurrence include the use of a computer to: gain access to communications networks, and, thereafter, steal information from someone else's computer; and placing a subroutine in a existing program to divert funds to another account or inflate billing charges.

Banking institutions are especially vulnerable to this form of computer-related crime since many employees of banking institutions use computer terminals in the normal course of business. Tellers could juggle deposits or shift money from dormant accounts to their own and managers could create fictitious loan accounts or investments.

In these cases, the computer system is either directly or indirectly involved in the conversion of something of value. The methods used by criminals of today have changed substantially with the increased reliance on computer systems in our society. This has been and will continue to be especially true where fraud, deceit, and embezzlement are involved since the schemes are being continuously modified to fit our changing environment.

The investigator, to be successful, has had to anticipate and adjust to environmentally imposed changes in criminal methodology. The advent of automation is no exception to this rule and the FBI has taken positive steps to prepare for computer-related crime investigations.

Since 1976, the FBI has conducted a three to four-week training course which has been attended by 166 FBI Agents and 83 non-FBI law enforcement officers. This course requires no prior knowledge of computers, yet, at the conclusion of the training all students are able to operate and program a computer. Students access a data base consisting of records which would be found in a real banking environment and are involved in the execution of a mock search warrant. This course is currently scheduled three times each year.

The FBI has also provided a one-week condensed version of the above-described course to 203 non-FBI personnel at the FBI Academy and an additional 568 law enforcement officers have been trained on-site at 22 schools. These road schools are conducted three to six times each year.

The Training Division of the FBI is currently in the process of obtaining a state-of-the-art computer system to supplement the current training that is provided.

To augment the trained Agent force assigned throughout the United States, as the needs arise, our Technical Services Division provides telephonic or on-site technical assistance and conducts complex analyses of seized magnetic media evidence on the FBI's computer equipment.

Another facet of computer-related crime involves federal jurisdiction. This is true irrespective of the violation or the method involved. The authority on issues of jurisdiction is the Department of Justice and U.S. Attorneys offices. Therefore, when information is received regarding a possible violation, including those that are computer-related all jurisdictional questions are decided through consultation with the Department of Justice and/or the appropriate U.S. Attorney. Evaluations are made as to the appropriate statute vis-a-vis the violation and the prosecutive merits of the particular case.

The FBI is often asked to statistically summarize its computer-related crime investigations. This has not been possible, since the FBI collects only certain management-oriented statistics on its investigative activities on a statute-by-statute basis. In the absence of a computer crime statute these investigations are categorized or classified according to the statute that will most probably be utilized in the prosecution. Therefore, no system nor facility exists which differentiates between computer-related and non-computer-related crimes.

Informal discussions and surveys of white-collar crime squad supervisors in our 59 field offices yielded a conservative estimate that less than 100 cases involving computers were opened between April 1, 1981 and March 31, 1982. It might be argued by some experts that this figure supports a popular theory that less than 20 percent of the detected computer-related crimes are reported. These same experts may well argue that the apparent aversion to reporting computer-related crimes is an underlying problem facing the investigator. We have observed that the traditional approach of using informants and sources is relatively ineffective in developing information to initiate investigations of computer-related crimes. We rely on referrals and the reporting of possible violations in the computer area.

The FBI's in-house seminars with our experienced investigators, discussions with academic and private sector experts on computer-related crimes, and informal internal surveys, provide a means to evaluate our own effectiveness and ability to successfully meet the challenges of investigating computer-related crimes. We find that given the current reporting environment we are fully capable of meeting these challenges effectively and efficiently; however, we believe the criminal justice system would be better served by appropriately drafted federal computer crime legislation.

Mr. EDWARDS. Thank you very much, Mr. Clarke.

The FBI deserves a compliment for staying up to date on this and moving on your own like you have. That is very good.

Mr. CLARKE. Thank you, Mr. Chairman.

Mr. EDWARDS. Mr. Bayse.

Mr. BAYSE. Mr. Chairman and Congressman Nelson, I appreciate the opportunity to appear before you today to discuss the prospect of Federal legislation concerning computer-related crime.

As you are aware, the subject of computer crime is complex and controversial—surrounded by diverse views on amount, types, motivation, and financial impacts related to criminal acts directly involving computers.

While recognizing the divergence of views and capacity of statistical data associated with computer-related crimes, our analyses lead to the conclusion that Federal computer crime legislation is appropriate and necessary for current and future criminal justice purposes.

In this regard, Federal legislation in this important area is supportable for the following reasons:

Computer-related crimes possess unique properties which distinguish them from conventional crimes. In a 1976 report to the Congress, the General Accounting Office indicated specifically that computer systems have added a new dimension for potential crime.

Information—such as corporate trade secrets—has become a valuable commodity which is being managed by computer-based systems like other key resources, and has been the target of computer-related criminal activity.

As automation technology continues rapidly to advance, the new kind of crimes we are facing will come more clearly into focus.

However, at this time there are approximately 40 statutes which may be applied to crimes involving computers. A single Federal statute would work in favor of the criminal justice system by making clear the substantive violation being cited.

Several FBI practitioners have expressed the need for a Federal statute which goes to the heart of the issue of computer-related crime and cuts away unnecessary, costly legal problems associated with application of current laws.

For example, if a computer is a clearly identified instrumentality of a crime, it is inefficient and sometimes ineffective to adapt an existing theft or fraud statute, for example, interstate transportation of stolen property or fraud by wire, for a substantive violation.

Among current statutes applicable to computer-related crime, penalties are variable. It is plausible that the higher penalties in previous versions of proposed computer-related crime Federal legislation would have a deterrent effect in this area.

This is an important consideration in light of a recent General Accounting Office [GAO] report highlighting vulnerability of Federal information systems to fraudulent, wasteful, abusive, and illegal practices. We reference here GAO Report MASAD-82-18 published April 21, 1982.

One of the findings of the GAO study is that increased vulnerability occurs as investment rises in automated information systems in Federal executive agencies. These agencies and their computers are entities to be covered under provisions of any proposed legislation. With projected increases in Federal automation, this aspect of the legislation becomes commensurately important.

Technology trends are clear and suggest the need for Federal legislation. Industry and Government projections indicate that in this decade the United States, and other countries, will experience a

proliferation of telecommunications networks supporting interconnected multicomputer complexes.

These computer/network configurations represent a trend toward distributed information processing and distributed data bases spanning large geographic regions in support of organizational functions.

Increased access to such decentralized information systems is on the upswing with terminal access points increasingly available for executives, officeworkers, and others throughout geographically dispersed organizations nationwide.

These trends tend to accentuate the vulnerabilities pointed out in the previously cited General Accounting Office report and to point up the national scope of the computer-related crime issue.

Another clear trend is the growth of personal computers or home computers projected at about 5 million by 1985. Such devices can stand alone or be connected to telecommunications networks. We are seeing this latter type of computer being used directly to support gambling, narcotics, racketeering, and theft.

There are significant efforts to improve security and integrity in Government information systems. Security, privacy, and integrity controls, and auditability are emphasized and mandated in recent Federal legislation and regulations.

These positive efforts represent congressional and Federal executive management initiatives which would be compatible with and complemented by appropriately drafted Federal computer crime legislation.

Having reviewed many of the criticisms aimed at the original bill proposed by Senator Ribicoff, there appear to be some valid and beneficial observations; however, a substantial amount of criticism lacked specific focus or any apparent constructive motive.

Significantly, many of the previous criticisms overlooked the basic elasticity/flexibility of the judicial process. The courts will address and set out specific interpretations of the Federal law. None of this prior criticism should serve as a major impediment to soundly structured Federal legislation.

An issue which is relevant to a need assessment for Federal legislation is that of reporting. Consistent, accurate reporting of occurrences of computer-related crime is essential to planning, resource management, research, and investigative effectiveness.

It is suggested that reporting requirements be reviewed in formulation of Federal legislation.

These remarks have been set forth to discuss the need for Federal legislation. In this regard, proposed legislation can benefit from continuing review, clarification, and selected modification.

That concludes my remarks, Mr. Chairman.

[The prepared statement of Mr. Bayse follows:]

STATEMENT OF ASSISTANT DIRECTOR WILLIAM A. BAYSE, FEDERAL BUREAU OF INVESTIGATION

I appreciate the opportunity to appear before you today to discuss the prospect of Federal legislation concerning computer-related crime. As you are aware, the subject of computer crime is complex and controversial—surrounded by diverse views on amount, types, motivations, and financial impacts related to criminal acts directly involving computers.

While recognizing the divergence of views and scarcity of statistical data associated with computer-related crimes, our analyses lead to the conclusion that Federal computer crime legislation is appropriate and necessary for current and future criminal justice purposes.

In this regard, Federal legislation in this important area is supportable for the following reasons:

Computer-related crimes possess unique properties which distinguish them from conventional crimes. In a 1976 report to the Congress, the General Accounting Office indicated specifically that computer systems have added a new dimension for potential crime. Information (such as corporate trade secrets) has become a valuable commodity which is being managed by computer-based systems like other key resources, and has been the target of computer-related criminal activity. As automation technology continues rapidly to advance, the new kind of crimes we are facing will come more clearly into focus. However, at this time there are approximately forty statutes which may be applied to crimes involving computers. A single Federal statute would work in favor of the criminal justice system by making clear the substantive violation being cited. Several FBI practitioners have expressed the need for a Federal statute which goes to the heart of the issue of computer-related crime and cuts away unnecessary, costly legal problems associated with application of current laws. For example, if a computer is a clearly identified instrumentality of a crime, it is inefficient and sometimes ineffective to adapt an existing theft or fraud statute (e.g., interstate transportation of stolen property or fraud by wire) for a substantive violation.

Among current statutes applicable to computer-related crime, penalties are variable. It is plausible that the higher penalties in previous versions of proposed computer-related crime Federal legislation would have a deterrent effect in this area. This is an important consideration in light of a recent General Accounting Office (GAO) report highlighting vulnerability of Federal information systems to fraudulent, wasteful, abusive and illegal practices. We reference here GAO Report MASAD-82-18, published April 21, 1982. One of the findings of the GAO study is that increased vulnerability occurs as investment rises in automated information systems in Federal executive agencies. These agencies and their computers are entities to be covered under provisions of any proposed legislation. With projected increases in Federal automation, this aspect of the legislation becomes commensurately important.

Technology trends are clear and suggest the need for Federal legislation. Industry and Government projections indicate that in this decade the United States (and other countries) will experience a proliferation of telecommunications networks supporting interconnected multicomputer complexes. These computer/network configurations represent a trend toward distributed information processing and distributed data bases spanning large geographic regions in support of organizational functions. Increased access to such decentralized information systems is on the upswing with terminal access points increasingly available for executive, office workers, and others throughout geographically dispersed organizations nationwide. These trends tend to accentuate the vulnerabilities pointed out in the previously cited General Accounting Office report and to point up the national scope of the computer-related crime issue. Another clear trend is the growth of personal computers or home computers projected at about 5 million by 1985. Such devices can stand alone or be connected to telecommunications networks. We are seeing this latter type of computer being used directly to support gambling, narcotics, racketeering, and theft.

There are significant efforts to improve security and integrity in Government information systems. Security, privacy, and integrity controls and auditability are emphasized and mandated in recent Federal legislation and regulations. These positive efforts represent congressional and Federal executive management initiatives which would be compatible with and complemented by appropriately drafted Federal computer crime legislation.

Having reviewed many of the criticisms aimed at the original bill proposed by Senator Ribicoff, there appear to be some valid and beneficial observations; however, a substantial amount of criticism lacked specific focus or any apparent constructive motive. Significantly, many of the previous criticisms overlooked the basic elasticity/flexibility of the judicial process. The courts will address and set out specific interpretations of the Federal law. None of this prior criticism should serve as a major impediment to soundly structured Federal legislation.

An issue which is relevant to a need assessment for Federal legislation is that of reporting. Consistent, accurate reporting of occurrences of computer-related crime is essential to planning, resource management, research, and investigative effective-

ness. It is suggested that reporting requirements be reviewed in formulation of Federal legislation.

These remarks have been set forth to discuss the need for Federal legislation. In this regard, proposed legislation can benefit from continuing review, clarification, and selected modification.

Mr. EDWARDS. Thank you, Mr. Bayse, and thanks to all three of you for really very helpful testimony.

We are going to have some questions but there is a vote on the floor of the House and we will have to recess for about 10 minutes.

[Recess.]

Mr. EDWARDS. The subcommittee will come to order. We apologize to the witnesses for this delay.

Couldn't the FBI have a system without too much trouble where you could enter into a computer—and I don't know much about computers, as you will find out—when a computer was used just so that you could get a printout of the crimes that took place in which a computer was involved?

Mr. BAYSE. Yes; we could augment our reporting system so that when one of these crimes took place we could keep a file on those through the current reporting system that we have but it would take some augmentation and some extra consideration by our field supervisors and the agents to identify the specific crime and what may be even more helpful might be a synopsis of exactly what took place.

Mr. EDWARDS. Do you have that in mind?

Mr. BAYSE. I will defer to Mr. Clarke.

Mr. CLARKE. We are currently on a semiannual basis asking them in our white collar crime survey to highlight those types of crimes where a computer was used.

The problem that exists there is that we would also be missing other types of offenses that would fall outside of the white collar crime program where a computer might also have been the instrument or the target of the crime itself, for example, a fraud against the Government or destruction of Government property type of situation. So that is not all inclusive.

We are collecting some data along those lines.

Mr. EDWARDS. It seems to me that you have in the FBI and the Department of Justice, of course, some very, very sensitive information and some that must be computerized, at least indices and things. How do you protect it? How do you make sure you don't have a mole or somebody there who is accessing the computers and getting information?

Mr. BAYSE. We spent a great deal of effort and financial resources securing our information systems. One, they are all controlled in FBI space. All of our people have extensive background investigations that have access to our computer systems.

We work hard on the internal controls to protect systems such as separation of duties so that one person isn't in a critical position without having some checks and balances.

In addition, we encrypt all of the transmissions for our sensitive investigative systems from the terminal end out in our offices and we have about half of our offices on line now at the computers.

We use special access methods and some of the national security equipment to protect both access emanations and to encrypt the data transmissions.

I would say probably one-third of the cost or maybe half of our sensitive information systems goes for security, particularly in the foreign counterintelligence area.

Mr. EDWARDS. Well, you are going to be a big help in our drafting of this legislation, not in this Congress, I am sure, but we certainly hope with your assistance and with that of Mr. Nelson that if it is deemed advisable by the subcommittee and the full committee, and so forth, to have some legislation on this issue.

Mr. Nelson.

Mr. NELSON. Thank you, Mr. Chairman.

I want to address a question to Mr. Olsen concerning his statement on page 4 that because decades old-statutory elements designed to deal with other crimes have been stretched too far to accommodate modern criminality, continuing on, there is merit in legislation that would directly address computer crime.

Let me make just a prefatory statement. When I passed this similar legislation in the Florida Legislature back in 1978, I had had the prior experience in 1977 of being the chief sponsor of the RICO statute which had been in existence in the Federal Government for 10 years but which Florida had not had. One of the theories that we had in passing that statute was to bring together a specific new kind of crime so that you could go after the criminal enterprise instead of the unrelated street crime. The experience in Florida since then has been phenomenally successful under the RICO statute.

One of the criticisms, of course, that was then raised and when in 1978 we started with the computer crimes legislation was, well, what is the need for it? There are already criminal statutes through which you can prosecute.

Our feeling at the time was since it was a case of first impression—we were the first State in the country to even consider the legislation and we really didn't have any data but looking back to our experience in developing RICO, we thought that there were, in this sophisticated age of electronic gadgetry and this sophisticated age of electronic data transfer in the billions of dollars that are going back and forth on an international level which didn't apply to us in Florida at the time in our limited jurisdiction, that it just made sense, even though we didn't have any data, to try to describe a new crime which would give prosecutors more efficient and effective tools to go after.

Now, with that as a prefatory statement, could I ask do you build on your statement there on page 4?

Mr. OLSEN. Yes; I think the questions that we have from both an investigative and prosecutive standpoint involve whether or not we are going to face statutory impediments to being able to actually make a case when an actual fraud has been perpetrated. Not that we couldn't prove that there was a fraud but that we wouldn't have the sufficient trigger mechanism to justify Federal prosecution and the result is that sometimes you end up trying to develop a case to satisfy a statutory framework that was designed for other purposes.

We would find ourselves in a situation where the Bureau, for example, was expending tremendous amounts of resources on a case potentially simply to satisfy one of the mail or wire fraud statutes that we have, even though all the elements of a fraud, perhaps even of enormous magnitude, were already there.

And I think the question we are facing is really are we going to wait to find out that we have a bad experience with an enormous fraud but without adequate Federal statutory guidelines and authority to investigate and prosecute.

It is possible, for example, in this area to do that which historically has not been possible to perpetrate a fraud without actually physically moving yourself and the property but simply to do it through the computer, either through an electronic transfer or through a computer fraud itself, with the result that in one single transaction you could have millions of dollars lost, not just from trade secrets but actual transfers of money.

And one of the questions is do we have adequate safeguards in our present statutory framework. While the administration has not taken a position with respect to a specific legislative vehicle, I think it is clear from what you have heard this morning that both the Bureau and the Department of Justice view this as an area where we should actively consider a specific vehicle and to work with this committee to do so.

Mr. NELSON. When you say manipulation of a computer and transfer of enormous sums of money, you mean someone tampering with the program and siphoning off money that goes into some secret bank account someplace?

Mr. OLSEN. Yes.

Mr. NELSON. And under the existing Federal laws, are you saying that that would be difficult to prosecute?

Mr. OLSEN. I am saying it might be. It would depend on the facts and the circumstances of each case. But the problem that we are looking at is whether or not there is a pattern or trend of cases that present that type of a risk.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. EDWARDS. We thank the witnesses very much. You have been very helpful and we will see you again.

Mr. OLSEN. Thank you very much, Mr. Chairman.

Mr. EDWARDS. Our next witness is Mr. Milton Wessel, an attorney with Parker, Chapin, Flattau & Klimpl in New York.

Mr. Wessel has taught courses in computer law at a number of law schools around the country and is currently affiliated with Columbia University Law School.

And you will introduce your colleagues, please?

TESTIMONY OF MILTON R. WESSEL, ESQ., PARKER, CHAPIN, FLATTAU & KLIMPL, NEW YORK, N.Y., ACCOMPANIED BY KENNETH RYNNE AND KENNY HAYASHI

Mr. WESSEL. I would like to introduce my colleagues, Mr. Chairman.

I am delighted that you indicated at the outset that this is an educational session, because to my right is Kenny Hayashi and to my left is Ken Rynne, both of whom were students at Georgetown

Law School last semester in the computer course that I taught. Both concentrated on the computer crime area, and both produced outstanding work.

Their research is in-depth. Their understanding of the nature of the problem is excellent, from my reading of their papers and from my knowledge of them, and I know both would be delighted to respond to whatever questions the committee might have.

Mr. EDWARDS. Well, we welcome them also, Professor, and we would be grateful, of course, if the fruit of some of their labors could be made a part of the record at the appropriate time if any of the three of you think that would be appropriate.

Mr. WESSEL. I think it would be appropriate but, Mr. Chairman, the papers were prepared for their own and my views. I do not in any way question substance, nor do they. But sometimes characterization may enter the picture, which in a public forum may be inappropriate. So, I would like permission, if the committee would consent, for them to be able to edit their papers and only then submit them for publication.

Mr. EDWARDS. Well, without objection, they would be welcome for the record.

(The material referred to appears in the app. at p. 63.

Mr. WESSEL. I am also delighted that one of Congressman Gephardt's fine legislative aides is present in the hearing room.

Computer crime is an important issue in itself but it is an even more important issue, in my view, as a manifestation of the "ignorance," and I use that word advisedly, that we in our society have regarding so many aspects of "computers and society" problems.

That ignorance runs the gamut of economic problems, privacy problems, other constitutional problems, intellectual property problems, and so forth. And I would like to focus, because of this committee's inquiry today, on computer crime. But I would like to also suggest that it might well be that the committee would consider taking a more broad look at computers and society problems, with a view toward noncrisis management of an area which I think everybody would agree will soon be one of the most critical areas with which American society, and perhaps world society must deal.

Now, I know that it is a rather difficult assignment in light of what is happening in Lebanon and in South America and with banking and with so many other issues. It is very difficult to focus on a long-range problem. Yet, society somehow must deal with the kinds of issues which the information age is quickly bringing upon us.

I brought with me just a couple of examples—very current examples since I received the committee's invitation—of the kind of extravagant comment which circulates concerning computer crime, about which I say there is precious little information.

One is an ad from one of the current computer publications. It is a picture of a dagger stuck into a video terminal set, with green blood oozing out. Obviously an effort to sell security systems. I don't question it, but the picture that it evokes in the mind of the individual seeing it of horrendous crime is, I think, rather more hyperbole than it is fact.

Lest the committee think these are just a sales efforts or the efforts of those who are trying to gain the immediate personal objec-

tive—last month, I and perhaps even members of the committee, received the prestigious American Law Institute, American Bar Institute CLE review. That is a document that goes out to all attorneys in the country who are likely to be attending these very significant educational efforts. In the left-hand column is a headline which reads, "Rise in Computer Crime Demands New Techniques. International Criminal Law Course Set for October 1–2."

I read the first page. I read the follow over page carefully. I am not as young as I once was, so I read it again. I found absolutely nothing whatsoever dealing with computer crime or computer criminal law enforcement.

So, after my third reading, I sent a letter to the Institute and said "I am interested in this area. I would welcome some indication from you of the nature of the computer crime subject matter that is going to be covered." I got back a letter from the ALA/ABA saying, "Here is a copy of our issue of August 6, 1982. That says what is covered."

So I sent back another letter saying, "I have read that several times and I see nothing about computer crime." Some of the people whom I respect very greatly, of whom two are here in the room, Donn Parker and Susan Nycum, I would suspect would be on this program and yet nobody is there. "Please tell me what the program is."

I then received a telephone call from a member of the ALA/ABA group saying that maybe they were engaging in a little excess. "This program doesn't have anything to do with computer crime. What we meant was that computers are making it more difficult to deal with international criminal problems."

Now, those two trivial examples I think are really symptomatic of what so many have done with the obvious dangers which computer crime might present.

The last witness testified effectively and forcefully as to what might be. And I can't question what might be.

But it seems to me that when we deal with a statutory proposal which I would like to come to in a minute, we ought to have something more than just speculation about somebody taking all the money out of Chase Bank and passing it over to Poland what have you. We ought to have some hard data. We ought to have some real live examples.

I have been teaching courses in computers and law at Columbia for 11 years now. That is my regular school on a continuing basis. I have also taught the course at four other law schools: Georgetown last semester, and two of the students are with me now; Stanford, Duke and NYU, I don't pretend that I have seen everything, of course, because the seminars cover a broad range of subjects.

But in none of those 11 years of experience and probably 20 separate seminars with students like Ken Rynne and Kenny Hayashi doing their research work, have I seen any hard indication that there is a problem here which would justify Federal Government involvement.

There may be a problem. There are some problems but it is a far cry from speculation and minor problem to the next step of statutory enactment.

I have for 17 years been general counsel to the Association of Data Processing Service Organizations which presently is made up of something like 560 computer service companies throughout the United States. I suspect there are very few you could name who are not members of that organization.

The association certainly does have security and privacy guidelines, as you would expect. And I am not purporting to speak here on behalf of that association. But as general counsel over those 17 years, obviously across my desk pass the problems of the industry, whatever they may be, ranging from straightforward economic problems, whether a carrier offers insurance coverage, on to privacy problems and so forth. The level of computer crime problems that come across my desk is at almost the noise level. It is there; I don't suggest that people are not concerned about it. But it does not evoke within the membership any strong feeling that there are major legislative actions which need to be taken.

Almost universally, the attitude in the industry, is that "we in the industry shall do our job through better management, better security measures and better controls." Maybe there is a need for a crime statute. Nobody says there isn't. But neither has there been great demand for that kind of thing.

Perhaps I should say, before I make the next statement, that I am not a registered member of any political party. However, I do have a strong feeling as an individual that we ought not to have new legislation unless it is needed. It is a simple matter of freedom: I prefer not to give a government power unless a clear need has been demonstrated.

I also feel strongly that to the extent one can take action at the local or the State level, one ought to do it at the local or State level as you have done in Florida, Congressman Nelson. Before Federal Government statutes are passed, it seems to me there is a strong presumption to be overcome that the interference with freedom is justified and that it cannot be achieved at the local level.

I have been a prosecutor three times in my career. At one time I was a special assistant attorney general in charge of all organized crime enforcement in the United States. This was shortly following the so-called Appalachian crime convention, which you may recall took place back in the late 1950's. It was front page headline news worldwide. There were the most dramatic cries that "we need wiretap legislation"; "we need to get rid of search and seizures restrictions"; "we can't deal with organized crime." There we had a problem. There was no question but that organized crime existed. A major question was what types of legislation were appropriate, if any.

I was called into Government in early 1958 and set up a unit with 20 lawyers, and 5 offices throughout the United States. We examined that problem in the same way I am urging this committee to examine this problem. It did not take very long for us to find that the problem was not lack of statutory power.

There was more than enough statutory power. The problem was enforcement. It was the splintered, divided jurisdictional problem that government on every level had in dealing with what in essence was a worldwide kind of conspiracy.

On recommendations, some accepted, some rejected, dealt with the prosecution problem, as an administrative, a management problem. Many will credit the present strike force approach to that original set of recommendations.

I don't suggest that we have solved the organized crime problem. I don't suggest that the RICO statute wasn't useful. I do suggest that before one goes to the extent of major legislative effort, one should examine the underlying assumptions which too often are taken for granted.

In addition to that, crime statutes very frequently offer excuses to those who ought to be doing the job. Both students here are convinced, as I am, that computer crime problems today are largely management problems—business management problems. That does not mean one can eliminate computer crime anymore than one can eliminate rape, prostitution or any other kind of crime. But in a free society where we do not choose to place a policeman in every living room, we have to live with some level of crime.

I think we are all convinced from what we have seen that this can be dealt with very largely on the management/educational/security level.

I don't suggest there hasn't been important work done. There has. The FBI has done some excellent training work. The IBM Corp. particularly has done very important work in the area of computer security. So have other organizations.

The courts are beginning to recognize the problem and to impose liability in areas where computer users have failed to take appropriate security action. The September 14 current issue of Law Week—I just happened to pick this one up yesterday as suggesting how much one can learn by inquiring into the problem—reports the case of *Thompson* v. *San Antonio* merchants. There a court held that a credit reporting agency that failed to program its computer so as to protect against excessive error and failed to design procedures to detect error, is liable for actual damages of $10,000 for resulting humiliation and mental distress, to another.

Now, when the courts recognize this problem and begin to impose, liability on those who fail to do what they ought to do, we may be dealing with the matter in a far better effective way than by mandating from Washington or even from the State or local level some new rule which limits the freedom of individuals.

Incidentally, the *Thompson* case is not sui generis. The *Vecco* case goes back 10 years holding much the same thing—that those who failed to have backup tapes are not going to recover punitive damage from those who steal their computer tape because they should have had backup. They should have had security measures.

Now, what is my suggestion? I am certainly aware of the committee's time limitation. I think there are a number of ways in which we ought to approach this.

First of all, we certainly need education at virtually every level, including in the law schools. Today's law students will to be leading the country in years to come in terms of criminal law enforcement, statutory enactment and so forth. There are precious few law schools that have any course at all dealing with computer issues, much less computer crime issues.

I did a survey of computer law education in 1977, and discovered that there were very few courses given throughout the country. The number had, in fact, dropped since 1973, which was the most recent information I had, for comparison purposes.

We have got to educate our businesses, our law enforcement officials, the old-time cop on the beat has got to be educated to the extent necessary to deal with something that has come along since he got his badge.

Accountants certainly have to know how to deal with computers, not just the major 8 or 10 national firms but those at the working level throughout our society. Fifty-person accounting firms need to have computer competence.

We have to develop computer industry professionalism and an ethical code which make it clear to those both in and out of the computer industry that computer crime—whatever it may be and there is still no definition for it—but whatever it is, is as bad as antitrust crime or other kinds of white-collar crime.

It was not very long ago when people were able to brag about antitrust violations. Fifty years ago it was almost a badge of honor to receive an antitrust charge. It showed you had succeeded. It wasn't until some people went to jail from some major corporations that it began to be clear that society regarded income tax and antitrust violations as antisocial. Then it began to be made clear to those involved in white collar crime that it was antisocial. Organizations and businesses began to conduct internal enforcement, through their legal counsel and otherwise. We need to do that in computer areas, so that those who think they are "playing games," realize that they actually are causing harm that reaches throughout society in much the same way that stealing from a store is finally included in the ultimate price the average person pays.

We certainly need to understand the implications of computer crime at a level so that the thinking person in the street can understand the nature of the problem in the same way that he or she understands the nature of the privacy problem, about which has been a good deal of information.

I believe this committee would do very well if it would ask the Office of Technology Assessment to do a special study on computer crime. I see in the room Dr. Weingarten, who is one of the senior people of the Office of Technology Assessment in the computer area, and whom I know to be interested in this area. OTA's most recent publication does include some discussion of the computer crime problem. But they ought to be given, in my judgment, a chance to come back and advise this committee and the Congress just what the problem is and what might be done in order to manage it and deal with it in a socially acceptable way.

And, finally, and I will be brief, but I would welcome questions in this area, I believe we need a national effort to understand "computers and society" problems in the economic area generally, not just in computer crime but in the many other areas of which computer crime is one manifestation. These problems one day may overwhelm us. If and when they do come—I am speculating, of course—but if and when they do come, computer systems may it be so embedded in our structure as a result of the various kinds of

machines one sees all over the streets at banks and elsewhere, that we really can't change.

And instead of being able to manage our future, our future will have managed us, We may have given up a vital part of the freedom which is the essence of this country and our society.

I am urging that there be a national inquiry similar in structure, to that conducted in the late 1930's by the Temporary National Economic Committee. It examined in great depth the then most serious economic problem, which was alleged concentration in American society.

TNEC brought together the relevant information throughout society, with a full spectrum of views, so that anyone who chose to examine the problem—as this committee might—would have an encyclopedia of data and opinion with which to deal.

Unfortunately, its results were published not too much before December 1941 and, of course, the ball game has changed dramatically. But even today, TNEC's reports and analyses serve as an important source of information and learning.

I urge this committee to carefully consider the possibility of such an inquiry into the economic effects of computer systems on society.

Mr. EDWARDS. Thank you very much. That was very, very interesting testimony.

Without objection, your written statement will be made a part of the record.

Mr. WESSEL. Thank you, Mr. Chairman.

[The statement of Mr. Wessel follows:]

STATEMENT OF MILTON R. WESSEL

I am pleased to be invited to testify to this Subcommittee on the subject of "computer crime". The matter is an important one in itself and, even more so, as another manifestation of our broader "computers and society" problem. I understand that the specific provisions of HR 3970 will be considered at another session.

For more than a decade I have been teaching an upper-class seminar in "Computers and Law" at Columbia Law School in New York City, and, on brief visiting appointments, at Duke, Georgetown, NYU and Stanford law schools. Computer crime takes up one of the fourteen two-hour classroom sessions. At the end of the course, many of the students confess, along with me, to ignorance of what computer crime is, what its dimensions are, and what, if anything, needs to be done about it. Our ignorance is not for lack of attention or study, but because the information needed to support proper conclusions simply does not exist.

This same lack of information characterizes many other areas involving the economic effects of computer systems on society generally. After discussing the immediate subject I would like to describe one approach to remedying our ignorance, through a Temporary National Information Committee ("TNIC").

COMPUTER CRIME

Computer systems play an increasingly important role in our society. The discipline of techonology assessment tells us that any major technological advance—the printing press, the automobile, nuclear power, genetic engineering, and certainly the computer—fundamentally affects the ways in which we live. We must expect computer systems to have some impact on the ways crimes are committed, as well as on criminal law enforcement.

Technology assessment, however, is at best an uncertain art. Where there is little more, it may be necessary to act on the basis of assessment alone. Some believe this may have been the case when controls on recombinant DNA research were first considered. But when dealing with a problem whose essence is empirical, and where there is no apparent crisis at hand, as here, we should exhaust reasonable research and study before turning to government for severe relief.

A number of persons have labored long and hard on computer crime. Donn B. Parker's work at Stanford Research Institute is seminal. It clearly demonstrates the need to pay attention to the matter. Yet I am confident Parker will agree that our information on computer crime is sorely lacking in scope and reliability.

First, we do not even have a single definition of computer crime. Depending on the speaker and purpose of the presentation, it may be a crime against a computer system, such as the magnetic erasure of electronic impulses from a tape; it may be a theft from a computer system, such as stealing a disc, drum or tape on which sensitive information has been electronically recorded; it may be an improper access to and misappropriation of proprietary information from a data bank, even without an erasure or taking of tangible property; it may be a tampering with a software system to commit a crime, such as the modification of a program to divert bank funds from a depositor's to a thief's account; it may be a use of a computer system to assist in a crime, such as in the Equity Funding fraud; it may be almost anything else in which some aspect of a computer system or a computer-person is involved. And it may be any combination of the above. Some types of computer crime may require a degree of computer expertise, and others none at all. Indeed, one individual who was employed by a computer company and charged with a straightforward murder, consulted me as an attorney because he somehow had been led to believe that he needed a "computer lawyer".

Second, however it may be defined, we do not have adequate information about the extent of the problem. Many figures are bandied about, but there is little hard data. One research study estimates the annual cost of "computer abuse" as $300 million, with an average loss per incident of $450,000. A GAO study reports total known and reported "computer-related crimes in federal programs" to be $2,161,413, with a per incident average of $44,110 and a median of $6,749. The two studies are not fully comparable, but the vast differences are apparent and confirm the inadequacy of the data base.

We often hear that what we know is just the top of the iceberg, and that only 15 percent of computer crime is actually reported. A 1980 Law Enforcement Assistance Administration (LEAA) publication quotes "FBI experts" as estimating "that only 1 percent of all computer crime is detected, only 14 precent of that is reported, and only 3 percent of those cases ever result in jail sentences." Accordingly these same experts conclude that "only one of 22,000 computer criminals goes to jail." One finds little source support for such guesses, however. A year after this LEAA report was published, Donn Parker referred to these same figures, saying, "These numbers are all reported without any foundation of published fact." Three times as a crime prosecutor I have learned how little evidentiary support there can be for the often flagrant "informed source" statements about the innerworkings of syndicated crime. Some computer crime estimates appear to be much the same.

Third, we do not know enough about the individuals who commit computer crimes. One widely reported criminal "profile" study finds the typical computer abuse perpetrator to be young ("between 18-46 years of age, with a mean age of 29 and a median age of 25"), skilled, intelligent, verbal, eager, in a position of trust, involved in collusion, evidencing the "Robin Hood syndrome" (which justifies harming organizations and computers, but not people) and the "differential association syndrome" (which results from following the accepted practices of associates.[1] Readers of this study draw all kinds of conclusions about the special investigative and prosecutorial techniques required to deal with these kinds of "white collar" criminals. Yet the study is based upon an interview of only seventeen perpetrators, hardly enough to justify such important enforcement conclusions. The study does not deal with those involved in the "dozen terrorist attacks on computer in [the] U.S.", referred to in a fact sheet supporting HR 3970, or those with other motivations. Such essentially anecdotal evidence may be helpful in suggesting avenues of further research, but absent a crisis, is hardly sufficient to support major governmental action.

IMPROVING ENFORCEMENT

Crime is a serious problem. Law enforcement's charge is a difficult one. Certainly additional substantive power might ease its assignment. But grants of power almost always carry a price in human freedom. I believe that the alternatives to substantive crime legislation should be explored adequately before we decide whether the crime-reduction benefit of a proposed statute will outweigh its human-freedom cost.

[1] The "Peninsula Ethic", is another similar reference. It justifies fishing around in a computer system and taking whatever is found as being in the public domain.

On November 14, 1982, we mark the twenty-fifth anniversary of the so-called "organized crime convention" at Appalachia New York. Then far more than now, there was a cry for new measures against syndicated crime. Some were Draconian, going even beyond the Smith Act's unconstitutional restraints on subversion. As a former organized-crime prosecutor, I was called back into government to lead an inquiry into the matter. It took our unit exactly ten months to hire staff, establish offices throughout the nation (here in the District and in Chicago, Los Angeles, Miami and New York), conduct extensive grand jury and other investigations, and submit our conclusions to the Attorney General. Despite the admittedly serious organized crime problem, our final report (published in 1961 by this Committee) stated:

"The conclusion of this report is that the greatest need is for more effective prosecution under existing law through a modern law enforcement structure, not for new laws and regulations."

Last week the Judiciary Committee considered a proposal calling for a secure national identification system to help relieve the illegal alien problem. Seven years earlier, Frances G. Knight, head of the State Department's Passport Office, had proposed issuance of ID cards to American citizens, complete with fingerprints; variously there have been proposals for an SUI (single universal identifier), and a national data bank or procedure linking together existing data banks, all designed to help resolve the illegal alien problem, or the tax evader problem, or the fugitive problem, or the subversive problem. That they might do so I have no doubt. But the price would not be an easy one to pay.

I do not mean to engage in hyperbole. Certainly neither HR 3970 nor any other proposed computer crime prohibition of which I have heard extracts a price as great as the identification and data bank proposals. But neither has the need for computer crime relief been demonstrated to the extent it has been for illegal aliens, tax evasion or subversion. Thus, examined as a simple cost/benefit equation problem, there is little more justification for substantive computer crime legislation at this point, than there is for these other proposals.

I do not suggest that there is no computer crime problem, or that we should sit on our hands and wait for a crisis to develop. Although I do not consider that the need for a major governmental action has yet been demonstrated, I do believe there is already far more than enough justification for major remedial effort, in addition to further research. A number of organizations, especially IBM, have done important work improving the security of computer systems. ADAPSO (the Association of Data Processing Service Organizations) has published security guidelines for its industry. But we need much more. LEAA, the FBI and others have begun the difficult process of training criminal investigators, prosecutors and police in the necessary computer technology. But we need much more. There have been steps toward developing a computer "professionalism", and creating ethical standards making clear that computer crime is every bit as antisocial as tax evasion, antitrust violation, and other white-collar crime. But we need still far more. Certainly, we need more and better "computers and society" educational programs in our schools, universities, professional societies and private industry. A computer scientist should not be awarded a Ph. D. without at least some exposure to societal responsibility issues, yet rarely is there such a course requirement.

These are all long-term remedies, however, and are not likely to produce the early kind of "order-of-magnitude" advance which I consider to be needed during the next few years. I believe that the TNIC approach to which I referred earlier would constitute an important step in this later direction, and will now turn to that proposal.

TEMPORARY NATIONAL INFORMATION COMMITTEE (TNIC)

In 1970 a computer scientist, Dr. Bruce Gilchrist, and I began to study the various ways in which government regulation was affecting the computer industry. The study was supported by the American Federation of Information Processing Societies (AFIPS), the federation of computer societies in the U.S. At the time, Gilchrist and I were AFIPS' Executive Director and General Counsel respectively. Gilchrist is now Director of Computing Activities at Columbia University.

Our study was completed in 1972. It concluded that government regulation was indeed having enormous impact on the industry, but that there was a startling lack of information and understanding about what was going on. Our recommendation, set forth in a book published in 1972 by AFIPS Press entitled, "Government Regulation of the Computer Industry", was that we needed a broad interdisciplinary study of a number of computer economic issues, procedurally similar to that conducted by the Temporary National Economic Committee (TNEC) beginning in 1938.

TNEC was a Congressionally mandated inquiry into what many believe to be the the then most critically important economic issue—alleged concentration in the American economy. Whatever their economic or political views, many observers consider that TNEC was successful in marshalling the best information and talent in our society regarding the problem. Gilchrist and I concluded that the evidence supporting a similarly far-reaching inquiry into certain computer-related economic issues was equally persuasive. In contrast to TNEC, however, we believed that the effort could and should be sponsored, supported and funded outside government. Its members would be volunteer societal leaders from government, industry, academe and citizen groups. Its funding would be donated. Its power to compel testimony would be based on societal obligation alone.

Following publication of the book, major computer-related inquiries were conducted and reports published, by the Privacy Protection Study Commission (the "Privacy Commission"), the National Commission on Electronic Fund Transfers (the "EFTS Commission") and the Commission on New Technological Uses of Copyrighted Works (the "CONTU Commission"). There were a number of other studies, including those conducted by the former Department of Health, Eduction and Welfare, the Federal Communications Commission, the Office of Telecommunications Policy, the Commission on the Postal Service, the Office of the Vice President, and of course many committees of the Congress. As helpful as these efforts have been, however, neither individually nor collectively have they explored the broad range of issues involved in computer economic impact, nor have they treated the full range of societal concerns. Indeed, ADAPSO, to which I have been General Counsel for almost seventeen years, has long been troubled that it and its industry were denied a full participatory role in the EFTS Commission's inquiry into vital aspects of its business.

Attached are copies of papers prepared by Professor Harlan Blake of Columbia Law School and John L. Kirkley, Editor of the computer industry's trade publication, Datamation, and me, and editorial comment supporting the TNIC approach. There may be incipient recognition of the usefulness of this approach, but I fear that if we have to wait for these efforts to mature into action, we may one day find crisis at last upon us, well before the necessary remedial action has been taken.

Although its focus would be different than earlier inquiries, TNIC's assignment into computer economic effect would include many computer societal effect issues, especially computer crime, because of their inevitable economic consequences. Indeed, one of the difficulties in dealing with computer crime, as with much white-collar crime generally, is that the common absence of violence or apparent victim masks its serious dangers to society. However, TNIC would of course build on and not duplicate the work completed by the organizations and agencies to which I have referred.

Many concerned citizens are aware of the potential effects of computer systems on their privacy. Other computer system effects are not so apparent. It might be useful to describe three of them.

(1) Competitive impact. As suggested in my articles with Harlan Blake and John Kirkley, there is evidence that computer systems are linking formerly independent and separate segments of our economy into tightly integrated "packages." This phenomenon, which the computer industry describes as "bundling", has long been a source of industry concern. "Unbundling" (with respect to computer services, as the result of the IBM/US antitrust consent decree in 1956, and with respect to aspects of software, as the result of IBM action in 1969) has been identified as a major contributor to the computer industry's development. "Rebundling", however, appears now to be taking place. It includes not only the hardware and software components of the past, but other components over which the vendor may have domination. For example, in an EFTS system regulated communications and banking activities may be bundled with proprietary information. Clearly these systems serve societal wants, or they would not be saleable. But they may also create restrictive linkages similar to those tying, franchising and licensing practices which have long been prohibited by law. TNIC might consider whether such anticompetitive consequences can (or should) reasonably be avoided, say by developing computer standards, which would make it possible to plug into and out of a computer system as easily as we plug into and out of an electric light outlet, and by application of the doctrine of "maximum separation", which seeks to eliminate undesirable cross-subsidization and other anticompetitive interactions between separate commercial activities.

(2) Computer prediction. One of the great benefits of the computer system is its ability to analyze information and make predictions, with ever-greater accuracy as the software improves and the volume of relevant data increases. Yet however accurate, certainty in this life is impossible, with or without computers. Inevitably some

individuals and organizations are improperly caught in the prediction web, because they are assumed to be what they are not. They are "stereotyped."

There is nothing especially new or startling about predictions derived from stereotyping. Banks have "redlined" specific geographic areas; insurers have predicated rates and coverage on age, sex, residence, and employment and marital status; credit grantors have based credit on the length of employment records; employers have denied jobs to applicants who perform poorly during testing of ability, interest, loyalty or honesty.

Prediction has deep and serious Fourth Amendment and Due Process implications, however, which are at the heart of this Subcommittee's jurisdiction and concern. Our legal system has traditionally sought to reduce government's inevitable errors to societally acceptable minimums, through concepts such as "probable" and "reasonable" cause or suspicion, "reasonable doubt", "burden of proof", and "substantial evidence." More recently, law has been developing which in some circumstances restricts the use of certain prediction parameters, including race, religion, age and sex. As the use of computer prediction increases, my suspicion is that this development of restrictive evidentiary standards and parameters will continue. Perhaps that is as it should be. But every resulting restriction has a cost both is limiting the freedom of those who wish to make predictions and in introducing uncertainty into decision making. TNIC's inquiry might develop other and better approaches. As an alternative, for example, consideration might be given to a constitutional or Sherman Act-type principle requiring that certain major kinds of prediction be based upon a reasonable selection of the least offensive available parameters. Such a principle might make it possible to balance the myriad pluses and minuses involved in each of what will undoubtedly be a burgeoning number of prediction systems, on a far more satisfactory case-by-case basis.

(3) Dispute resolution. "Socioscientific disputes", of which computer-related controversies are but one example, are posing increasingly serious problems to society. The IBM case may not have reached the proportions of the Manville or Love Canal tragedies, but it comes close. When dismissed by the government earlier this year, it was only days short of its thirteenth anniversary. It had been on trial before a judge more than six years, with 700 trial days, 87 live witnesses, 860 deposition witnesses, 17,000 exhibits admitted to evidence and 104,000 transcript pages. Had the case continued through final appeal, which undoubtedly would have taken several more years, its judgment would have dealt with an industry as different from that when the complaint was filed in 1969, as space travel is to the horse and buggy. Surely this is no way to resolve a problem.

I have advocated the "procedural rule of reason" as a preferred advocacy tactic in socioscientific disputes, the "state of the science" conference as a better way of finding the credible scientific evidence needed for public policy decisions, and greater attention to institutional responsibility by those involved in the decision process, including the judiciary, law firms, corporations, educational institutions and professional societies, as a means of assuring that the interests of the greater society will be considered adversarial dispute resolution.

These specific aspects of socioscientific dispute resolution may not be appropriate subjects of TNIC concern as such. However, I would hope that TNIC would apply new innovative procedures of dispute resolution in its work, and that at its conclusion it would serve as one model of how to produce the credible expert inputs needed for societal decisions.

CONCLUSION

"Computer crime" is an exciting subject. It can sell products, services and ideas. Last month I received a copy of the prestigious ALI-ABA CLE Review,[2] with a bold front-page headline entitled "Rise in Computer Crime Demands New Techniques; International Criminal Law Course Set for October 1–2." The headline caught my attention, as it must have others. Undoubtedly it sold registrations to the many who read little more than headlines. Yet there was not a single word in the article to follow about computer crime or its enforcement! Those who do speak and write about these subjects often do so most dramatically, referring to the "Trojan Horse attack" and the "trap door" and "salami" techniques.

Government has a vital part to play in our lives. There is a developing belief, however, that our society may have gone too far in relieving the private sector of

[2] A weekly publication of the American Law Institute-American Bar Association Committee on Continuing Education.

the obligation to do its part. We must not permit dramatic showmanship to mislead us into reversing our direction.

I do not consider that there has been any demonstration of a crisis or emergency created by computer crime. We have not adequately defined the problem, we do not know enough about its dimensions, and we do not know how to attack it. The evidence does not disclose a need for government to take drastic action.

The evidence does demonstrate, however, a need for information, education and discussion, and for further private sector action. TNIC would produce the information, and stimulate the debate and understanding required to support the considered action by government, industry or anyone else regarding computer crime and the economic impact of computer systems on our society generally.

TNIC may need Congressional endorsement if it is to get off the ground, but it can almost as effectively be housed in the academic or private sectors as in government. It does not require any major grant of governmental power or even public funding. I hope that this Subcommittee will consider such an approach to the computer crime problem.

[From the Columbia Law Alumni Observer, September-October 1981]

WHERE IS THE COMPUTER TAKING US?

(By Harlan M. Blake and Milton R. Wessel)

America is well advanced into the computer age. We all observe this as we travel and glance at the ubiquitous airline and hotel computer terminals, or stay at home and receive our monthly computerized telephone or electric utility bill or bank statement. What most Americans do *not* realize is that right now extremely important decisions are being made and massive investments planned in computer-related systems of communication, banking and marketing, among others, that will deeply affect their own future and the nation's. These giant new systems will profoundly change national and international economic structure and performance. They will alter business decision-making, rearrange economic power, and limit alternatives in control of the performance of the economy. The systems are so complex and intertwined in all branches of our society and so enormously costly, that once the investments are made, there is no turning back. Yet fundamentally important questions which they raise about our future have not been answered. Indeed, they have not even been discussed in the public forum. We need to deal with these forces intelligently, but have not yet faced up to the job.

Whether we live in the "information", "post-industrial", or other society, many of the technological and economic forces at work are very different from those of an earlier day. The societal environment of the 1980's has its genesis in the tremendous scientific and technological investments of World War II. Today's resulting economic developments promise to be as powerful in their impact as those created by the nation's industrialization of a century ago, its emergence as the world's leading industrial society after World War I, or the world-wide economic collapse and great depression of the 1930's.

Although we now have far more sophisticated economic analytical tools than we had during the 1930's, the problems of international economic interdependence are much more complex. Indeed, many despair of the ability of human intelligence to deal with them. The computerization of economic information as well as of the international commercial and financial decision-making process, exacerbates this complexity—even though computerization, properly used, could have the contrary effect of increasing our capacity for intelligent problem solving.

The nation's economic problems are all-pervasive. From persistent inflation, high unemployment and massive balance of payments problems, to declining productivity and recurrent pressures for economic protectionism, economic concerns touch most significant aspects of our society. One finds problems in almost any domestic industry one examines—even in our once vaunted steel and automobile industries.

Within the information-oriented world economy, computer applications lie at the heart of the decisionmaking process. Increasingly, the major commercial entities seek to provide network links coupled with computer power and service not only to their own corporate components but to independent firms in related industries. Will these new information processing, distribution and control hierarchies make for more vigorous competitive markets and social efficiency, or will they result in cartels, or monopoly, or Zaibatsulike financial-industrial combines? We submit that

today no one knows the answers to such questions. Yet irreversible patterns are being forged.

Under somewhat similar circumstances in the 1930's, Congress created the TNEC—the Temporary National Economic Committee. TNEC brought together our nation's best economic thinkers on what was then the key economic concern: the apparently growing concentration of economic power. The Committee developed significant analyses. It identified economic consensus, where it existed. It published pervasive recommendations, and exerted enormous influence on national economic policy. Before we can deal adequately with the critical concerns of the 1980's and the future, we need another TNEC-type look at what is happening.

Of special interest is the vast and rapidly growing branch of computing known as the computer services industry. A few examples from this branch will illustrate the nature and dimensions of the problem.

The term "computer services" today includes a variety of sophisticated products and services (such as esoteric software operating systems and time sharing) which were unknown at the industry's inception only a few years ago. Initially, however, it meant simply the traditional computer service bureau of data center, which performed rather mundane "bread-and-butter" operations for customers who did not have their own computers. Payroll and accounts receivable processing are good examples of these early industry services.

In 1956, a federal court antitrust decree required IBM, the then largest equipment and services supplier, to "unbundle" computer services from the remainder of its operations, A totally new and separate IBM subsidiary was created, named "Service Bureau Corporation." It operated at arm's length from IBM in accordance with what has come to be called the "doctrine of maximum separation." Most industry observers agree that it was this separation which helped make it possible for independent entrepreneurs to compete with IBM on a head-to-head basis. Certainly the new computer services industry quickly thrived. It now accounts for a highly competitive, multi-billion dollar market.

In 1969, unbundling again enhanced competition in a computer industry segment, this time "software". Still under antitrust pressure, IBM unbundled some of the computer software which it had been packaging, pricing and marketing as one single product with its hardware, Again, those entrepreneurs who had considered themselves unable to compete with the software previously furnished "free" by IBM, jumped in. The software sub-industry is now itself a billion dollar infant, growing dramatically.

"Unbundling"—the separation of different commercial activities so that each stands on its own competitive merits—is thus one cornerstone on which the computer services industry is built. With the new technology of the 1970's, however, previously separated activities are being joined into new and integrated ones. Although the ingredients of the integrated systems are still widely available separately, a form of "rebundling" is beginning to emerge. Examples abound:

Electronic Funds Transfer Systems ("EFTS") link the once separate activities of banking, communications and computing together, and "package" them as a single product.

Point of sale ("POS") systems add retailing and other aspects of distribution to the computing and communications package.

Delivered information systems (e.g., the lawyers' LEXIS of WESTLAW legal research services) add specialized data to the computing and communications package.

In other ways new commercial applications of technology can narrow or eliminate distinctions between previously separated types of commercial activity. The best-known example of this is the obfuscation of the once clear distinction between computing and communications. For more than a decade, the FCC, the courts, and Congress have been struggling to decide what elements of these activities should be regulated as communications, and how. The lines dividing "mail," "telegram," "mailgram" and "telecopy" are similarly becoming ever more difficult to discern.

Despite the presence of a few larger firms, until now the computer services industry has been made up of numerous comparatively small firms engaged in vigorous competition, with prolific and rapid innovation and spectacular reductions in throughput cost to consumer. One important consequence of rebundling and the blurring of formerly separate product markets, however, can be to encourage an industry made up of ever larger economic enterprises. Ultimately one or two financial and conglomerate giants could come to dominate the market.

Whatever its cause, the computer services industry trend toward merger and acquisition is well-documented. In addition, many of our largest economic organizations are either already involved in computer services or positioning themselves to enter. Some, such as AT&T and CITICORP, hold government licenses or franchises

in one of the activities involved in the package, and thus have monopoly power granted by what may be outdated law.

Newer systems, with arrays of minicomputers in offices and plants linked by wire or satellite to each other and to remote giant computer banks and data bases, relay relatively less on large hardware components and increasingly on systems design and specialized software. Developments in technology and burgeoning new applications move so rapidly that traditional U.S. dominance in world markets can disappear quickly. Japan, particularly, has lost no opportunity. The decisive competitive arena will be in software and service systems. Even IBM, the world's hardware leader, and AT&T, the nation's traditional monopolist of long-line communications, appear to know that they must position themselves more centrally in this new wave or jeopardize their present positions in the economy.

The result of these and other developments has been to threaten the competitive positions of independent computer service firms engaging in less than all the elements of the expanded, integrated, or rebundled products. The industry's present customers—often competitors or potential competitors (or suppliers or customers) of the new conglomerate entities—seem certain to lose freedom of action as they are drawn into the information web and sphere of influence of the computer-service conglomerates. What are the implications of all this for the continuing vitality and creativity of the industry? For the vigor of competitive markets among users of the industry's services? At this point no one knows the answers to such questions.

In the absence of guiding national policies, the participants in the competitive battles underway have necessarily turned to the best dispute-resolution mechanism available to them, the adversarial arena. The consequence has been a continuing series of destructive struggles. The most extreme example is the federal government's antitrust litigation against IBM, now well into its second decade. The trial itself has passed its sixth anniversary, with the number of exhibits and pages of testimony having reached the point where Kafka would have had difficulty describing it. When and if it is ever finished, the decision will deal with an industry which is not the same as the one which was the subject of the complaint filed in 1969. The government's more recent litigation against AT&T could be another example of the chaos which results from deciding such questions in this fashion.

The computer services industry is especially concerned with the special issues posed by the entry of governmentally licensed organizations into the computer services marketplace. For example, it seeks to prevent the largest banks from overwhelming the industry by virtue of an unfair "package" advantage in the offering of computer services by those who hold a legally privileged position as sources of credit. A huge variety of other such proceedings have been brought, several of which are still pending. They include litigations against national and home loan banks, administrative hearings before the Federal Reserve Board, the Comptroller of the Currency and the Federal Home Loan Bank Board and legislative hearings. Most involve different statutes and regulations, are decided by different arbiters and tribunals, take place in different economic contexts and different parts of the country, and relate to such different circumstances generally as to virtually insure that the results cannot reflect the well-defined and consistent economic policy we so badly need.

The "computer privacy" issue has had much attention in recent years, and deservedly so. But that attention may have the unfortunate side effect of leading some people to believe that the "computer problem" is under control. To the contrary, the computer's impact on society is likely to be as far-reaching as that of the printing press or the automobile, and perhaps more so. We need to deal with all its consequences, not just the obvious ones.

The new computer applications offer important benefits to the public, or they would not be thriving. It is premature to suggest that changing industry structure is necessarily harmful, or that the national interest requires that any of those involved be barred from what they are doing. Certainly no new regulatory agency or structure is proposed, nor even likely to be indicated following study and evaluation. We do suggest, however, that the nation must gain as complete an understanding of what is happening as possible. Failure to assess the economic and social implications of the new technology, including its effect on basic market structure, verges on irresponsibility. To this point, the American computer services industry has furnished a classic case of competition in its finest sense, characterized by enormous opportunity and innovation. It is, far and away, the world leader, with a contribution to American esteem as well as to business productivity and the balance of trade. At stake is not only its future, but as we have suggested, national and international economic structure, and even domination of the enormous power inherent in control of computerized information.

We are dealing with extremely complex economic and technological forces. No one claims that there are easy answers, or that the proposed TNEC-type study will produce a new and dramatic national consensus. To permit developments to just happen however, without a serious attempt to understand and evaluate, is an abdication of our responsibility as a society to do the best we can.

[From Datamation]

FOR A NATIONAL INFORMATION COMMITTEE

(By Milton R. Wessel and John L. Kirkley)

We are entering the information age woefully lacking in information.

Our society is being transformed. New patterns of economic and social interaction are being created; the very roots of human society, the fundamental processes, are being altered by the worldwide impact of the computer/communications revolution. International trade, national boundaries, social customs, all our most cherished institutions, the way we live, work, and die, are undergoing an accelerated metamorphosis unprecedented in history.

But if the truth be known, most of us haven't the vaguest idea of what's going on. And that is why we are recommending the establishment of a national body to gather and organize data about this revolution so that we, as a country, can make informed decisions about the directions our technology and our society will take.

It is true that almost every country in the first, second, and third worlds, including the U.S., has its study committees, government white papers, social gurus and futurists. But all of us view the world through the myopic lens of our prejudices and perceptions.

Some countries, notably France, the Scandinavian countries, and Japan, are further along than we in establishing national policies that indicate how computer and communications technology will be meshed into their social and economic institutions. France, in the wake of the NORA report, a government sponsored assessment of computer related technology, is wiring its schools and its cities. We may not like what the Swedes and Danes are doing, but at least those people have been leaders in passing privacy laws and dealing with the transborder flow of data. "Japan Inc." has become an accepted cliché for that country's tightly coupled relationship between government and industry. The U.S. has passed some privacy laws and completed studies on the implications of the electronic funds transfer systems, but our approach has been far more piecemeal.

John Eger, a CBS vice president and former Datamation adviser, commented in a recent speech, ". . . let me acknowledge that what we are witnessing in the U.S. and abroad is a classic case of technology outstripping the law and the political and institutional framework established by it."

And that is the problem: the technology driving the computer/communications revolution is moving far faster than the ability of any of us, individually or collectively, to deal with it.

There are several reasons for our impotence in the face of such massive change. First, we are operating with outmoded assumptions. Our political and our industrial leaders, even within the computer industry where one would expect forward thinking to thrive, are steadfastly peering into the past to make their decisions. The industrial revolution, begun in the 19th century and accelerated in the industrial world since World War II, emphasizes a goods-oriented economy with clearly defined markets that are serviced by workers on the farms and in the factories. When we think of more jobs for the steadily swelling ranks of the unemployed in this country, we try to find ways to resuscitate the automobile factories, the steelworks, and the oil fields.

But in fact we are no longer just an industrial economy. We have become a service economy with over half our work force busy producing, storing, using, and transferring knowledge or information. As Eger pointed out, "Almost half of our GNP is related to this activity, and considering the plight of our steel, shoe, automotive, and TV manufacturing industries, it is believed our strength in information services represents one of the greatest assets in our effort to shore up a sagging U.S. economy and enhance our ability to penetrate foreign markets."

A by-product of this 19th century mind-set is a failure on the part of our leaders and the public to recognize the extraordinary impact computers and communications are having on the economic and social fabric of our country. Computer literacy is growing, thanks to the ubiquitous computer arcades, home video games and per-

sonal computers, but the real, long-term impact of this tidal wave or processing power remains a mystery. We know the computer revolution is important: a lot of purple prose has been expended to the effect that our industry has invented the most significant technological advancement since the wheel or the discovery of fire. Discounting these hyperbolic excesses, it does seem to be true that computer/communications are fundamentally altering human life.

Compounding the lack of awareness of the magnitude of this revolution is a problem that is uniquely American, stemming from our frontier heritage and our innate distrust of monolithic government.

We set great store in our rugged individualism and its marketplace analog, the free enterprise system. We rely on the rough and tumble of the open marketplace to sort things out and we become justifiably concerned when any large organization, whether it be the government, a huge regulated monopoly, or a corporation, becomes so large and powerful that it threatens to overwhelm us and our competition.

AN ACHILLES HEEL

But this same philosophy, which contributes so much to the competitive vigor of our domestic marketplace, can be an Achilles heel in the international marketplace. Many other developed countries have realized the importance of these new tools and their governments have sliced bureaucratic red tape to support their national computer companies, maximize their position as exporters of technology, and protect against being overwhelmed by foreign imports.

We have been struggling for years with the Japanese to open Nippon Telephone and Telegraph to outside procurement: France is fiercely protectionist, especially in the minicomputer area; and other European countries are using "nontariff barriers" such as trade restrictions based on privacy and transborder dataflow laws to protect their domestic information markets. Canada's recently passed Bank Act, which restricts the flow of banking data to U.S.-based service bureaus, is an example on our own borders. Many foreign countries provide low interest loans, tax credits, research and development grants, and other financial incentives to support their domestic computer and communications industries. The U.S. is one of the few major countries that has not yet really begun to develop a national, coherent policy regarding its information industry.

Finally, despite our attempts to place limits on governmental growth and preserve the sanctity of the individual, we are being frustrated by the sheer size and complexity of the issues with which we are dealing and the corresponding size and complexity of existing institutions that by default are likely to be delegated the responsibility for dealing with these issues.

Theodore Rozak in his passionate book. "Person/Planet," states the problem succinctly. "Only now do we see that the scale of things can be an independent problem of our social life, a factor that may distort even the best intentions of policy. It has taken our unique modern experience with the public and private bureaucracies, the mass market, and state and corporate industrialism to teach us this lesson. We have learned that human beings can create systems that do not understand human beings and will not serve their needs."

We seem to be rapidly moving toward a form of social entropy; disorganization and randomness are setting in and the computer/communications revolution, rather than providing the glue that binds our economic and social efforts, may be a powerful catalyst toward disintegration.

One of the most obvious manifestations of our lack of focus is our showing in the international trade arena. When a handful of Arab countries can disrupt our transportation and energy systems, when the Japanese can cause widespread layoffs in our basic manufacturing industries, when companies within our own borders are selling wholesale goods to foreign firms who then sell them back to American consumers at dump prices and thus undermine American competitors, when we attend international forums on privacy and transborder dataflow and have no national policy to expound—then, despite our technological advances and our economic power, we appear confused and vulnerable to the whims of the global marketplace.

Internally we don't seem to be faring much better. A few issues have caught the attention of our lawmakers. Concerns about privacy and electronic funds transfer have resulted in some legislation and not a few study committees. Regulatory agencies such as the FCC have unsuccessfully attempted to define computers and communications. Now the FCC is trying to draw the distinction between basic and enhanced services; it may run into the same problems as before. The courts, the Justice Department, and the antitrust laws have proven ineffective.

And Congress? Back in 1976 a Right to Privacy committee, headed by Nelson Rockefeller, complained in its report to the President titled "National Information Policy" that "the information policies emerging from the Congress continue to be developed in an ad hoc piecemeal fashion by numerous congressional committees struggling to frame responses without the benefit of a comprehensive overview of the field. And information issues have apparently been mounting beyond the congressional capacity to respond." The executive branch also came in for much the same criticism. Today, six years later, the confusion has been compounded; nothing has changed but the complexity of the issues.

But if the government is floundering, many large corporations both here and abroad are not. They correctly see the new information era as an enormous opportunity and they are moving swiftly to position themselves to take advantage of the information bonanza that is fast becoming a reality. AT&T happily shed its operating companies in return for a premier position in the information marketplace. Merrill Lynch, McGraw-Hill, Dun & Bradstreet, and Citibank are just a few of the large companies jockeying for position in the information age.

Many of these companies have come to realize that there is more to this information business than just making pots of money in the short term. The are acutely aware of the fact that information is power and that the actual control of the data is more important than the sophistication of the delivery system. Robert Weissman, a D&B vice president, made these comments at the time of his election as chairman of the board of ADAPSO in 1981: "Data is becoming a new control point in our information society. It is certainly growing faster than either CPUS or lines of code. There is no famine in data—rather, there's plenty of it. In fact, more than can be handled, and data is becoming even more important. . . . I pose a rhetorical question to you as we take a look, for example, at the importance of data versus software. As suppliers to your customers, would you prefer to have the best data management system . . . or would you want to have control of all the data that your customer needs?"

CONTROL OF DATA

It is this control of data that will ultimately determine who the major players are in the new information marketplace. The private sector is moving into the vacuum created by inadequate information and the lack of any effective national policy.

Three major ramifications of the use of data as a control point are: (1) a competitive struggle for the ownership of data with the probability that a scattering of very large, individually owned databases will develop; (2) use of data to leverage competitive advantages with the serious concern that tying and other monopolistic practices will be used; and (3) political entities, especially the federal government, will use data as a political control point, or as Weissman said, "as a basis for political power and survival."

Of course, the ownership of valuable data is a fundamental practice in business, no matter what the enterprise. In the computer/communications field, given the fast-moving pace of the technology and the intense competition, this is especially true. Although dealing with technology and not databases, the recent FBI "sting" operation that embarrassed Hitachi and Mitsubishi points to the great lengths (and dollars) to which companies will go in order to obtain proprietary data.

But there is the possibility of an even more subtle abuse that can keep smaller firms from competing at all.

For example. Dennis Binder, an associate professor of law at Ohio, writing in the Mercer Law Review, discusses the legal retrieval system, LEXIS–OBAR, which, at the time the article was written in 1975, contained New York and Ohio statutes and cases, federal cases, and tax materials. SEC and FTC materials were scheduled to go on the system. Terminals existed in corporate law firms and major accounting firms.

There were several problems for what Binder calls the "average practitioner." First of all, the terminals were expensive. But even if the average lawyer could handle the capital outlay, the very nature of the information in the system discriminated against him. Because LEXIS is a commercial venture designed to maximize profits, it was designed for the corporate attorney who can afford to pay the freight. "For that reason," says Binder, "it will be a long time before the system contains materials, such as probate, real estate transactions, domestic relations, workmen's compensation, landlord-tenant, and criminal law, which are geared to the average practitioner who is primarily concerned with 'bread and butter' law."

Clearly, in the last seven years the LEXIS database has become far more comprehensive, but it still discriminates. And, in a legal conflict between a large corpora-

tion and a small client, the use of LEXIS could give the corporation a decided advantage despite the merits of the case.

Or consider the New York Times database, an extensive and useful service. It is, in fact, so useful that other newspapers and other media, both large and small, thoughout the country, could find it quite economical to drop their own morgues and rely solely on the Time's database. Eventually the Times' stories would become the only source of journalistic history. What the Times reports, what the Times thinks, becomes reality. As other viewpoints, as other data, simply vanish because of the lack of accessibility, the informational content of the world becomes less rich, less varied. It is a subtle form of involuntary thought control much more effective than the heavy-handed techniques of totalitarian regimes.

One of the most striking examples of data as a competitive control point is the movement toward a national electronic funds transfer system. Under the banner of ecnomics of scale, EFTS represents a major opportunity for a few huge institutions to dominate the retail credit market and eventually be the major partners in a closed-loop system that could sound the death knell for many small firms.

Consider, for example, a future EFTS system that links the point-of-sale terminals in major department stores with an EFTS system. The computer communications hookup includes the wholesalers supplying the department stores, the credit authorization company, and the market research activity within the bank. You, the consumer, no longer have a wallet full of credit cards. Yor have found that one of the few major EFT suppliers can supply all your credit needs and so, when you activate your home shopping terminal or use your coded EFT card, you set off a chain of events that activate the control nodes in this closed loop system. Your purchase is recorded by the store and at the same time your account with the bank has been automatically debited. The store's inventory of that item is reduced by one unit and if the inventory falls below a certain point the wholesaler is automatically notified to ship a predetermined number of replacement units. Information about your purchase becomes a part of the system, yielding information about you as an individual and as part of a class of consuming individuals (age, salary, geographic region, etc.). These proprietary data are then used by the bank and the retailer to enhance their competitive position still further.

It sounds convenient and efficient, and it is. But this type of closed system, privacy considerations aside, can have a disastrous effect on competition.

According to Professor Binder, "We could end up with two national bank cards controlling a large percentage of the retail credit in the country. If the past practices of oligopolies in our economic history is any indication, the two systems could end up as Tweedledum and Tweedledee. Entry barriers would be prohibitively high. In addition to confronting two established brand names, the potential entrant would also have to set up a national consumer-POS system. Credit service could deteriorate and competition in such matters as terms of payment could decline . . . The presence of individual credit plans is lost; credit could become expensive to both consumers and retailers."

AT THE WHOLESALE LEVEL

A further brake to competition would also occur at the wholesale level under such a closed system. The major department stores would naturally tend to deal with wholesalers who could qualify as participants in the system; in other words, the large name brands that could afford the ante to hook into the elaborate electronic network. Smaller, perhaps more innovative manufacturers would find themselves squeezed out by the giants and a further reduction in the variety of goods and services available to the consumer, as well as in price competition, would take place.

But most important would be the control of the data. The bank would be in a prime position to gather extensive information about the consumers and the retailers on the system. This knowledge would not only be immensely valuable, but its ownership by the few monolithic banks would effectively stop any competition in its tracks. By using these data in different ways, the banks could move into other competitive areas with devastating results to the smaller firms that stood in their way. This trend is already visible, with Citibank being the most aggressive.

The FTC, in an "Economic Report on Corporate Mergers," put the danger in perspective". . . When large conglomerate enterprises engage in systematic reciprocity, industrial bigness and conglomeration rather than real economy threaten to become the keys to business excess. The ultimate result is an inflexible economic system composed of an industrial elite knit together by the exchange of reciprocal favors."

Electronic funds transfer may be one of our most discussed computer systems, but few people appreciate that it represents a combination of computing, communica-

tions, banking, and information. Until now most of these ingredients have been available separately. One common EFTS model, however, is to offer the system as a packaged or bundled product—take it all or leave it all; the parts are not separately available, EFTS, then, is a rebundling of products that were formerly unbundled.

The phenomenon of unbundling has been a major impetus to competition in the computer industry. IBM's 1956 consent decree with the U.S government resulted in the unbundling of computer services and the creation of Service Bureau Corp. (SBC), an event that many see as marking the birth of the computer services industry. In 1969 IBM unbundled much of its software from hardware and gave a major competitive boost to the computer software industry. Unbundling has been the subject of a number of other such developments, though of less significance.

The rebuilding of EFTS thus represents a reversal of an important pro-competitive computer industry trend of many years standing.

Perhaps even more significant is the fact that one of the bundled ingredients is information. Information promises to be the future point of dominance and control of computer systems. Until the early 1970s, hardware was the key ingredient: these were the years of IBM dominance. Now the key is shifting to software because of the proliferation of different computer systems through the minicomputer, microcomputer, distributed data processing networking, large-scale memories, and other developments of the last decade made possible by the chip. As technology advances and software becomes ubiquitous and less proprietary, the shift will be to information.

Our message is simply that he who controls the data will soon control the whole system, for better or for worse.

If concentration of power in the private sector through the use of computer/commmunications systems has its pitfalls, this consolidation within the government can be even more dangerous.

A report issued this spring by the U.S. Office of Technology Assessment, titled "Computer Based National Information systems Technology and Public Policy Issues," discusses some of the problems associated with large, complex information systems. "It is not hard to . . . envision the potential damage that could be caused by the failure or misuse of such systems as they grow larger, more complex, and more centralized.

"Some of the risks may be *physical,* as in the air traffic control example or with a computerized nuclear reactor safety system. Others may be in the form of *economic* losses, such as the failure of an automated securities market. Still other risks may be *social,* as for example, if the larger data systems such as the National Crime Information Center of an EFT payment system were misused by the government or by private concerns to exert undue control over individuals."

There is another severe potential loss, one that occurs when the public and private sectors collide. If, for example, the power to control the EFT system is concentrated in the hands of one or two large organizations, or if a few huge computer companies become utilities, squeezing out the smaller service bureaus, the government would be forced to regulate the organizations, treating them as public utilities. Although, as Binder comments, this might be better than allowing them to become unrestrained monopolies, past experience with government regulation indicates that we would see a stifling of innovation and technological progress.

These few examples of losses in international trade, the growth of oligopoly and monopoly, and increased governmental bureaucracy, only hint at the complex issues that the computer communications revolution is creating. We are awash in books, pamphlets, reports, and articles on the information age. Yet nowhere does there seem to be anything resembling a comprehensive and comprehensible view of what's actually going on. Nor are there any guidelines available to tell us how to go about constructing a unified national place for coping with the emergence of the information age.

Of course we can do nothing. The advocates of a totally free and open marketplace would find this the obvious choice: let the marketplace decide. And perhaps that is the answer, but let's know what we are doing and why.

Nowhere is it written that science and technology must proceed unchecked. Nowhere is it guaranteed that technological innovation will solve the problems that technology has created and that information policy should take a back seat to the frantic razzle-dazzle of high-tech competition. The more our systems become encompassing, the more we need to systematically confront and understand them.

For as James Tules says in his book, "The Politics of Privacy".[1] ". . . when very sophisticated technologies go wrong, the consequences may be extraordinarily unac-

[1] James Rule, Douglas McAdam, Linda Stearns, David Uglow, "The Politics of Privacy". New American Library (1980).

ceptable—so much so that the possibility of avoiding such technologies altogether, or of systematically limiting certain of their applications, must be taken seriously as one of the options for rational planning."

NEED FOR RATIONAL PLANNING

If we are to engage in rational planning, one of the prerequisites is information. It is one of the ironies of our time that, as we enter the much-heralded information age, we have so little usable information about the very processes we are engaged in. As we mentioned earlier, massive amounts of literature about the information revolution exist in almost every conceivable format, but its accumulation has been piecemeal, fragmented, a bibliographic barrier that is enough to deter even the most dedicated planner.

Before we can make fundamental policy decisions that will affect our long-term national welfare both at home and abroad, we must cull the data about our current situation from the myriad of sources available and bring them together in some comprehensible fashion. And that is why we are recommending the formation of a working body patterned to some degree after the Temporary National Economic Committee (TNEC) of the late 1930's.

The United States had emerged from World War I as a major economic power, but the euphoria of the '20s ended in the great depression. TNEC was established to develop data that would allow society to plan for the future and not let another depression bring this country to its knees. Participants included the best economic minds of the time. Their work has enormous influence because it represented the most coherent, unbiased body of data about economic conditions in the U.S. that had ever been compiled.

We need such a body to deal with the massive confusion surrounding the computer communications revolution. Like TNEC it should bring together the best minds we have, and its participation should include experts in technology, government, international trade, and societal issues, a well as economics. Because we are in a transition from an industrial society to an information society, the committee's members will have to be comfortable in both worlds. As Amitiai Etzioni observed in a New York Times op-ed piece in June, we have been and will continue to be a two-track society for a long time to come, with strong elements in both industrial-based sector and in high-technology industries.

This new body—let's call it Temporary National Information Committee, for want of a better name—could be funded by either the private sector or the government or both. The key is that there be no strings attached.

TNIC's primary charter will be to create a database, a coherent body of information about the computer/communications age we are now entering and how it is affecting our lives economically, politically, and ethically. This database should be freely available to all who wish to use; in other words it should be accessible in a variety of ways.

TNIC should be a publisher. Bibliographies will be essential, but ever more important will be the committee's job of bringing together all the random sources of information and informed opinion and organizing them into an accessible and coherent whole.

As clarity begins to replace the confusion that a runaway technology is creating, we, as a nation, will be able to make decisions regarding the size of our institutions, how our technology will be employed, and what our posture should be with regard to international trade. We will be able to at least take a stab at measuring the risks associated with implementing these technologies and decide whether the benefits outweigh the dangers.

In short, we will be able to move away from our too often employed modus operandi of making a mess of the present and then hoping that future generations will clean things up. We need our latter-day TNEC, and we need it now.

[From Datamation, February 1982]

BACKING INTO THE FUTURE

(By John L. Kirkley)

With the long overdue dismissal of the IBM trial and with AT&T's moves into the unregulated marketplace, the everchanging computer industry has made another major readjustment.

That's why, when we heard the comment, "What we need is another national study committee," we didn't turn pale and make for the nearest exit. Normally we would greet such a statement with the same enthusiasm we reserve for root canals. But the national committee proposed by lawyers Harlan Blake and Milton Wessel is another matter entirely.

We chatted with Milt Wessel about the proposal in his Fifth Avenue law office not too long ago and found him as feisty and articulate as ever. One of his many activities is acting as legal counsel to ADAPSO: Milt was also a Datamation advisor some years back.

Right now, he says, major decisions are being made and massive amounts of money are being committed to computer-based information systems that will profoundly change the nation's and the world's economic structure. The whole fabric of our society will be impacted. Yet there has been no public debate: in fact, there is no real, clear understanding of how computers and communications are changing our lives.

Banks, oil companies, retail stores, brokerage houses, publishing firms . . . hordes of cash-rich enterprises are feverishly competing to gain the upper hand in the information age. All this frenetic activity which is restructuring the economics of the '80s, will impact long into the 21st century on how we live and work.

At present there is no structure and no coherent direction. Our government does not have a unified information policy, and we have yet to do the basics: the work of gathering information about the complex relationships involved in computers, communications, society, and the economy. We do not have the data we need to make informed decisions about this country's future.

So, Wessel and Blake are proposing a committee patterned on the TNEC—Temporary National Economic Committee established by Congress in the 1930's. The overriding issue of that day was the growing concentration of economic power. The committee, composed of the top economic thinkers of the time, gathered and analyzed economic information and made recommendations. It identified economic consensus where it existed. It was a repository for information. a focal point for decision-making data gathering by government, business, and industry, and it wielded enormous influence.

This is the type of body they would like to see created today. They propose private rather than government financing and they stress that the committee must operate with no strings attached.

We endorse the idea of this committee. Although there is no shortage of people and institutions addressing these issues—agencies like the Office of Technology Assessment and individuals like Tony Oettinger at Harvard—there is no one unbiased focal point for the many divergent views and opinions.

Primary funding ought to come from those businesses that have the highest stakes in the new information age—the banks, retail stores, publishers, and the like.

Even if the committtee's efforts are only marginally effective, they will be better than the babble we have today.

As Blake and Wessel said in a recent article in the Columbia Law School alumni newspaper, "We are dealing with extremely complex economic and technological forces. No one claims that there are easy answers, or that the proposed TNEC-type study will produce a new and dramatic national consensus. To permit developments to just happen, however, is an abdication of our responsibility as a society to do the best we can.

[From Infosystems, December 1980]

PUBLISHER'S MEMO—TIME FOR A NATIONAL COMPUTER STUDY?

Those of us close to the computer industry recognize that momentous decisions are being made daily and large-scale investments are being committed regularly in computer related systems for communications, banking and marketing that will deeply affect this country's future. Some are concerned that events are moving too swiftly and that enough questions have not been asked beforehand.

Two of those concerned people are Harlan M. Blake, professor of law at Columbia University Law School, who is special antitrust counsel to ADAPSO, and Milton R. Wessel, a lawyer and author of "Science and Conscience," and counsel to the association.

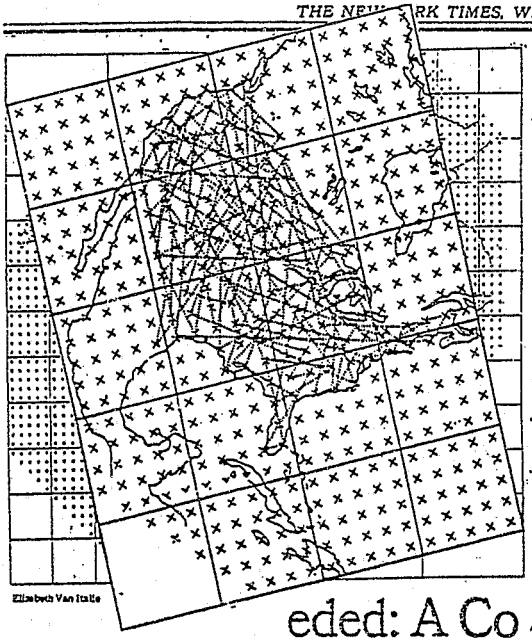
Blake and Wessel are calling for a Temporary National Economic Committee on Computers in America's Future. They point out that the giant new systems now being put in place "will alter business decision-making and the structure of econom-

ic power and limit alternatives available to control the economy's performance." They add that the systems are so complex and intertwined in all branches of the economy and so enormously costly that once the investments are made there is no turning back. "Yet fundamental questions they raise have not been answered—indeed, not even asked, much less discussed, in the public forum."

They pose a serious question of their own. Citing the fact that major business entities increasingly seek to provide network links and considerable computer power and service not only to their own array of corporate components but also to independent firms in related industries, they ask: "Will these new information processing, distribution and control hierarchies promote more vigorous competitive markets and social efficiency or result in cartels, monopoly or financial-industrial combines?"

Maybe a National Computer Study should be commissioned to find out. And if one set is up, we volunteer the services of our Associated Publisher and Editorial Director, Arnie Keller, to serve on it. But it's getting late.—ROBERT E. DIMOND.

THE NEW YORK TIMES, WEDNESDAY, OCTOBER 22, 1980



Elizabeth Van Ittle

eded: A Co mputer Stu dy Unit Ne

By Harlan M. Blake and Milton R. Wessel

It is time for the nation's leadership to make an in-depth assessment of the effects of the burgeoning use of computer systems.

We need a Temporary National Economic Committee on computers in America's future. Its effort might be similar to that of the Temporary National Economic Committee of the 1930's, which brought together the nation's best thinking on the era's key economic concern: the apparently growing concentration of economic power. It identified consensus where it existed, developed analyses of major significance, published persuasive recommendations, and exerted enormous influence on national policy.

America is well advanced into the computer age. What most people do not realize is that momentous decisions are being made and large-scale investments planned in computer-related systems in communications, banking, and marketing that will deeply affect the nation's future and their own. These giant new systems will profoundly change national and international economic relationships and performance. They will alter business decision-making, the structure of economic power, and limit alternatives available to control the economy's performance. The systems are so complex and intertwined in all branches of the economy, and so enormously costly, that once the investments are made there is no turning back. Yet fundamental questions they raise have not been answered — indeed, not even asked, much less discussed, in the public forum.

In the information-oriented world economy, computer applications lie at the heart of most commercial decision-making. The major business entities increasingly seek to provide network links and considerable computer power and service not only to their own array of corporate components but also to independent firms in related industries. Will these new information processing, distribution, and control hierarchies promote more vigorous competitive markets and social efficiency, or result in cartels, monopoly, or financial-industrial combines? No one knows, yet irreversible patterns are being forged.

The vast, rapidly growing computer-services industry is of special interest. Until now it has been essentially a small-business industry. It has furnished a classic example of free competition characterized by enormous opportunity and innovation. By far the world's leader, it has contributed to business productivity and the balance of trade. However, rapidly advancing technology has begun to blur the lines that once divided separate commercial activities. Computing and communications already have become "compunications."

The Federal Communications Commission, the courts, and Congress have been struggling for more than a decade to decide what elements of this new activity can or should be regulated as communications, and how.

The lines dividing mail, telegram, mailgram and telecopy are becoming ever more difficult to discern. Electronic funds transfer systems, grocery-checkout systems, and delivered-information systems all create new integrated products replacing separate ones. For example, they combine retailing, data, and management financial services into one product or service. The computer-services industry's accelerating trend toward merger and acquisition is well documented. Many of our largest business organizations are involved in computer services or are positioning themselves to enter. Some, such as communications carriers and banks, hold Government licenses or franchises in one of the activities involved in these newly packaged products and thus have monopoly power granted by what may be outdated law.

These and other developments have threatened the competitive positions of independent firms engaging in less than all the elements of the newly broadened, integrated, or "bundled" products. Perhaps more important, customers of these independents — often competitors or potential competitors (or suppliers or customers) of the new conglomerate entities — can lose freedom of action as they are drawn into the information web and sphere of influence of computer-service conglomerates.

What are the implications of all this for the continuing vitality and creativity of the computer-services industry? For the vigor of competitive markets among users of the industry's services? For national and international economic structures, and even for domination of the enormous power inherent in control of computerized information? No one knows.

Harlan M. Blake, professor of law at Columbia University Law School, is special antitrust counsel to the Association of Data Processing Service Organizations. Milton R. Wessel, a lawyer and author of "Science and Conscience," is counsel to the association.

Mr. EDWARDS. Incidentally, when you mentioned the cop on the beat, it reminded me that yesterday in the House of Representatives, the Stark bill was enacted, and I hope it will happen in the Senate, too, where these computer companies, especially Hewlett-Packard, will be able to give a computer to every public school in the country, and be able to deduct 80 or 90 percent of the cost so it is not too expensive for them.

We are talking about the cop's sons and daughters that you are referring to, who are going to get whatever experience there might be doing that.

Mr. WESSEL. Yes, Mr. Chairman. This generation is growing up with a competency I certainly lack and which my generation in general lacks. The trouble is we are building into our society literally billions and perhaps trillions of dollars worth of mechanisms which cannot realistically be destroyed. These ATM's—automated teller machines—which one sees at virtually every bank, they represent staggering investments, yet in fact, are only the beginning of the electronic funds transfer society. They have yet to be placed in the home or to work through television sets. That is coming.

Citicorp has announced its plans. Chemical Bank has announced its plans. So have others. The electronic society is coming and maybe it ought to come. I don't know the answer to that. I do know that once we have billions of dollars of investment, this Congress is not going to say, "we are going to destroy it." It will say, "we are going to deal with it, and here is what we are going to do."

Unfortunately, at that point we may find ourselves with another level of limitation of freedom.

Mr. EDWARDS. Well, your suggestion of an OTA study is a very good one. They did a splendid study for this subcommittee of the FBI's telecommunications system criminal recordkeeping, fingerprints recordkeeping, which needs much modernization.

Where is this data that we do need? I think part of your testimony is that the data is just not available yet to do any legislating and I agree. The gentlemen from the FBI and the Department of Justice testified to that fact also.

As a matter of fact, I think they were talking about getting some kind of a cross-index system where they could get a printout on a national basis as to where and how many computers are involved in Federal crimes

Mr. WESSEL. I heard that, Mr. Chairman. I would suggest that you direct that question as well to Donn Parker who is to follow me, but I believe that that is, with all respect, close to impossible at this time.

At the very minimum it is something that is so difficult to do that I would suspect it is more hope than it is reality.

There has been a lot of work done, particularly by Donn Parker of Stanford Research Institution, and Susan Nycum, who is here with him, and some others.

Had it been that easy, I think we would have it. It may be the data doesn't exist and it may be the data hasn't been put together. I don't know which it is.

I suspect—I do not know and I certainly don't expect the committee to act on this suspicion—but I suspect the data doesn't exist.

There just isn't that much. These figures one hears appear to be pure speculation.

The following quotation is on its face so extreme that perhaps it will appear that I am engaging in hyperbole myself; I am reading from a Law Enforcement Assistance Administration publication, entitled "The Investigation of Computer Crime." Listen:

> Experts at the Federal Bureau of Investigation say only one of 22,000 computer criminals goes to jail. They estimate that only 1 percent of all computer crime is detected. Only 14 percent of that is reported and only 3 percent of those cases ever result in jail sentences.

It reminds me of a person who pulls out of the air the fact that the population of Afghanistan is 4,613,732—not 4, or 1, but 732. How does he know? This quotation is ridiculous on its face. Everybody who has looked at those figures, incuding the two persons with me and including Donn Parker who has lectured about it, finds the same total lack of support for it. If one had at least bounded these figures as rough guesses, then it might not be so misleading, but these are very specific. There is 1 percent detected, 14 percent reported; 3 percent get jail sentences. That is just ridiculous.

Mr. EDWARDS. Maybe we ought to get that gentleman or that woman to testify some day and ask them where they got those figures.

Mr. WESSEL. The answers might be "I am sorry. This is highly confidential. We couldn't give you that information, Mr. Chairman." I think you can sense the sarcasm in my voice. I do think this kind of publication in a Government brochure, which is relied upon by law enforcement people as gospel, on its face ought to be dealt with for what it is.

Mr. EDWARDS. Well, I believe there are a number of States that have this criminal statute already. What has been their experience? Have studies been made of those?

Mr. WESSEL. Well, I understand there has yet to be a single prosecution under the Florida statute. Mr. Hayashi.

Mr. HAYASHI. The Florida statute was the first computer crime statute ever enacted in law and that was in August 1978.

As of this moment, to my knowledge, there hasn't been any prosecution under that statute. From what I have seen through studying the area of law, all the prosecutions have been done under your traditional laws of theft of property, destruction of property, et cetera.

One of the problems that has been brought up is that the statutory coverage has been inadequate as far as the property end of things.

As far as the courts' handling of the computer crime problem with the property situation, three of the circuits at this time, the fourth circuit, the second circuit and the fifth circuit have all held that a statutory definition of a thing of value is constitutionally valid. It is not void for vagueness. There are two other Federal district courts which have also upheld such statutory definitions.

I think, just from looking at where the courts are going, the indicator is clear that the courts are becoming more aware of the problem and they are expanding the statutory coverage in the common law to cover the area of computers, and the specific assets of com-

puters which are obviously very special and require special treatment.

As far as specific incidents, I think I should mention I think it was a Department of Justice person had mentioned that the *Rivkin* case is an example of computer crime. I have a copy of the trial transcript from Rivkin's plea of guilty at trial. There was no computer involved. It actually took place in a teletype room and it was a teletype wire transfer. I am not questioning the credibility or the integrity of the person who mentioned that as an example. It just points to the problem that we don't really know what is out there. The more you look at it the more you see how easily the factual basis, all the different viewpoints are really founded upon. And I think you should be aware of that.

My own personal study for the class which Professor Wessel taught, I found that there were four basic viewpoints. One is the management viewpoint that the problem is essentially a management problem.

Another viewpoint is that as far as criminal statutes go is that you should limit it to just the tool use of the computer where you have a programing or reprograming of the computer and covering up the tracks of their crime as far as theft of assets.

The two other ones are a little bit broader. I think the bill at hand also encompasses a pretty broad range, perhaps unjustifiably.

I think you should reexamine the factual foundations. Rivkin is repeatedly cited for the proposition that there is a major problem with computer crime, that the assets are incredibly huge. There was $10.2 million involved in that theft but there wasn't any real computer involvement, not directly. There was a computer room in the bank and the teletype was located in the computer room but that is about the extent of the involvement of the computer.

Mr. EDWARDS. Well, thank you very much. I am sure Mr. Nelson has some questions.

Mr. NELSON. Thank you, Mr. Chairman.

First of all, I want to thank Mr. Wessel for his approach that we need more education. Far beyond the specific question of computer crime and the economic effect of computers on society, and as we rush into this high-technology world that is expanding every day, I think that education at all levels that you suggest is an excellent suggestion in law schools.

The turning of our ethical standards to understand, as you say, that crime by computer is just as bad as other white-collar crimes is very important. So, I appreciate that, and that is the approach, as I have gone to our chairman here and asked that these hearings start, that I want to have inquiry made with regard to potential need of a statute under that umbrella of trying to educate ourselves to this need.

Now, I want to ask Mr. Hayashi, what was the nature of your inquiry that you determined that there were not any prosecutions under the Florida statute?

Mr. HAYASHI. As far as that went, my study was a broad spectrum study of all the literature and some court trial transcripts as with Rivkin and some of the better known cases. As far as that one went, I found that I believe it was a Law Review article which mentioned that as of that time there were no prosecutions. I have

since gone to the literature and from that article, and I haven't found any other indicators of any prosecutions.

Mr. NELSON. Mr. Wessel, I would submit to you that the statement by your associate here is another indication of the statement as if it is gospel when, in fact, the proper research wasn't done. There have been two prosecutions under the Florida statute. One ended in the result of a guilty plea and another is presently in progress in Polk County.

I think, Mr. Wessel, in your pointing out that we do need a repository of information so we don't have an assistant of yours coming here before a congressional committee and stating as gospel that there is no prosecution under a particular law that was passed in 1978 underscores the need for the thesis of your statement, that we do need more up-to-date information on this.

You have mentioned Mr. Donn Parker that we are going to be looking forward to. He, as you well know, has tried over the past several years to start a repository of information-gathering in order for us to understand what is happening under the various State laws that have now succeeded Florida's passing of a computer crime legislation and to see what kind of success and effort is made.

So I thank you for your testimony .

Mr. WESSEL. Mr. Nelson, if I may respond—and I agree with your conclusion which is that it demonstrates again the need for more information—but in Mr. Hayashi's defense. He probably doesn't need it. He is an outstanding student and his grade is already in. He did a fine job. What he did, of course, was conduct a very broad study of an issue which is a major issue and he, of course, looked at the sources available. He could not in a 2-hour seminar conceivably have gone down and consulted with judges and prosecutors and so forth.

A guilty plea usually does not end up in a Law Review article or even as a citation in a book of any kind. A case in progress would be something you would only discover by speaking to a prosecutor. So it may be that when Mr. Hayashi spoke here in response to your question as I had before him, it should have been prefaced—and that is one of the reasons that I asked the chairman to be able to edit these documents—with "The research that I have done, which obviously did not include personal inquiry, suggests that * * *."

But with that caveat and I think it is a fair one in his defense, we have not purported to do the kind of work that Donn Parker has done. He has done outstanding work and had we had that kind of work on any broad national level, I would suspect we would be able to say today by pushing a button there are two cases in Florida, one of them entered a guilty plea and the other one is in process, and it is going to trial next week. But we don't have that.

Mr. NELSON. My suggestion to you would be in the advancing of your thesis which I think is very valuable for us to have, but in supporting your conclusion, if it is your conclusion that we don't need a Federal statute, do not have people speaking on your behalf making statements on the basis of which their source is a Law Review article, that, in fact, prosecutions haven't been made under this or that State statute and, Mr. Chairman, I will submit for the

record a more detailed breakdown of the survey that we have made in Florida as to the use of the statute that was there.

Mr. EDWARDS. It will be received.

[The information follows:]

HOUSE OF REPRESENTATIVES,
Washington, D.C., September 8, 1982.

MS. CATHERINE LEROY,
Chief Counsel, Subcommittee on Civil and Constitutional Rights, House Office Building, Washington, D.C.

DEAR CATHERINE: We have just completed an informal telephone survey of the state attorneys' offices of the ten largest judicial circuits in Florida with regard to Chapter 815 of the Florida State Code, the Florida Computer Crimes Act. I have summarized the views of the attorneys with whom we spoke. The telephone numbers of the individuals involved are also included, in the event that you would like to speak with them yourself.

As far as we could ascertain, there have been two prosecutions in Florida under this chapter since its adoption in 1978. The first ended in a guilty plea, while the second is still under investigation.

All of the attorneys with whom we spoke were extremely positive about the law itself, but cited two primary reasons for its infrequent application thus far. Most of the circuits have experienced few complaints of computer misuse and the attorneys noted a reluctance on the part of victims to report computer crimes. Another reason for the lack of prosecutions under the computer crimes act involves the peculiarly broad nature of Florida's grand theft statute—where there have been complaints of crimes in which computers were involved, the Florida grand theft statute was applied rather than the computer statute. Moreover, the attorneys cited unfamiliarity with the area of computers and the lack of resources with which to develop expertise as a motivation for prosecuting under the grand theft statute.

In Pinellas County, Assistant State Attorney Lou Kwall (813/530-6221) recalled only one case where the computer crimes act would have been applicable. That case involved the theft of trade secrets which, under Florida statutes, is not necessarily a felony. In preparing for the case, Kwall came across the computer crimes law and intended to use it to bring charges suitable to the seriousness of the crime. Unfortunately, the case never went to trial and Kwall did not use the law, which he considered invaluable in the prosecution of the case. Kwall noted that there were practically no instances of computer-assisted crime in Pinellas but that he would not hesitate to use the computer crimes law when applicable.

Danny Hernandez in Hillsborough County (813/272-5400) recalled a couple of cases where the act might have been applicable, but the computer played such a peripheral role that he chose to prosecute under grand theft. Hernandez did note that in cases where a computer played a significant role in the crime, he would feel comfortable in using the law.

In Duval County Special Prosecutor E. McRae Mathis (904/633-6634) has handled roughly one dozen cases with large companies as victims of computer-assisted crimes. Mathis chose to apply the grand theft statute, however, primarily because of his fear of trying to use a new law which would have been open to constitutional challenge. He expressed the opinion that such cases are difficult enough to prove under the grand theft law, and that with fresh witnesses he needed to go ahead quickly rather than take the time to develop an expertise in the area of computer crime before prosecuting. Mathis feels that the computer crime statute is "well-written" and a "solid" piece of legislation, and that there is a need for it, but the problem of using a new law with limited resources make prosecutors reluctant to apply it.

The 17th circuit's Economic Crime Unit in Broward County, headed by Michael Fischler (305/765-4206), has had some cases which could have come under the computer crime statute, but until recently it has been more effective to apply the grand theft law. However, they are currently investigating a large case in which a disgruntled employee crippled a company's computer. The attorneys in the office feel that the statute is an effective and needed one and intend to apply it more extensively as they gain expertise and experience in the area of computer crime.

The other case in which the computer crimes act was actually applied was prosecuted in the 10th district in Polk County. Tom Pobjecky (813/533-0731) handled the case, which involved a payroll clerk who used the computer to take funds from a Georgia-based construction plant working in Lakeland, Florida. He was prosecuted

under both the grand theft and the computer crime statutes, but pleaded guilty, leaving the computer crime statute untested.

Mike Ramage (305/547-7041) of the Miami state attorney's office said that his office had not received any complaints in the area of computer crime. His opinion on the law itself was that it was a strong and effective statute, but covered what was still a new area in which prosecutors did not feel comfortable without a working knowledge of computers. He also noted that victims are reluctant to come forward and report computer-assisted crime. Ramage feels that both the fear that public confidence will be reduced and the possibility of writing off losses on tax statements contributed to the small number of prosecutions in Florida.

The other large circuits in Florida reported no complaints over the last four years. The contacts and their numbers are as follows:

Orange County—Belvin Perry (305/420-3798).

Brevard County—Doug Chershire (305/269-8401).

Volusia County—Ray Stark (904/258-6034).

Palm Beach County—Frank Stockton (305-837-2391).

Obviously, this is by no means a comprehensive consideration of the effectiveness of Florida's Computer Crime statute, or of computer crime in general. The impression which we received as a result of talking to all these attorneys is that the law is a "good" one and will be used in the future as more cases are reported.

I have enclosed copies of letters along with an issue sheet which express various opinions on H.R. 3970. I have requested opinions from the individuals interested in computer crime on our mailing list. I will forward them as I receive them.

Please contact me if I can be of any further assistance.

Sincerely,

JIM SOUTHERLAND.

Mr. EDWARDS. We have also asked the Library of Congress for a study and a private clearinghouse for studies. So your suggestion that we accumulate data in great depth before we jump is well received.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. EDWARDS. Mr. Wessel, you are concerned about the privacy aspect of computers, the protection of the constitutional right to privacy?

Mr. WESSEL. Yes, Mr. Chairman. If I may take a minute or two to respond, there has been a great deal of work done, as I am sure you know, and the committee knows, with respect to privacy in general. There was a privacy commission and there have been a number of other privacy inquiries.

With regard to that more obvious area, I think we at least already are far enough down the line to have some awareness of what the problem really is. There has, of course, been some statutory enactment in that area.

Some of the less obvious areas have hardly been touched upon—even in the law reviews, Congressman Nelson—much less in major areas. One of them that concerns me more than anything else in the privacy area is the stereotyping effect of computer techniques.

Computers have as an exciting potential the ability to make predictions about virtually anything and at ever higher levels of confidence depending upon the sophistication of the software and the data furnished to the system.

They can, do things like predict which area is likely to be a high crime area, even down to the point of limiting it to a specific city block or a specific building.

They can perform many other similar kinds of predictions and, of course, there is a good to that because it helps us in so many different ways.

Computers can also predict which employee is likely to be a dangerous employee in terms of stealing or in terms of loyalty or in terms of whatever other problem is there. And categorize the individual as a member of a class which may or may not be valid, much the same way that an individual who lives in a redlined area by a bank is categorized as a low possibility for paying back a mortgage and doesn't get a mortgage—even though he, as an individual, is in fact a very good risk.

When we begin to do more and more of this prediction about individuals, we run the risk of classifying the minority elements into categories which are not valid for them.

I am not talking about minority populations as such, but the 1 percent, or 3 percent, or one-tenth of 1 percent, of any group being categorized in a way which prevents them from being able to enjoy their right to freedom in this country.

Now, some of that may be essential. Conceivably some would even argue that it is necessary to categorize divorced women as high risks in terms of getting credit cards, so that we won't give credit cards to them.

But I think we have come a long enough way to say that there are other ways we can identify these same risks. Maybe there are parameters to be selected, apart from sex or state of marriage and by using these other parameters we can cause a lesser inhibiting effect upon the individual.

We haven't begun to study that. I have with me an article saying that the Pentagon transferred 5,000 people from one place to another because they were high security risks. How did they know it? Where did they get that kind of data? Maybe it is valid as to some and maybe it isn't as to others. But certainly it is not valid as to all.

Mr. EDWARDS. That is kind of frightening.

We have to go back to the House floor for a few minutes.

Are there questions by counsel?

I think this would be an appropriate time to complete this set of witnesses.

We thank you very much.

Mr. Nelson and I are going to go down and vote. We appreciate your testimony.

We will recess for ten minutes.

[Recess.]

Mr. EDWARDS. The committee will come to order.

Our last witnesses are very well known in the field that we are discussing. Mr. Donn Parker of SRI International, is that Stanford Research?

Mr. PARKER. It used to be.

Mr. EDWARDS. And Ms. Susan Nycum, with the law firm of Gaston, Snow & Ely Bartlett in Palo Alto, Calif., close to the 10th Congressional District. Both have written and lectured extensively on the subject of computer abuse and computer crime and are probably the foremost experts in the country.

We welcome you both and you may proceed.

TESTIMONY OF DONN B. PARKER, SRI INTERNATIONAL, MENLO PARK, CALIF.; AND SUSAN H. NYCUM, ESQ., GASTON, SNOW & ELY BARTLETT, PALO ALTO, CALIF.

Mr. PARKER. Thank you.

I, Donn Parker, will talk briefly first, followed by Susan, and then we would be very eager to answer questions.

My name is Donn B. Parker. I would like to have my written testimony inserted into the record.

Mr. EDWARDS. Both statements, without objection, will be made a part of the record in full.

[The statement of Mr. Parker follows:]

TESTIMONY BY DONN B. PARKER AND SUSAN HUBBELL NYCUM ON COMPUTER CRIME

INTRODUCTION

Donn B. Parker

My name is Donn B. Parker. I have extensive qualifications in the computer field, having worked for 30 years in computer programming and computer systems management. For the past 13 years of my career, I have been a researcher and consultant specializing in the computer crime problem and computer security. I have a Master of Arts degree in mathematics from the University of California at Berkeley. I am currently a senior management systems consultant in the Information Systems Management Department at SRI International, Menlo Park, California. The statements included herein are my own and do not necessarily represent those of SRI International or any clients of SRI.

I have published widely. I wrote the definitive book on computer crime, "Crime by Computer," in 1976; a new book, "Fighting Computer Crime," will be published in January 1983. In addition, I have written two books for the professional audience, "Computer Security Management" and "Ethical Conflicts in Computer Science and Technology." My SRI associates, Ms. Susan Nycum, and I produced the definitive manual on computer crime investigation and prosecution, "Criminal Justice Resource Manual on Computer Crime," for the Bureau of Justice Statistics of the U.S. Department of Justice.

Susan Hubbell Nycum

My name is Susan Hubbell Nycum. I have practiced computer law for nearly 20 years and have been involved in the legal aspects of computer abuse for 13 years. I am a partner in the national law firm of Gaston, Snow and Ely Bartlett and am resident in the firm's Palo Alto, California, office. I am the partner in charge of the firm's Computer and High Technology Group.

I wrote the first articles on the legal aspects of computer crime, which appeared in the American Bar Association Journal, the Rutger's Journal of Computers and the Law, the University of Pittsburgh Law Journal, and others. I have performed studies of the legal aspects of computer abuse for the National Science Foundation, the Bureau of Justice Statistics in the Department of Justice, and the Office of Technology Assessment, as well as for private organizations.

I am a past chairman of the American Bar Association Section of Science and Technology, a director of the Computer Law Association, one of three American Bar Association members of the National Conference of Lawyers and Scientists. I have represented the United States as one of a three person State Department led delegation to the OECD meeting on national vulnerabilities, which focused heavily on computer crime.

THE CHANGING NATURE OF BUSINESS AND WHITE-COLLAR CRIME

As we enter the information age, business and white-collar crime is changing significantly. Valuable assets are increasingly represented by information, an intangible property, and its processing, transmission, and storage are rapidly becoming the targets of crime. Such crime includes fraud, theft, embezzlement, larceny, sabotage, espionage, extortion, and conspiracy. Because of increasing automation throughout society, however, the following changes are occurring:

New, greater requirements for trustworthy employees—Data processing employees are entrusted with their employer's information assets with little likelihood of wrongdoing being discovered.

New environment for business and white-collar crime—Some automated information crimes occurring inside computers are invisible to victims. Moreover, the same computers compromised in the crimes are sometimes needed to obtain evidence of loss before it can be electronically erased.

New forms of assets subject to criminal attacks—Money as well as inventory, marketing, and other data in electronic forms that are stored in computers and on computer media such as magnetic tapes make computers the new business vaults containing the targets of crime.

New criminal methods—The technical methods used in most reported computer crimes are impersonating another computer user and data diddling (false data entry). These criminal methods are far safer for perpetrators than the relatively infrequently reported exotic and complex methods of programmed fraud such as Trojan horse attacks (inserting secret instructions in legitimate computer programs), superzapping (unauthorized use of utility programs), or wiretapping.

New time scale—While business crime has traditionally been measured in minutes, hours, days, and weeks, we now measure some automated crimes in the computer time scale of a few thousandths and millionths of seconds.

New, wider geographical scale—The geography of business crime has broadened. A fraud in a computer connected to the dial-up telephone system in Washington, D.C. could be committed from a terminal in a telephone booth in Japan or anyplace else in the world.

THE NATURE OF COMPUTER CRIME

For purposes of study of computer crime for criminal justice, computer crime is defined as any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation, or prosecution. Computer crime is not a single type of crime different from other crimes. Rather, nearly all kinds of crimes can be committed through computers or be computer mediated. In fact, we have documentation of crimes of every known type involving computers except a few violent crimes such as rape and aggravated assault.

People can use computers in only four ways to perpetrate crimes:

A computer can be the object of attack. For example, international terrorists have used bombs and submachine guns to attack at least 28 computer centers of multinational companies and government agencies in Italy and France over the past 4 years.

A computer can be the subject of a crime by providing the automated mechanisms to modify and manipulate new forms of assets such as computer programs and information representing money.

A person can use a computer as a tool or instrument for conducting or planning a crime. A stockbroker used a computer to produce forged investment statements showing huge profits to deceive his clients and steal $53 million.

A person could use only the symbol of the computer to intimidate or deceive. The same stockbroker told his clients that he was able to make such huge profits on rapid stock option trading by using a secret computer program in a giant computer in a Wall Street brokerage. He had no such program nor access to the computer, but hundreds of clients were convinced enough to invest a minimum of $100,000 each.

Computer criminals have tended to be young, highly motivated, trusted employees without previous criminal records. Thus, specific computer crime statutes are likely to have greater deterrent value for these individuals who see themselves as problem solvers, not as crooks, than for career criminals, especially by confronting the amateur criminals with the criminality of their acts. They are convinced that they do not hurt people or even organizations, just computers. More career criminals are engaging in computer crime, however, as they find their typical environments for crime being filled with computers.

As computer technology advances, a new kind of computer criminal, the system hacker, has emerged as an outgrowth of the "phone phreaks" of the 1960s. A serious epidemic of system hacking and computer program piracy is evident across the country as high school and college students learn computer methods and gain access to telephone terminals and personal microcomputers. Sometimes they even are encouraged by their instructors to engage in technological trespassing, electronic vandalism, and violation of proprietary rights to computer programs through copying. One computer program manufacturer estimates that two out of three of the copies of their products in use have not been paid for, although their profits are still so large that they do not worry about it very much. We hope to start a major study of these growing problems very soon to estimate their size and develop solutions. We

believe that specific criminal statutes will act as an important deterrent and help solve these problems.

No valid statistics on the extent of computer crime committed or the losses exist. The many numbers quoted in the news media are not truly representative of experience because acceptable mechanisms for collecting comprehensive or valid statistical samples have not been established. A lack of concurrence for a definition of computer crime precludes comprehensive statistical evaluation. SRI has the largest collection of documentation of reported cases according to our definition; yet the tabulations of more than 1,000 cases of computer abuse that have occurred since 1958 worldwide represent only a few of all suspected cases.

More money is probably lost from all errors and omissions in the use of computers than is likely lost in all intentional acts. Nevertheless, we can and have controlled errors, and their cost is budgeted as a part of data processing. We do not predict or budget for fraud; its perpetration comes as an unpleasant surprise. Moreover, the size of individual, large-loss crimes has surpassed the accidental loss experienced by particular victims.

Computer crime has been identified as being easy to perpetrate. This notion is greatly oversimplified and incomplete. Some computer crimes have been relatively easy and safe to perpetrate, but only by those few people with sufficient skills, knowledge, resources, and access to assets. They would have been very difficult for anyone else. Certain small computer crimes have been rather simple to perform by clerical employees with limited technical capabilities and minimal difficulty of access to assets; other crimes have been very complex. Automated crime is relatively insensitive to size of loss. Once a criminal act has been planned, taking $100,000 or increasing it to $1,000,000 is sometimes only a matter of adding three zeros.

All prosecutors I have questioned indicate that they have been, or would successfully be, able to prosecute all known computer crimes using existing criminal statutes. However, many of them also indicate difficulty in applying those statutes for purposes never anticipated when they were created, and few prosecutors understand the possibilities for new crimes not covered by existing statutes. The conviction rate of those indicted is very high based on limited known experience. Without specific computer crime statutes, it is easier for victims not to report their loss to avoid embarrassment or unwanted attention and prosecutors to avoid prosecuting the crime from a lack of knowledge about computers.

THE FUTURE OF COMPUTER CRIME

On the basis of case-by-case studies working with victims and investigators, interviews with more than 30 perpetrators, and computer security reviews for clients, we make the following projections:

The incidence of computer crime will increase because of the increasing number of computers and the automation of business activities.

The use of computers for criminal purposes in bookmaking, drug distribution and sales, scams, and prostitution will grow beyond the few known cases. Electronic funds transfer systems offer attractive opportunities for fraud and rapid laundering of money as $400 billion per day domestically and $600 billion per day internationally are exchanged among interconnected bank computers and automated teller machines. Increasing use of data communications, voice data entry and computer output, optical data storage, video systems, and robots will also attract new forms of criminal activity. This requires that criminal statutes be comprehensive and technology-independent to avoid further rapid obsolescence of the law.

The size of losses in significant cases will increase dramatically because of the concentration of information assets in computer and communications systems in fragile forms subject to powerful manipulation by computers. Consider the $200 million Equity Funding Insurance fraud, the $21 million bank embezzlement in Los Angeles, the $10 million funds transfer fraud also in Los Angeles, the $53 million securities fraud in Florida, the $50 million commodity futures fraud in Denver, and the $18 million inventory fraud in Chicago, which were all record-breaking cases of their types. Some analysts have meaninglessly disputed whether these cases are in fact computer crimes on the basis of several different definitions in use. Each of 17 states with a computer crime statute has a different legal definition and, of course, no Federal legislation has yet been promulgated to settle this issue. Clearly, however, the use of computers in these cases contributed to creating the special environments, tools, and access to large amounts of financial assets with limited prevention and detection controls in place.

The potential for increased protection of automated business activities is far greater than was ever possible in previous manually performed activities. That po-

tential is now starting to be realized in modern computers. Computer manufacturers and service companies are providing more safeguards today to meet new and growing user demands for security. Although significant cases of business and white-collar crime will decrease, the increasing difficulty and danger of engaging in crimes involving computers will significantly increase the losses per case. We refer to this anticipated condition as the escalation of business crime.

The escalation of business crime may create new vulnerabilities, even though a recent study by an American Federation of Information Processing Societies Task Group concluded that the resiliency of society and limited dependence on computers precludes major problems today. We believe that by using such technical safeguards as cryptography, advanced management controls, and codes of conduct stimulated in part by strong criminal statutes we can continue to limit risks inherent in the use of computer technology to an acceptable level.

RECOMMENDATIONS

In conclusion, we recommend careful legislative action to advance federal criminal laws to deter and prosecute crime in the information age. Such legislation should focus on protection of information as a valuable asset subject to criminal acts by people with new technical capabilities and not just focus on rapidly changing computer technology. However, before enactment, all of the implications and effects of information age crime and proposed legislation should be identified and thoroughly reviewed in public by a national commission of inquiry to assure adequate attention from and support of the stakeholders.

Mr. PARKER. I have been in the computer field for about 30 years in programing and managing computer centers. For the past 13 years I have been doing research and consulting on the subject of computer abuse, computer crime, and computer security.

My associate, Susan Nycum, and I have published a number of the definitive reports on this subject over this 13 years, and I should point out the statements here are my own and not those of SRI or our clients.

First, I want to point out that business and government are changing dramatically as they increase their use of computer technology, and business and white-collar crime obviously are going to be changing also.

What we are really talking about are all the same old crimes we have always dealt with: Fraud, embezzlement, sabotage, espionage, conspiracy, and so on.

Computer crime has been identified as something different, but among our 1,000 reported cases that we have collected since 1958, we have examples of computers being involved in every known crime that we know of, except, possibly for rape and aggravated assault, although there was a movie once about a computer raping a woman.

But even though it is the same old business crime, we find that when computer technology is involved, we have a new kind of problem, even though they are the same old names.

It is a new kind of problem because the occupations of the people engaged in computer crime are new: Computer operators, tape librarians, and so on. So we have a new kind of business crime because we have new occupations in high positions of trust in computer technology.

It is a new kind of crime because the environments in which it occurs are new. Some business crime is now programed into computer systems and occurs inside the computer, once removed from human view. And therefore, we have a unique new kind of environ-

ment, an electronic environment in which business crime can occur.

It is a new kind of crime because the forms of assets of business and government have changed. We now have electronic money, your money and mine stored in computers and zapped through telephone lines. For example, we don't move gold around anymore. We dig it out of the ground, purify it, and rebury it. The transfer of gold these days is zapping bits and bites from computer to computer over telephone lines. That is electronic money.

Also, computers have created another new asset, computer programs; $3.4 billion dollars' worth of commercial software, computer programs, was sold last year, an entirely new asset that is in business and government today, and that is changing the nature of business crime because there is a new asset of value, a new possibility of loss, and some criminals are figuring that out.

It is also a new kind of crime because the methods of perpetration are new. We are dealing with such methods that are referred to in jargon terms as data diddling, superzapping, wiretapping, asynchronous attacks, piggy-backing, scavenging, and so on. These are all of the new kinds of methods by which ordinary business crime is now being done, and that is making it a new problem.

The time scale of business crime is changing. Some business crime now occurs in 3/1,000ths of a second. In 3 milliseconds, a crime has been committed and the evidence has been erased.

We have thought of business crime in terms of minutes, hours, days, weeks, and so on. Now we are dealing with some business crime in the computer time scale of milliseconds, microseconds, nanoseconds, picoseconds, and we have a new measure now called femtoseconds, a quadrillionth of a second.

We are also changing the geography of business crime. If I could find a telephone booth in Outer Mongolia, I could theoretically be conducting a crime in a computer system in New York City or anyplace where there is a computer interfaced to our dial-up telephone system. That makes every telephone in the world a prospective site of some kind of fraud anyplace else in the world where there happens to be a computer interfaced to a telephone system.

So, in all of these ways, we are dealing with a new kind of crime because of these changes in the old kind of crime that we still call by the same old names.

There are a lot of people who get confused and say, well, a computer crime is something different than violation of antitrust law, or computer crime is something different than insider trading, or computer crime is different than various other kinds of business crime. That is nonsense. For every one of those kinds of crimes, we have cases recorded that have involved computers. There are many definitions of computer crime. Everybody has his own for his own purposes and so do we for our research; 13 years ago, we defined computer abuse as any intentionally caused loss where a computer was involved. That has served us very well in doing our research to find methods of reducing computer abuse in the study of computer security.

We identified four different roles that computers play in computer crime. In every case we have been able to identify one or more of these four roles and no others.

First, the computer can be the object of the attack. A person can attack a computer. We have 5 cases where computers have been shot with guns and 28 cases of computers being blown up in Italy and France in the last 4 years by international terrorists.

The second role is where the computer is the subject of an attack by being a unique environment in which a fraud takes place.

The third role is where the computer is the tool or the instrument. We have increasing use of computers by career criminals and by organized crime. For example, a pimp was caught in Santa Ana, Calif. He had a microcomputer with the names of 4,000 of his customers and their personal preferences stored on a floppy disc.

We also have found the computer used as a symbol in crime. Greenman, who was just convicted and given a 10-year Federal sentence in Florida, gathered together $120 million from a large number of investors on the basis that he claimed to have a super secret computer program that allowed him to engage in stock option trading to make very large profits.

Mr. EDWARDS. I am sorry to have to interrupt you, but we have another call to duty. It is really fascinating and we are going to hurry right back.

[Recess.]

Mr. EDWARDS. The subcommittee will come to order, you may proceed, sir.

Mr. PARKER. Fine. I was about to start a discussion of definitions of computer crime. It is obvious from testimony here today that we have many different definitions, and that is quite appropriate. I encourage that because each of us has different definitions for different purposes and as long as they serve those end purposes, that is fine.

We defined computer abuse, as I mentioned earlier, as any incident involving computers as subjects, objects, tools or symbols, and that has served us very well in studying the problems of computer security, how to make computer use safer for business and Government.

More recently, we have been doing work for the U.S. Department of Justice, Bureau of Justice statistics and developed a 400-page manual, the first definitive manual on investigation and prosecution of computer crime. We developed a new definition that served those purposes. A computer crime is defined as any illegal act in which the perpetrator, investigator, or prosecutor needed specific knowledge about computer technology that has served us well, because it included all the cases in which we were interested, and it excluded the ones that were not relevant to investigation and prosecution.

Now, as you have heard, you can define computer crime in such a way that it is just a management problem. You can define it in such a way that if a computer had not been present, a crime could not occur and thereby decide that there is hardly any computer crime at all. Or you can define it very broadly and end up with almost any business or white-collar crime today, one way or another, being a computer crime.

Some comments were made here about how much computer crime there is and I want to join with the others this morning in agreeing that there are no valid statistics.

The news media are filled with statistics about computer crime, but they are all nonsense as has been indicated. In fact, our 13 years of research at SRI has really been the only source, the open source of statistics on computer crime. We claim that our data are not necessarily representative of actual experience because there are no mechanisms by which we can collect information about the incidence or the average or total size of loss from computer crime, let alone solve the definition problem. Therefore our studies are based on a case-by-case basis in trying to determine the nature of this problem.

There are some other fallacies that need to be corrected. It is often said that computer crime is easy to do. There was an article in the Smithsonian magazine in June of this year that says computer crime is easy to do. This is a gross oversimplification.

We have found some computer crime is easy, very simple, and very safe to do, but, on the other hand, much computer crime is extremely complex and extremely dangerous to do because of the complexities and of the controls that are built into systems that are attacked in criminal activities. We cannot say that computer crime is easy or that it is difficult.

There are new computer criminals today. We think we have found new types of criminals. One example is the individual we call the system hacker. There is an epidemic across the United States today of juvenile system hackers, 13-, 14-, 15-year-olds and college students who are gaining the technology and capabilities and are using their home computers, their terminals in their high schools, dialing into business and academic computer systems, causing all kinds of mayhem in the form of technological trespassing into computers.

Mr. EDWARDS. Would that be a crime in most States?

Mr. PARKER. It definitely would be a crime in the California State statute. We have not examined whether it would be a crime in the 18 States that now have computer crime statutes, nor examined it relative to the current House bill.

We expect to start a comprehensive study of these new criminals, the juvenile system hackers, and it will include an exhaustive search for and accounting of all of the cases that have been prosecuted under the 18 State statutes and an examination of those cases.

The future of computer crime based on our case-by-case study and not on statistics, but as we define it is going to increase significantly if for no other reason, because of the proliferation of computers and the sensitive roles computers now play and will play in the future in business and Government.

But, I am optimistic that the incidence of all kinds of business and white-collar crime could decrease over the next few years as a result of the increasing use of computers.

I believe that the more business and Government use computers, the safer they become from the incidence of all kinds of significant, intentionally caused loss. My reason is that there are fewer people who have the skills, knowledge, and access to do this kind of thing, and we are advancing rapidly in computer security, both in detecting deviations from normal activity and in prevention and deterrence.

There are over 500 companies that are now offering computer security products today, both computer programs and hardware in the protection of businesses that use computers. I see a great increase in interest and concern on the part of managers in business and government in recognizing their vulnerabilities and using the very great potential that exists for effective computer-based controls in business activities.

At the same time, however, that the incidence of business and white-collar crime might possibly go down, the loss per case is likely to go up significantly. Now, again, there are no supporting statistics, but consider the 1980 $53 million securities computer fraud in Florida, the $50 million commodities fraud in Denver recently, the $21 million bank embezzlement in Los Angeles, the $10 million funds transfer fraud from Los Angeles to Zurich. By the way, we define this latter case as a "computer crime." We have spent many hours talking to the perpetrator in prison and have learned a great deal by studying that case that aids us in developing better controls in the use of computers in funds transfer systems.

I refer to this increasing size of loss as the escalation of computer crime. We are not going to have to be as worried about the incidents as we are with the amount that could be lost in any single case. Banks are now transmitting $400 billion every day through the four-wire transfer systems in use today domestically and over $600 billion every day internationally. So, a $10 million funds transfer fraud is an insignificant amount compared to the $4 billion a day that the bank was moving from computer to computer over telephone lines. Our greatest concern is this escalation issue.

In summation, I think specific computer crime status is extremely important for a number of reasons. For example, they can be used to gather statistics on prosecuted computer crime and used as a strong deterrent against the computer crime. We need very carefully developed legislation for computer crime. The legislation we have seen so far, both Federal and among the States, have many flaws in them, and a lot of work needs to be done to make them into really sound statutes.

In this process, it is essential to leapfrog the computer technology aspects. What we are dealing with today is information crime, not just computer crime. It is business and white-collar crime in the information age. Legislation that would focus on the computer and the computer programs would become obsolete very quickly because of the rapid advancement of the technology. For example, computers are defined as electronic devices.

In the next few years, we could anticipate that computers will not be electronic devices. They will be based on some other kinds of technology. For example, we are going from electronic pulses in data communications to light pulses. We are dealing with optics, not electronics, as more advanced concepts of data communications are developed. That is just one example of the way in which legislation should focus on this whole subject of information crime in the information age and not be constrained to thinking of it in terms of computers alone.

Along with this legislation, I would like to recommend that a national Federal commission be developed that would examine the

subject of computer crime, especially the escalation aspect that I mentioned earlier on a similar basis that has been done with national commissions in examining the privacy issues. The reason that I suggest that is because there has been a great lack of exposure of the computer crime problem and of suggested legislation for it among the stockholders, potential victims, trade associations, computer manufacturers, program manufacturers, and a wide segment of society; so that I think we should not have legislation until such proposed legislation has been thoroughly aired, and that we know all of its implications. I don't think we know all of the implications of changing our criminal statutes by expanding into the area of information as assets and dealing with business crime in the information age.

Mr. EDWARDS. Thank you. Ms. Nycum.

TESTIMONY OF SUSAN H. NYCUM, ESQ., GASTON, SNOW & ELY BARTLETT, PALO ALTO, CALIF.

Ms. NYCUM. Thank you very much, Mr. Chairman.

My name is Susan Hubbell Nycum. I am a partner in the national law firm of Gaston, Snow & Ely Bartlett. I am in charge of the computer and high technology group of that firm across the country. I am presently a resident in the Palo Alto, Calif. office of the firm. I have practiced computer law for nearly 20 years and have been involved investigating legal aspects of computer crime for 13 years.

I have written a number of articles on the subject, and I have performed studies for the National Science Foundation, the Bureau of Justice Statistics in the Department of Justice, and for the Office of Technology Assessment, as well as for a number of private organizations.

I have been asked this morning to focus on the experience with computers and information abuse under existing Federal and State laws, to give my impressions of any shortcomings, if any I have perceived, and any suggestions I might make for future direction.

I should like to emphasize that my views are, in all cases, simply my own, and they do not either reflect necessarily those of my partners, nor of the clients of Gaston, Snow & Ely Bartlett.

As Donn Parker has pointed out, there are essentially four categories in which computer crime, computer abuse, has occurred, and I would like to focus on the question of the experience in those four areas, from a legal point of view.

Just to quickly refresh those areas where the information system, itself, the components, the equipment, the communications, have been the target of the act, second where the information stored in the system, the programs, the trade secrets, the business data, the personnel information, have been the target of the act, third where the system is the perpetrating device and finally where the system is a symbol of the act.

Now, with respect to the legal analysis, the first category where the system, itself, the components, the equipment, the communications devices, and the like, are involved, that is not particularly troublesome for a prosecution. Those are the customary forms of property one deals with on a daily basis.

You can see it. You can pick it up. You can paint it, as they used to say in the armed services.

Sometimes it is difficult to identify; but so is a particular component of a stereo, for example.

But when we move into the second area and talk about the services involved and the information stored in those systems, it is more troublesome.

In the information area, let's turn to the question of what the Federal law is, and then we can look at the State law. And I submit this is where most of the problem lies, the intangible nature of the property that we are involved with.

The work I did initially indicated that there were approximately 40 statutes that were available in the United States Code and elsewhere for Federal prosecutors to use. There have been a few added since that original work.

The most helpful have turned out to be, over time, the wire fraud statute, and the mail fraud statute. Prosecutors have been very ingenious in focusing the wire fraud statute and the mail fraud statute in a particular situation, and they have been successful, and prosecutions have gone forward.

Also at the Federal level, the theft of services has been subsumed under a thing of value, and that has been upheld in a number of successful prosecutions. But when one moves beyond those situations, one finds a little more difficulty.

For example, the *Seidlitz* case that was referred to earlier this morning, was a theft of trade secrets by a former employee of a company over telephone lines to his terminal.

One of the counts was dismissed by the judge because it was a count for receipt of stolen property. The property was represented at that point in time in electronic impulses going from the computer to the terminal.

The judge said that those impulses do not constitute property within the meaning of the law.

Parenthetically, a case with similar facts was prosecuted in the State of California, one of our more enlightened jurisdictions and the judge in that case found that the mere transferring of electronic impulses did not constitute a taking of property under the criminal law, specifically section 499(c) of the California Criminal Code.

So, that is a problem.

We have another problem. Donn Parker and others have talked about the number of dollars associated with the software business, the point was made earlier today that it is a $3.4 billion industry.

Much of that property is protected under the copyright laws of the United States. The copyright laws do have criminal sanctions. Most of the published works are in object form, not source form.

The difference is, object form is not human readable; source form is. At this moment in time, there is civil litigation in the District Court for the Eastern District of Pennsylvania, in which the judge has refused a preliminary injunction because he is concerned that the object form of computer programs is not the proper subject of the copyright laws of the United States.

If criminal sanctions are not available for copyright infringement of computer programs in object form that would be a significant difficulty for this industry.

There are a number of criminal sanctions available under the Electronic Funds Transfer Act in the consumer area of that particular law. However, we are all aware, that what we might call the "financial supermarket" is being launched.

Plans have been announced for home services for electronic banking and retail sales. My concern is that particularly when we are talking about acts of alteration or destruction, as well as acts of fraud and theft, that the wire fraud statute and the criminal provisions of the Electronic Funds Transfer Act might not extend to cover the possibilities that will be present for abuse to the services that are being offered.

At the State level, the picture is much more varied. When I first looked at this area I noticed that the coverage in State law varied significantly. There was not one jurisdiction that was all good, for example; that covered all the areas equally well. And there were some jurisdictions, particularly the older States or Commonwealths, where, if they had not modernized the statutes, the old English common law with its notion of traditional need for tangibility property would not necessarily cover the kinds of activities that were in place.

Since my original work, 18 States have passed computer crime laws. They also vary, and there is not a discernible pattern that covers all of them to the same degree. Essentially, there are three models, one model is a comprehensive law that speaks to a number of particular aspects, and I congratulate the folks in Florida, for in my view, one of the best of those efforts, and I am particularly impressed because it was the first.

And then there are some that are specific, covering only, for example, electronic funds transfer or debit cards and the like, and then there are a number of others that simply redefine the property law in that particular State to cover computer systems.

Based on that study, I would see a number of positive aspects for the concept of a Federal law in this area, and I would think there are about four that come to mind easily. One would be to smooth out the disparities in the State laws. After all, there are a number of times when there is movement of information in information systems amongst the States.

For example, many companies now have offices doing business throughout the States.

Two, there would be a need to cover some of the loopholes I just described; for example, the question of the electronic impulses and whether or not it is a thing.

Third, the need to cover gaps that may exist with new services and products being introduced that have not previously been covered, and, fourth, a different kind of need, which is to focus attention.

Some of the State laws refer to authorized, and many companies and organizations do not set forth which is an authorized or an unauthorized act. In those States it is very important to find an unauthorized act in order to find that a crime has been committed.

Second, there are many times when a company or an organization may be a victim of a computer or information processing crime, and there are many responsibilities of that company, many exposures which might ensue without them knowing it. Profession-

als, computer programers and others in the professions, need to know what is and what is not lawful.

Third, consumers could use some help in knowing what the law is and is not, and we have heard already from the law enforcement community that they need an effective and straightforward law to use. I would hate to think that people decided not to prosecute because it was too time-consuming to figure out which law to use for that purpose, and thus some wrongs could go unredressed.

And, finally, I have had the privilege and responsibility on two occasions of representing the United States in international forums, and I have found that these have focused, to a significant extent, on computer crime.

I find that we in the United States are not acting in isolation any longer with respect to information systems services and products. We are very much a part of international commerce and international concerns. Sometimes we are joint venturers, such as with INTELSAT and other undertakings. Sometimes we are involved because of U.S. multinational corporations who have business dealings abroad and sometimes we are involved because of our participation in networks such as Swift, in which moneys are transferred around the world.

When I have been in these meetings, I have sometimes felt that if we did not seek to direct our own destiny, perhaps our friends abroad might focus their attention on us, and come with ideas of what computer crime laws we should adopt if we don't adopt our own.

Nevertheless, I would urge, as Donn has, the undertaking of a major study through the formation of a national commission. I have been a great admirer of commissions. I have had the opportunity to testify to three of them and have been very impressed with the opportunity for various viewpoints to be expressed, and also with the utility of the hearings and commission reports as an adjunct to any subsequent legislative history.

I would suggest that in addition to focusing on experience with computer crime laws that such a commission should also look into experience with some of the related laws such as, for example, the copyright law, the communications law, the electronic funds transfer laws, and others that might have bearing on this issue.

That concludes my remarks, and I thank you very much.

Mr. EDWARDS. Thank you very much, Ms. Nycum.

Your studies are financed by different companies, usually?

Mr. PARKER. Our research was funded for almost 9 years by the National Science Foundation, and for the last 3 years primarily by the U.S. Department of Justice, Bureau of Justice Statistics, and in addition, we have had private funding for some of the computer crime work and a great deal of private funding for the research and development in the securities side.

Mr. EDWARDS. There is always a crime involved, an underlying crime facilitated by the use of a computer. Do you think that there ought to be two crimes? We will say embezzlement. Embezzlement is a very clear-cut crime. Now, if you use a computer in embezzlement, do you think that is two crimes or one crime? It is not a crime now to use a computer to embezzle. Embezzlement is the crime, is it not?

Mr. PARKER. As I said at the beginning, we can still call these things by the same old things we have always called them. As you say, embezzlement. It was embezzlement. The point is in having new and specific statutes would be to cover the nature of that embezzlement that may not be well covered by the existing laws that would otherwise cover embezzlement.

For example, two programers in Philadelphia embezzled $144,000 of their employer's computer time, and embezzlement of computer services. Now, they stole computer time. They embezzled computer time, but they were convicted of mail fraud. I talked to these two programers sitting in prison cells, and they were bewildered, and they said we are programers. What are we doing sitting here in prison? How did we get convicted of mail fraud? We used our employer's computer, that is true, but everybody was doing it, and we were not doing anything more than anyone else, maybe a little bit more computer time than others.

It turned out that the Federal prosecutor decided that that was the only law under which he could successfully prosecute. These two guys had formed a private company and were selling the services on rescoring sheet music, using their employer's computer, and they advertised their firm through the mail.

Now, Gilbert and Sullivan aside, I think it would be nice to convict people for the crimes that they commit. They stole computer time. Let's convict them of stealing computer time, and this mail fraud thing. There is a great deterrent value among amateur and white-collar criminals, and we have talked to 30 of them now, when they are confronted with the fact, and they can't avoid being confronted with the fact that they are violating a real criminal statute.

Mr. EDWARDS. Mr. Nelson.

Mr. NELSON. Thank you, Mr. Chairman. This has been most educational for me.

Mr. Chairman, let me point out that Donn Parker was the fellow that, 5 years ago, we got to come to Tallahassee as the primary witness on the need, and it was a case of first impression, the first in the country. We had hardly any statistics, and yet we knew it was out there, and so we were going a lot on blind faith, and I had asked you earlier for permission.

I even have a report on the contact that we had done among the State attorneys in Florida, and we randomly picked out 10 as to what has been their success where they have had some ongoing prosecutions, and in one case a guilty plea under the statute that we passed 4 years ago; and so I want to first give my compliments to Donn for his testimony and for his direction as we fashion the words for that statute of first impression.

Let me ask a couple of questions here.

Susan, one of the areas that you listed, that you thought we ought to seriously look at the possibility of a Federal law, was that we needed to focus on what is authorized and unauthorized.

I anticipate that as we get into the 98th Congress, and we are starting to seriously consider legislation that one of the things that will be raised will be from computer users, programers who will say, don't squash our inventiveness—we want to play with these

computers, and we don't want to be restricted in our ability to play and invent.

Now, there is a certain degree of inventiveness that we want to continue to encourage. Knowing what we have fashioned together here as a first start on a bill that I have filed, H.R. 3970, do you know how we might improve that so as not to discourage inventiveness and yet to draw a line and say, this is authorized, but when you step over the line, it is unauthorized?

Ms. NYCUM. Well, my thought on that subject is that it would be very helpful to learn from a variety of vested interests, the programers, various communities of users, and of developers, what they think. That is part of the notion of having a forum such as a national commission to look at this or hear testimony from a variety of sources as to their views of what seems to be reasonable. Because I really at this point, myself, could not tell you and would not want to speak on behalf of all those people.

Mr. NELSON. Yes, Donn.

Mr. PARKER. Just one point: There are two kinds of unauthorized activity. There is exemplary unauthorized activity that results in significant advances, as you have suggested, and there is malicious unauthorized activity, and it seems to me that it would be a fairly straightforward thing to add words to the bill that would distinguish between those two kinds of unauthorized activities, making one a crime and avoiding making the other a crime.

Ms. NYCUM. Well, if I could just comment, the case involving Mr. Seidlitz was one where he suggested in his defense, and he was quite vociferous, was that the reason he did what he did was not to steal. He was not guilty at all. What he had done was for the purpose of indicating that the security system of the company was lax, and that if he stole something, he could go in the next morning and lay it on the person's desk and say, see, you have a problem here.

So, then, we still get down to the question of what would be or would not be the intent of a particular individual.

Mr. NELSON. Well, in our definition in the bill, we have said we tried to get that maliciousness into it, and we need to keep perfecting this along the line, but we have said, and I am going to shorten it here, whoever uses with intent to defraud or false or fraudulent pretenses, or embezzlement, steal, knowingly convert—those are the words that we put in the draft, trying to get at that. So as you all talk over time, keep us advised on how you think that we can perfect that.

Let me ask you this: I thought those were dramatic examples, Susan, that you gave of present cases that have been thrown out of court in Federal court because present Federal law did not apply.

I did not get the name of the cases.

No. 1, you spoke of a Baltimore case.

Ms. NYCUM. That was the *Seidlitz* case, *United States* v. *Seidlitz.*

Mr. NELSON. Then you spoke of a similar California case, and you used the statute.

Ms. NYCUM. *People* v. *Ward;* that is a 1972 case. It is reported only in the computer law service.

Mr. NELSON. And then you mentioned a Pennsylvania case.

Ms. NYCUM. Yes, sir. That is a piece of civil litigation in *Apple Computer Co.* v. *Franklin Computer Co.*

Mr. NELSON. And that is where the copyright laws did not apply?

Ms. NYCUM. Well, the preliminary injunction was denied because the judge was not sure that there was a copyrightable subject matter involved. That decision is on appeal.

Mr. NELSON. Mr. Chairman, just one other comment. I remember one of the cases that Donn Parker had told me about when we passed that legislation 4 years ago on the floor of the House in Florida. I used this example, and I want to take this opportunity just to share it with you. An airline pilot was flying on a cross-country flight one day, and he was on automatic pilot, and so while he was bored, he did something that he never had done. He pulled out his paycheck and he started calculating all of the deductions and then subtracted it to see if the final result on his paycheck worked out.

He found out there was 25 cents missing. So he happened to be checking with the other employees of the airline, and he found that all employees' checks were missing between 15 and 25 cents. Someone had obviously gone in and altered the computer, but they never could figure out who it was or how to get at this person.

Well, one day, one of the executives of the airline was gazing out his office window, and he happened to have a view of the employees' parking lot, and there in the midst of the Chevrolets and the Fords and the Volkswagens was a Rolls Royce. And they happened to check on the owner of that car and found out it was one of the programers, and he ultimately "fessed" up.

Under the 18 States now, and this is my question, would any of those State laws give us the tools to apply to this particular case to prosecute successfully or since we were dealing with a company that goes across State lines, would we need a Federal statute in that particular case?

Mr. PARKER. An answer to that would certainly be out of my area of competence, since I am not an attorney, and I think maybe an attorney might hold back a little bit in giving a final response to that.

But the point is that there are cases like that in which, and you can document them. It is easy to describe them in which there would certainly be serious question as to whether a particular State in a particular State jurisdiction, or in a Federal jurisdiction, that there is adequate law to cover that particular case.

And we can cite even a more recent case, the *Weg* case, in the State of New York, in which an individual was prosecuted for the theft of computer services and the judge said this case does not come under the theft of services law in the State of New York, and he let Mr. Weg go because he said that the law was not sufficient for the theft of computer services under their general law of theft of services.

So that the case that you describe, I would guess that some lawyers could easily argue that there would be little means of prosecution in some jurisdictions, and most likely a reasonable means of prosecution in others.

For example, under the Florida computer crime law, or the California computer crime laws, which might be particularly more

adapted to that particular kind of crime, but the kind of crime you describe is called the Salami attacks, taking small slices over a period of time so that no one individual loses very much or misses it very much. This is a very sophisticated kind of fraud, and we have very few cases of that having happened either, because the guys doing it have been so smart that we have not been able to discover it or that it has only been discovered by accident.

Susan.

Ms. NYCUM. Well, I was just thinking that the particular situation, you might assume that that is a traditional embezzlement. It is the means of going about it that might be the problem. You might also consider it as a form of larceny by trick, possibly, and certainly part of a scheme or artifice to defraud, which seems to be the focus of a number of the new State laws, the 18 that we talked about earlier.

But if you have the problem of the representation of those assets going into the hands of the person, you may have the old electronic impulses specter rising again.

So, even though you know something has happened that is untoward, you may not have the capability of getting from A to B and finding that a punishable offense.

Mr. NELSON. Thank you, Mr. Chairman.

Mr. BOYD. I guess I ought to direct a brief question, if I may, to Ms. Nycum, and this has to do with Mr. Parker's example about the use of computer time, a conviction resulting from the use of the U.S. mails. Isn't computer time "property"?

Ms. NYCUM. That is a very interesting question.

Mr. BOYD. We are not talking impulses. We are talking actual time.

Ms. NYCUM. We certainly had no problem under Federal law in finding it to be a thing of value because that is how it would fit under Federal law. In some States, however, it is more difficult to find computer services constituting a thing of value. This goes back to an economic analysis and a number of other problems in finding something taken of value. If I could make the analogy to a hotel that is or is not full; if someone sleeps in there overnight in a full hotel, clearly there has been a denial of the opportunity to sell that room.

On the other hand, arguably, if that hotel is not full, that same room cannot be offered the next day; and so maybe nothing was taken; there was not any economic loss.

I think that is spurious, but in some jurisdictions that kind of argument could be raised.

Mr. BOYD. Similarly, I would tend to agree with your analysis of the question involving the airline, 25 to 15 cents per check, in the sense that it would seem to me to be a traditional embezzlement situation. Since the individual is converting airline money to his own personal use, it would seem to come under standard State law. Would you agree?

Ms. NYCUM. That would be my feeling. But I do point out that some of these things which seem academically straightforward, turn out to be sometimes in practice not so easy.

One of the things I am constantly reminded of is that the criminal laws are to be strictly construed, and therefore any extension

that we might want to make would be vigorously argued against by defense counsel.

Mr. PARKER. Thank you.

Thank you, Mr. Chairman.

Mr. EDWARDS. Thank you to all of the witnesses, and thank you very much. We will be calling you again. You have been very helpful.

[Whereupon, at 12:50 p.m., the hearing was adjourned, to reconvene subject to the call of the Chair.]

APPENDIX

APPENDIX I

COMPUTERS AND CRIME: A DEFINITIONAL QUESTION

FOREWORD

"The Problem"

There is a problem with computers, and there were problems writing about it. The development of this paper, from its embryonic days, reflects the myriad complexities surrounding the problem. Thus, this paper is in its fifth generation of evolution. In examining the subject of computer-related crime, a hierarchy of awareness developed, each level built upon the previous stage.

To begin with, when first examining the subject of computer-related crime, one is impressed upon by what a friend termed the "Wow" Factor. Loss figures (in dollar terms) are thrown about in the thousands, millions, and even the billions. The view is from the standpoint of awe.

Then, one begins to concern oneself with possible solutions to an apparently horrendous problem. One looks to the "experts" such as Donn Parker, the godfather of "computer abuse", for solutions. And the legal/legislative regime is looked to, also, for aid in dealing with the problem.

Dissent in the ranks is noticed as one delves deeper. As the problem is examined by its many component parts, evidence mounts that the problem is not as it is popularly viewed. The facade of a monolithic view begins to crumble. A school of thought, epitomized by John Taber, becomes a force in the picture.

A fourth view emerged from the distrust and disillusionment with the views already expressed in print: does this entity (the problem) called "computer crime" actually exist?

The fast-developing area of artificial intelligence raises and helps to focus disturbing questions which remain unanswered and largely unasked. But it is this "disturbing" quality which signals the red flag of warning that these very questions should be asked. This paper is the author's latest stage of evolving awareness on the subject of computer-related crime. As with any body of legal scholarship, it is subject to change in accord with any new and relevant information. Though it does go beyond any other study both in breadth and depth, a promise of simplistic solutions to the problem can't be made.

A special note of thanks to Cheryl Bush of CBEMA for her efforts in the midst of her own job demands. Also, the author gratefully acknowledges the help of the American Society of Industrial Security (particularly Patty) for making their library and files available.—Kenny Hayashi, July 18, 1982.

COMPUTERS AND CRIME: A DEFINITIONAL QUESTION

"A society without any objective legal scale is a terrible one indeed. But a society with no other scale but the legal one is also less than worthy of man."—Aleksandr Solzhenitsyn,[1] Harvard Commencement 1978.

Recently, increasingly more press time has been given to the subject of computer-related crime. (It should be noted at the outset that the use of the term "computer-related crime", as opposed to "computer crime," is deliberate). In February of this year, Time Magazine printed an article on the "Crackdown on Computer Capers",[2] the law student division of the American Bar Association's Student Lawyer published an article on "Computer crime",[3] and the National Law Journal wrote that "Firms Face Computer Theft Issue".[4] In March, The Washington Post featured a story that a "Computer 'Break-in' Method Poses Big Crime Risk".[5] The Library of Congress Congressional Research Service updated and revised a monograph on

"Computer Crime and Security".[6] In April, the United States General Accounting Office (GAO) delivered a report to Congress on "Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive and Illegal Practices".[7] In May of this year, the Second [8] Privacy and Security Federal and State Legislation Status Report [9] indicated that fifteen states now have computer-related abuse laws. Further, a federal "computer crime" bill,[10] which was introduced on June 18, 1981 by Representative Nelson of Florida, awaits consideration in the Judiciary Subcommittee on Civil and Constitutional Rights.[11]

Underlying much, if not all, of this focused activity is the assumption that this entity called "computer crime" exists. The American Criminal Law Review, one of the most respected legal journals in the country, assumes (implicitly) that this entity exists.[12] As noted above, others, in positions of influence, have acted on this assumption and have passed statutes hoping to influence the course of events.

It is this author's contention that there are actually four different perspectives from which to view the current state of computer-related crime. It is these schools of thought which provide the foundation for the "scaffolding" of activity which presently exists. Unfortunately, in the midst of this activity, no one has examined the divergent schools of thought which underlie this activity. Also, much of the so-called factual basis, upon which two of the schools of thought are founded, are found to be questionable when subject to close scrutiny.

It is this author's stated belief that the current problem with computer-related crimes is primarily a management problem, and not a legal one. Further, the current activity directed towards "computer crime" is actually the result of unease, a misdirected knee-jerk reaction, to various of computer technology. This unease has been channeled into the reaction typical of a well-trained lawyer: that "there ought to be a law . . ."

Finally, it is contended that, since the problem is actually a management one, there is no such thing as true "computer crime"—yet.

I. THE "COMPUTER ABUSE" SCHOOL (DONN PARKER)

"The public reacts to tragedies even when it doesn't understand them, because they appeal to the most basic human instincts. Anyone can imagine himself in the same position. But the story of a climb, however remarkable it may be, can only be boring for those who do not understand the technicalities of the sport."—Lionel Terray,[13] Les Conquerants de l'Inutile.

A. The Definitional Problem

The most broad ranging studies on computer-related crime have emanated from Donn Parker and the Stanford Research Institute (SRI). These studies have also been the most influential, being the basis for much of the press and much of the legislative activity associated with computer-related crime.[14] Unfortunately, because of serious flaws, the work of Donn Parker enjoys much more press coverage and importance than is warranted.

At this time, SRI has produced three reports to the National Science Foundation (NSF).[15] For convenience, all of SRI's work will be consolidated as the "SRI Study." [16] Also, other reports have been provided for specific government agencies.[17] Further, a host of articles have been published in periodicals.[18] These works have been the most significant reason for the public reaction against what is commonly referred to as "computer crime."

Originally, the intent of SRI was to do a broad spectrum study involving criminology, sociology, technology, and law. Therefore, the focus of this study was "abusive" use (and non-use) of computers; a focus even broader than the subject areas used to narrow the study.[19] This intent was carried out in the first report, Computer Abuse. In Computer Abuse, the report was co-authored by Parker (for technology), Susan Nycum (for law), and Steve Oura (for sociology).[20] This report was reviewed by academics in each of the related fields before release.[21]

Subsequent reports, however, demonstrate a deterioration in scholarly standards. These were authored solely by Parker. The multidisciplinary approach is not implemented, and the acknowledgements do not credit any academic reviewers.[22] Despite these missing elements, the multidisciplinary intent evidently remains. Indicators of why this course of action was taken are in a popular book by Parker:

"The first proposal for my research was titled 'Computer-Related Crime.' Law researchers reviewed the proposal, saying, 'Parker, you are a computer technologist. What are you doing, trying to decide what is a crime? After all, there are only six people in the whole world qualified to address that subject.' I next changed the name of the research to 'Antisocial Use of Computers.' Sociologists who reviewed

the proposal came back to me and said, 'Parker, you are a computer technologist. What are you doing, trying to decide what is social and antisocial? After all, there are only six people in the whole world qualified to address that subject.' I thought to myself, 'All right, you guys, I will play your game.' I changed the title of the research to 'Computer Abuse'—a term that had not been used or at least formalized before. I was then able to define the problem as I wished . . ." [23]

Parker holds a Master of Arts Degree in Mathematics.[24] But his interest was crime, thus, he was constrained to adopt the buzz term "computer abuse" to win government acceptance for SRI's contract proposals.[25] SRI (and Parker) apparently use the term "computer crime" in public appeals,[26] saving the more neutral term "computer abuse" for formal occasions such as the reports to the National Science Foundation.[27]

SRI's original definition of the term "computer abuse" is an "intentional act in which one or more victims suffered, or could have suffered, a loss and one or more perpetrators made a gain. The incident must be associated with computer technology or its use." [28] But this definition has undergone subtle, previously unnoticed changes through the passage of time.

As Parker notes, the term "computer crime" implies the direct involvement of a computer in the commission of a crime. [29] SRI's use of the term "computer abuse" causes much confusion because the SRI study does not just study"computer crime." Instead, the SRI collection of cases includes civil suits, errors, and other non-criminal matters.[30] Despite this distinction, many have taken the term "computer abuse" as equivalent to "computer crime."[31]

However, the problem with SRI's work is not as simple as the public's misunderstanding between the terms "abuse" and "crime." The issue of definitions is further clouded (what about "obfuscated") by SRI's own inconsistent use of the term "abuse." Reference to the SRI collection of cases as "crimes" in several published reports has furthered the misapplication of the SRI study.[32]

As was noted before, the definition of "computer abuse" has gone through subtle changes.[33] In the 1980 update, Parker stated that the definition of "computer abuse" is:

"Any intentional act associated with in any way computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made a gain." [34]

The most significant variation with the first, previously noted definition of "computer abuse" is the phrase "in any way." Parker seems intent on stretching his already vague definition of what the SRI study is actually about to cover all bases.

The reason for this change seems to be because of some well-reasoned criticism.[35] There are cases where the offense is more notable by the lack of a computer. For example, SRI File Case #7725 [36] concerns a fraudulent sale of non-existent computer equipment. Others concern the false advertising of non-existent computer dating services.[37] The tie between these situations and computers is so tangential, yet they are included as examples of "computer abuse." In extending the avowed scope of the SRI study, albeit post-hoc, Parker concedes that he is refining the definition of the problem that is being examined. Elaborating on this point, Parker states:

"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.[38]

Upon close examination, it is obvious that there are many flaws with the SRI study in the definition of the problem with computer-related crime. SRI and Donn Parker's predisposition to characterize the problem as a criminal and a private security one must be examined in light of the definitional flaws." [39] Further, as will be examined in the next subsection, the data base used by SRI [40] to justify its stance is subject to much deserved criticism.

B. The Fact Foundation Question

A friend once described the "facts" and "figures" espoused about computer-related crime as the "WOW" factor. Claimed loss figures are "computer crime" results in the loss of $100 million [41] annually, or $300 million annually [42], or more depending on which source one looks to.[43]

Stanley Rifkin's theft of 10.2 million from Security Pacific Bank is cited as an example of a "computer crime." [44] The "round off fraud" (where a person programs a computer to round down and siphon off the remainder to their account) is noted as a serious threat to the banking industry. [45] The scandal at the Equity Funding Company, an insurance company, reputedly involved a take of more than $27 million. [46]

There are indications that the often-quoted dollar loss figures are incorrect. In fact, given that so many rely on the STI study's figures, despite the fact that the study is of "computer abuse" and not computer crime, renders the credibility of those who quote such figures suspect.[47] Further, the SRI study found an estimated annual loss of $300 million, and an average loss per incident of $450,000.[48] Yet, the General Accounting Office's Report on "Computer-Related Crimes in Federal Programs" reported that the total known and reported loss was $2,161,413, with a per incident average of $44,110.[49]

The discrepancy between the GAO loss per incident and the SRI figure is obvious. What is not so obvious is why the SRI figure is more than ten times as big as the GAO figure. The GAO study noted that the government's uses of computers are no different from the private sector's.[50] As far as credibility is concerned, the source of the GAO study were ten federal investigative agencies. There were:

Army Criminal Investigations Division Command;
Navy Investigative Service;
Air Force Office of Special Investigations;
Department of Justice, Executive Office for United States Attorneys;
Department of Justice, Federal Bureau of Investigations;
Department of Agriculture, Office of Investigation;
Internal Revenue Service;
Department of Health, Education, and Welfare, Social Security Administration;
Department of the Interior, Division of Investigation; and
Veterans Administration, Investigation and Security Services.[51]

One cannot fail to note the investigative capability embodied in this list.

The file search by the agencies turned up seventy-four cases for GAO analysis. GAO rejected five for not fitting their criteria for "computer-related" crime,[52] leaving sixty-nine known cases in the federal government. Contrast this figure with SRI's figure of 370 reported incident of "computer abuse." [53] By virtue of a larger sample size it would seem that the SRI study would have a better data base. But the SRI study if one of "computer abuse", giving it broader parameters than the GAO study.[54]

Further, there are cases in the SRI collection which do not even involve computers. Once case involved telephone equipment which was falsely wired to allow outside calls to be placed from certain phones. This case was included because SRI was considering classifying telephone systems as computers.[55]

Rifkin's theft of $10.2 million is often cited as an example of why computers need special protection. Rifkin supposedly accessed Security Pacific's computer via public telephone, and ordered the computer to transfer the $10.2 million to a bank account across the country.[56] In actuality, no computer was involved. Rifkin gained entry to the wire transfer room to observe the teletype operators, on the false pretense of doing a study to automate the wire room.[57] Access should never have been allowed. Rifkin obtained the identification code used by bank employees to effect transfer by observing the teletype operators.[58] He wrote the identification code down, left the premises, and called the bank from a nearby pay phone.[59] Rifkin pretended to be a bank officer and gave the code of the day, and effected the transfer of $10.2 million.[60] Despite the lack of involvement of a computer, Parker classifies this incident as "computer abuse," because the transfer cage was located in the computer room.[61]

The Equity Funding fraud may be one of the largest frauds ever committed. But its status as a "computer crime" is much disputed.[62] The use of a computer increased the loss level, over a paper-and-pencil stock fraud, but did not change the essential nature of the crime. Equity Funding appears to be no more than a classic stock fraud.

Other often-cited examples of "computer abuse" (or "computer crime") also lack veracity when examined more closely. Round-off frauds, where a programmer programs a bank computer to round down the fractions of computed interest and credit them to his account, are probably fictitious.[63] It is impossible to steal a significant amount in this fashion and has never happened.[64] Yet, despite the spurious nature of such cases, SRI keeps them "in the file as real cases until proven otherwise." [65]

SRI justifies keeping "cases," despite their suspect or mythical nature, because they might be "plausible, indicate possible forms of computer abuse, or suggest types of computer vulnerabilities." [66] This is contrary to accepted standards of research. The accepted methodology requires that only proven cases be used in one's data base. Also, SRI's indexing of its files to reflect the varying status of each case is an inadequate remedy. SRI, itself, often fails to indicate the speculative nature of its work in published works.[67]

Given that the SRI study's loss figures vary so widely from the GAO study's, and that the data base of SRI is questionable, it is likely that the GAO study more close-

ly reflects the truth of the matter. As was noted prior,[68] the investigative agencies, which supplied the information for GAO's data base, are highly credible sources. Contrast this with SRI's sources of information: news clippings, excerpts from magazines and books, court proceedings, reports of law enforcement agencies, interviews with persons possibly involved, questionnaires from computer users, and documentation from anyone willing to report a possible case.[69]

The cases in SRI's collection are often no more than news clippings.[70] These are gathered by project staff members scanning the media, clips sent by intersted parties, and by the engagement of a newsclipping service. The newsclipping service collects all United States clips reporting non-violent crimes, suspected frauds, and civil suits. These are scanned for involvement, or likely involvement, or computers.[71] One must consider the facts. SRI keeps a "case" on file until proven not to have happened otherwise. The file is often called a "computer crime" file, despite the number of civil cases, and cases shown not to involve a computer.[72] The sources of the SRI study are of questionable validity. The criterion used to define "computer abuse" or whatever SRI actually is focusing its efforts on isn't well defined. Thus, the best that can be said of the "computer abuse" school is that the validity of conclusions drawn from the SRI study, concerning the "growing problem of computer crime," rests on a very shaky foundation.

II. THE "TOOL OR TARGET" SCHOOL

"Human beings have an amazing capacity to store contradictory information in separate compartments of their brains, allowing them to simultaneously hold beliefs that seriously conflict with one another."—Galen Rowell, In the Throne Room of Mountain Gods.[73]

The definition of the problem of crime, related to computers, is obviously much narrower than that defined by the "computer abuse" school of thought. Yet there still remains much disagreement on what the problem is. The "tool or target" school of thought is derivative of the SRI "computer abuse" school. Thus, it must explain its usage of both the SRI study's flawed data base and the SRI study's unreasonably loose usage of definitional terminology. That no explanation has ever been attempted is indicative of the level of critical thought attendant to this school.

The "tool or target" definition of this school of thought derives from the narrowing of focus of what the crime problem associated with computers really is. Instead of the broadly defined "computer abuse" used by the SRI study, several have suggested that the uniqueness of the "computer crime" problem results from the instances where the computer is used as a tool to commit the crime, and when the computer is a target of a crime.[74]

Despite serious questions on the validity of SRI's work, much activity has, nevertheless, issued, based on such a foundation. For instance, a bill is before Congress which would amend Title 18 of the U.S. Code. Introduced by Representative Bill Nelson on June 18, 1981, this proposal would make "a crime the use, for fraudulent or other illegal purposes, any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce." [75] Prior versions of this Federal Computer Systems Protection Act of 1981 died in committee.[76] Fourteen states have now computer abuse related laws. They are:

1 Arizona—October, 1978.
2 California—January, 1980.
3 Colorado—July, 1979.
4 Florida—August, 1978.
5 Georgia—April, 1981.
6 Illinois—August, 1979.
7 Michigan—March, 1980.
8 Minnesota—March, 1982.
9 Montana—March, 1982.
10 New Mexico—April, 1982.
11 North Carolina—January, 1980.
12 Rhode Island—May, 1979.
13 Utah—May, 1979.
14 Wisconsin—April, 1980.

The current spate of legislation reflects the problem of defining the focus of all this activity. There is no consensus on the definition of a computer.[77] And there is no clear focus on what the problem with computer is. The phrase "computer abuse" appears time and time again. In fact, a perusal of the plethora of literature on the subject reveals that there are at least 24 different terms used to describe what the problem is in relation to computer.[78]

Aside from the list of legislation, the list of published works based on the SRI study are legion. There is no precise dividing line between those who subscribe to the "computer abuse" school and those who subscribe to the "tool or target" school. Listed below is a limited sampling of books, professional journals, and other miscellaneous written works. The listing of them in the main text is deliberate. Many of these are highly respected sources, and have helped provide the basis for the perpetuation of the notion that the crime problem related to computer requires legislative action.

Books

Becker, Jay. The Investigation of Computer Crime.
Bequai, August. Computer Crime.
Becker, Jay. Computer Crime: Expert Witness Manual.
McKnight, Gerald. Computer Crime.
Parker, Donn B. Crime by Computer.
Practicing Law Institute. Computer Abuse.
Practicing Law Institute. Computer Abuse 1976.
SRI International. Computer Crime.
Whiteside, Thomas. Computer Capers.[79]

Professional Publications

ABA House of Delegates, Criminal Justice Section. Recommendations in support of federal computer crime legislation.
American Criminal Law Review. Computer Crime (1980).
American Criminal Law Review. Computer Crime (1981).
Becker, Louise. Computer Crime and Security (1982 update).
Bloombecker, Jay. The Trial of a Computer Crime.
Genigani, Michael. Computer Crime: the Law in '80.
Huston, Cynthia E. Computer Crime in the Future: Evolutionary and Revolutionary Risks.
Parker, Donn B. Computer Abuse Assessment (1975).
Parker, Donn B. Computer Abuse Perpetrators and Vulnerabilities of Computer Systems.
Parker, Donn B. Computer Abuse Research Update (1980).
Rivlin, Gary. Computer Crime.
Roddy, John. The Federal Computer Systems Protection Act.
Tunick, David C. Computer Law.
Volgyes, Mary R. The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Arts Review.

Miscellaneous

Committee on Government Operations, United States Senate. Problems Associated with Computer Technology in Federal Programs and Private Industry—Computer Abuses.
Koba Associates Incorporated. National Conference on Computer Related Crime Summary Report (1980).
Subcommittee on Criminal Justice, Committee on the Judiciary, United States Senate. Computer Systems Protection Act of 1979, S. 240 Hearing.
Subcommittee on Criminal Laws and Procedures, Committee on the Judiciary, United States Senate. Federal Computer Systems Protection Act, S. 1766 Hearing.[80]

Many cite Stanley Rifkin's theft of $10.2 million, and the Equity Funding Scandal in support of their thesis that there is such an entity as "computer crime." [81] Use of magnets to erase magnetically recorded data,[82] use of doctored blank deposit slips (placed in the bank's convenience bins) to credit funds to a criminal's account,[83] and boxcar thefts from the Pennsylvania Railroad [84] are also often-cited as incidents which suggest that legislative action is needed to protect computer systems. Unfortunately, they are all myths.

As was pointed out, the factual foundation upon which so much of this activity is founded is very weak at best. Parker concedes that most of the cases involving the use of magnets to erase data prove fictitious.[85] Recall that SRI considers an incident to be true until proven otherwise.[86] This could easily account for the status of the not-disproven. The doctored blank deposit slip stories follow the same pattern as the magnet erasing stories, as far as credibility goes. In fact, Magnetic Ink Character Recognition (MICR) printers sell for as much as $130,000.[87] MICR printing is expensive, technically demanding, and uses a special, magnetically sensitive ink. Banking

equipment capable of MICR printing contain counters so that unauthorized use can be easily detected.[88]

In the early 1970's, the bankrupt Pennsylvania Central Railroad had 217 boxcars, worth several millions of dollars, disappear. This incident is repeatedly cited to support the proposition that assets can easily be manipulated through the use of a computer, and the tracks of the perpetrator can easily be covered up through the manipulation of the same computer.[89] Unfortunately, for those who cite this incident, there was no computer involved. The boxcar thefts were perpetrated solely through the manipulation of manual records.[90]

As noted earlier, Rifkin's theft and the Equity Funding scandal are also a flimsy basis on which to justify legislative action against "computer crime." [91] However, the GAO study may provide an independent basis for justifying the view that the nexus between a computer system and its "tool or target" involvement warrants legislative action against the threat of "computer crime."

The GAO study netted 69 cases of what was termed "computer-related crime." In comparison with SRI's claimed incidents figures, GAO's seems remarkably low. Especially significant is that the federal government is the single largest user of computers in the world.[92] Also significant is that the government's uses of computers are no different from those of the private sector.[93] The GAO itself expressed puzzlement over the great discrepancy between its figures and those of the SRI study.[94] Surprisingly, GAO never questioned its basic assumptions about SRI's infallibility, nor about the actual seriousness of the threat of computer-related crime, nor about the extent of the threat of computer-related crime.

The GAO attempted to marshall some explanation for the discrepancy between its own study, and that of SRI. One explanation that was offered was that federal agencies do not customarily differentiate between computer-related crimes and other crimes. Another explanation was that yet undetected or unreported cases may exist.[95] While these rationales may justify some discrepancy, they do not explain away the fact that the average loss per incident in the SRI study is 10 times larger than that of the GAO. One must keep in mind the difference in the quality of the investigative sources between the two studies.

The GAO study, though better than the SRI study, is itself flawed. It demonstrates unquestioning acceptance of basic assumptions. It appears that GAO was trying to reach the idea that "computer-related crime" equals "computer-crime," and also jump on the bandwagon that proclaims that a new type of crime, "computer crime," exists.[96]

The GAO study's own report refutes the contention that a new type of crime has come into being. Of the 69 cases, a majority of 43 were simply false record entries.[97] These are fraudulent acts, regardless of whether the instrumentality of the act was an IBM typewriter, or a computer. It is no surprise, then, that the reporting agencies did not differentiate between these and other non-computer-related crimes.

Others of the offenses run in a similar vein. Nine involved no dollar loss. Their effect was different, such as involving an invasion of privacy.[98] Eleven more exclusively involved the misappropriation of output. This crime involved such incidents as misappropriating returned checks, and eliminating or altering notices designed to provide controls and balances.[99] Three exclusively involved the unauthorized or inappropriate use of facilities and supplies. Offenses under this category included developing programs on organizations' computers for outside sale, doing commercial service-bureau-type work for outsiders, using remote terminals for personal benefit, and duplicating files for sale.[100] Thus, it is obvious that the vast majority of the "crimes" involved behavior which could easily be charged within the parameters of the current legal structure.[101] Only four of the incidents exclusively involved destruction or alteration of information already contained by the computer.[102]

But it is these crimes, where the operator performs unauthorized processing or the programmer alters a computer program, that strike fear into the hearts of many. These types of crimes are what concern those who view the crime problem associated with computers exclusively when the computer is used as a "tool" to commit and even cover up the occurrence of the crime. This use of the computer as a "tool" will be examined, in its purest form, in the next section.[103]

III. THE "TOOL" SCHOOL

"The few pitons I left behind were carefully re-inserted by Rusty when he followed me up, since he distrusts any scaffolding he has not erected with his own hands."—Tom Patey, One Man's Mountains.[104]

The act of using a computer as a tool to perpetrate and cover up a crime embodies the essence of what makes a computer unique. There are certain characteristics

which distinguish a computer from a file cabinet, or other office furnishings. They are the speed of the transactions, the form and concentration of assets, the ease of transborder removal of assets, and the manipulability of the assets by a programmer (or operator).[105] The key element is the ease with which the assets associated with a computer can be manipulated.

John Taber is the only one to focus exclusively on this element of computers as the essence of what constitutes "computer crime." Taber defines true "computer crime" as incidents where a crime has, in fact, occurred and "in which a computer was directly and significantly instrumental." [106]

From this foundational definition, Taber notes that there are at least two examples of "computer crime." One is also one of the earliest criminal incidents, involving a computer, reported in the media.[107] In 1965, the National City Bank of Minneapolis computerized its checking accounts. The culprit programmed the computer to ignore overdrafts on his account. According to Computerworld Magazine, he stole $1,357.08. He was caught when the bank reverted to manual processing due to a computer failure. He had intended an extended "float" of his account balance, rather than a theft, but lost control. Soon, his overdrafts piled up to the point of not being easily coverable.[109]

The second incident Taber cites is the Flagler Dog track trifecta fraud.[110] In Florida, the Flagler Dog Track used two computers to compute odds and payoffs in trifecta betting. Because of the volume of the necessary computations and their time consuming nature (even for a computer), the dog race was often over before the calculations were finished. When an accomplice would communicate to the computer room the results of the race, the operator would immediately halt further execution of the computer program. At a console, the operator then "deducted" a number from the count of losers, and added that same number to the count of winners in computer storage. The computer was, then, restarted and the program was allowed to complete its computations. Later, the gang printed fraudulent winning tickets which other confederates cashed the next day. Because winners were paid from the pool of the losers' money, each winner simply got a bit less. The loss therefore appeared difficult to detect.[111]

While the "tool" school focuses on the key characteristics of computer systems which evokes visceral reactions, this does not mean that a new type of criminal act has emerged. Creating a new type of crime is logically inconsistent with Taber's own stance. As Taber himself points out, "it would mean defining offenses by the instrument of the acts, rather than by the acts themselves." [112] Perhaps Taber is suggesting that special consideration should be given to crimes where the instrumentality used to perpetrate it involves a computer and its special charcteristics. This would be analogous to felony laws which invoke higher penalties when a gun is used in the commission of a crime.[113] But the nature of the criminal act involved remains the same.

The best that can be said about the phrase "computer crime," then, is that it is a rallying point, a "buzz" word to describe such penalty enhancement concerns. Otherwise, as used by the "computer abuse" school, and by the "tool or target" school, the term "computer crime" is a "fuzz" word, obfuscating the real issues involved. The essence of computer-related crime is a management problem.

IV. THE "MANAGEMENT PROBLEM" SCHOOL

"All machines are amplifiers."—Cooper's Postulate to Murphy's Law.

Mankind makes mistakes. Machines amplify those mistakes. That is the essence of this perspective. Unfortunately, the mistakes made by business management can lead to a company's self-destruction, especially where a computer system is concerned.

The crime problem involving computers will not be solved by further "computer crime" legislation. In fact, efforts in this area detract from focusing attention on where it should be directed. If the "experts" are correct; if it is difficult to detect a crime involving a computer; then the deterrence value of a single statute prescribing the use of a computer as an instrumentality of the offense is minimal.[114] The core of the problem is a management one. Management is also where the core of the solutions lie.

There are two component parts to securing a computer system: prevention and detection. The three basic tenets of prevention are: (1) never alone, (2) limited tenure, and (3) separation of functions.[115] By "never alone" is meant the concept of not allowing free run of facilities. The Union Dime embezzlement is a classic example of failure in this area of security management.[116] When the concentration of information assets is so great that it affects the tangible monetary assets directly,

greater security measures were obviously needed. The fact that an $11,000-a-year bank clerk could steal more than $1 million after hours without even the possibility of challenge to his activities demonstrates failure of management to abide by a basic security concept.[117]

"Limited tenure" is the second tenet of prevention. The amount of time spent at a given task increases opportunity. This holds true especially with security personnel themselves. The security personnel might not become directly involved in the commission of a crime. However, the familiarity with company personnel, or boredom with the job, could easily lead to a relaxing of watchfulness.[118]

"Separation of duties" is the final tenet of prevention.[119] It seems likely that few companies separate programmer from operator functions.[120] It is this vulnerability which could lead to the scenario of a person manipulating the data base or the program itself to commit a crime the classic "tool" usage).

Auditing is one of the mainstays of detection once a crime is committed. The Flagler Dog Track trifecta fraud could not have succeeded without lax auditing.[122] In September of 1976, the Security and Exchange Commission issued a formal administrative order instructing the accounting firm of Seidman and Seidman to improve its auditing procedures. Seidman and Seidman was accused of negligence in auditing the books of Equity Funding. Although the actual fraud has been carried out by a client, Equity Funding, the SEC maintained that the audits were not carried out in accordance with generally accepted accounting procedures. Critical areas of the audits were carried out by inadquately trained personnel, and unwarranted reliance on management representations had taken place.[123]

Computer audit programs and other software security devices are becoming increasingly accepted. Levels of password access are now part and parcel of computer systems software.[124] Auditing procedures are being further enhanced by the inclusion of signal emitters built-in to remote terminals. Each remote manufactured would emit its own unique signal when switched on, and accessing a central computer.[125] Thus, the array of defenses combat the feared, anonymous penetration of a "mainframe" grows increasingly available.

The General Accounting Office recently published a report concerning the inadequate protection federal agencies have given and continue to give to computers and telecommunications.[126] The report concluded that many senior managers are not fully aware of how highly vulnerable their systems are. Also, even if management in federal executive agencies are aware of the vulnerability to deliberate or accidental losses, they are doing very little to implement information security programs.[127] The fact that management is doing little to protect information assets is evidenced by 1) the limited resources committed to risk analysis, 2) failure to define data processing operations in accordance with the Office of Personnel Management (OPM) criteria for personnel security programs, 3) failure to provide contingency and backup capabilities, and 4) failure to provide a separation of duties.[128] Yet the hue and cry has been that the problem is a criminal one requiring legislative action.

The evidence is mounting that the problem is actually a management problem. The various studies of "computer crime," as flawed as they are, all agree that programmers are seldom the perpetrators of criminal acts involving computers.[129] In fact, the culprit is usually a manager or data clerk.[130] Yet fear and hostility are expressed by the various federal agencies against the threat of crimes perpetrated by programmers.[131]

This paranoia against programmers is astounding, especially when one realizes that the Department of Justice's Bureau of Prisons currently operates a burgeoning data processing service.[132] This service employs programmers who happen to be convicted felons. Customers for this service have included the Department of Agriculture, Department of Commerce, Department of Defense, Department of Justice's Bureau of Prisons, General Services Administration, and the Internal Revenue Service.[133]

The contradiction is obvious. On the one hand, at one point the Department of Justice was asking for extremely broad statutory powers to cope with the threat of "computer crime." The argument was that "computer crime" is easy to commit and difficult to detect.[134] On the other hand, this same agency does not see anything wrong with persons convicted of serious offenses programming the agency's computers.[135] The truth is that "computer crime" is not easy to commit. The Department of Justice's Bureau of Prisons' computer programming program is a perfect example of this. In fact, an additional benefit of the program is that the recidivism rate of those in the prison programmer program is extremely low.[136]

Legislative sanctions to "unauthorized" uses of computer overreaches into common private industry practices. Such "unauthorized" uses include balancing checkbooks, charting stocks, writing unauthorized programs, and other such uses of

computer time. Other problematic uses include attempts by students to "crash" the systems.[137] Employers' views on "unauthorized" uses varies. Some flatly forbid non-business uses of a company computer. Others forbid the use in theory but do not police machine usage in practice. Others even go as far as "winking" at the practice. Still others permit the practice as a fringe benefit. In fact, many companies have never considered such usage to be a problem.[139] Thus, acts forbidden at one company may be fully encouraged at another.

Fears that student attempts to "crash" a university computer lead to criminality are without basis. Reports of a threatening, "newly" discovered method of accessing computer files graced the headlines recently.[140] The "newly" discovered method is supposed to be a simple yet effective method of breaking in to limited access files from a remote terminal. It was discovered by an unknown student at the University of California at Berkeley.[141] The source of these reports was SRI.

Aside from the general credibility hurdle, which SRI must overcome, there is a real issue of the "newness" of this discovery. SRI was reported to have notified the FBI, the National Security Agency (NSA), the Justice Department, and manufacturers about the problem. The NSA assumed a very ho-hum attitude toward SRI's announcement. To the NSA, this was simply another one of the class of vulnerabilities called trojan horses.[142] In fact, Colonel Robert Schell, deputy director of the NSA's computer security evaluation center, explained that the particular method that SRI finds so disturbing was discovered independently by the Air Force in the early 1970's.[143]

Taber notes that professors themselves encourage students to attempt to "crash" the system. Aside from the fact that the victim is usually a student system (not used for university business) this custom serves two important purposes: it teaches students the need for system reliability and aids research, using free, willing labor to test to the reliability of a system against a sustained, ingenious attack.[144] When the switch is made from the academic environment to the professional one, the person's priorities change also. Instead of attacking the computer, the former student applies his or her skills to protecting the system and keeping it going.[145] The fact that programmers are so seldom involved in criminal incidents where a computer is involved is evidence that Taber's proposition is largely correct.

Accepting for the sake of argument that financial institutions and other large computer users do not report "crimes" because of fear of damaging business reputation or confidence, one must, then, also accept the fact that legislation is not the answer.[146] The passage of the Florida "computer crime" bill, one of the earliest state bills, has not resulted in any prosecutions under the new law.[147] There are three possible explanations: 1) institutions are not reporting for the above stated proposition, 2) prior, existing laws were adequate to handle the situation (thus, the new one isn't used), or 3) there is no such thing as "computer crime" (thus, no prosecutions).[148] Accepting any, or all, of these propositions can only lead one to the conclusion that the problem is a management one, and not a legal one.

Given the concentration of assets contained in present-day computer systems, and given the fact that the vulnerabilities of a computer can be guarded against, management's failure to take adequate precautions is appalling. Turning a blind eye to the potential risk of loss does not solve the problem. Acknowledging the risk of loss problem, but failing to take any corrective action, is absurd. Blaming computer technology for posing a threat is the easy way out which has been taken in the past. It is so much easier to point to the abstraction of "computer crime" or "computer abuse" and say that that is where the problem lies. In actuality, it is the people and the policies implementing computer technology that are the true culprits. It is time for business management and the legal regime to put aside its awe and face the problem squarely. Past policies of lax security management must give way if this important technology is to fulfill its proper function as a tool to serve the benefit of mankind.

"Rockfall, waterfall, icefall, avalanche: the climber must deal with each in turn or become their victim. Knowledge is power is life."—Yvon Chouinard, Climbing Ice.[149]

Computer technology has raised controversial, new issues. But the problems are unlike what so many perceive them to be. The problems are not with a new type of crime. The crimes committed with the aid of a computer still remain the classical crimes of fraud, theft, destruction of property, et cetera. The tool used to help perpetrate them may have changed, but the acts themselves remain the same. Instead of new laws trying to reach the mythical entity, "computer crime", the legal community should concentrate on fine-tuning the existing body of law.[150] The efforts aimed at computer "abuse," "fraud," "crime," et cetera, are misdirected efforts.

A current problem area in computer technology is the area of software protection. Recently, theft statutes have been expansively interpreted to encompass computer

software as a "thing of value," a sign of the judiciary upgrading its understanding of the nature of computer assets.[151] Legal sanctions remain an after-the-fact remedy of the problem, however.

Such problems actually reflect the neglect of a primary responsibility of business management.[152] Assets so greatly concentrated in location, and so movable, must be better protected than they have been. Rifkin's theft and the Equity Funding scandal have demonstrated that better security management and better accountability are needed in this computer age.

The Equity Funding scandal, alone, raises a fearful specter. Solzhenitsyn pointed out a growing problem of cracks in the veneer of western civilization.[153] When management itself perpetrates a crime, no true accountability can exist. If Equity Funding-type scandals become more than a weak undercurrent, civilization as we know it might cease to exist.

An underlying criticism of much of the scholarship which has gone before is the "mind set" which has been demonstrated by so many. Parker and SRI must be rightfully credited for alerting the public to the existence of problems associated with computer technology. However, the way in which this problem with computer-related crime has been characterized by so many, including Parker, leaves much to be desired. Solzhenitsyn once noted that in the United States "scholars are free in the legal sense, but they are hemmed in by the idols of the prevailing fad." [154] The schools of "computer abuse" and "tool or target" have proved Solzhenitsyn right, unfortunately. The blind reaction of so many in the legal community that "there ought to be a law" further exemplifies Solzhenitsyn's point.

The blind acceptance of newspapers as a scholarly source should have triggered the warning bells. Originally, the phrase "computer crime" was a buzz phrase used to catch the eye of a person reading popular media. From its beginnings, "computer crime" has become an entity with a life of its own; though no computer has ever committed a crime.

Artificial intelligence (simulation of human thought) research has added new dimensions to the crime problem related to computers. True "computer crime" [155] requires a computer to form the necessary "criminal intent" in order to be legally culpable for a criminal act.[156] The formulation of criminal intent of a computer seems to be a highly unlikely event.[157] But developments in the field of artificial intelligence may prove things otherwise.

Speed of computer processing will undoubtedly increase.[158] The capacity for analytical thought, formerly a characteristic thought to separate mankind from other life forms, is part and parcel of modern computers. Computers are being developed which will employ "hunches" instead of following a line of thought to its logical end. Thus, creative thought is coming within reach of computer technology.

The disturbing questions which artificial intelligence research has precipitated are just now being asked: do we need all of this technology? what limits might need to be imposed upon it? what are the social costs, long and short-term? Answers to these questions and ways of dealing with the dilemmas they pose have not been found.

Thus, at this time, considering the unchecked, explosive developments in the realm of artificial intelligence, the best one can say is that there is no such thing as "computer crime"—yet.

APPENDIX

THE LEGAL COMMUNITY'S RESPONSE TO COMPUTERS AND CRIME

A. The Judicial (Criminal Justice) System

An overview of the judiciary's response to computers and crime reveals a growing awareness of the true parameters of the problem. Despite initial skepticism,[159] application of existing statutes has been shown to be sufficient to meet the problems posed by computer technology.

Case law is often used to support the proposition that crimes involving a computer are difficult to prosecute. The two cases most frequently cited for this proposition are Ward v. California [160] and U.S. v. Seidlitz.[161]

In Ward, the defendant was indicated for theft of a trade secret and grand theft. Ward has accessed a computer source program by using a remote terminal. Defendant Ward moved to dismiss the charges. His motion was based on the argument that a lack of probable cause to believe that the program was a trade secret within the meaning of the statute prohibiting theft of trade secrets. Ward also moved to a dismiss based on a lack of probable cause to believe the program was property within the meaning of the grand theft statute. Both motions were denied.[162]

Sufficient facts demonstrated that the program was safeguarded carefully, as is required for statutory trade secret protection. The area of conflict lies with the court's interpretation of the word "article". The trade secret act required a carrying away of the "article". The court, in dicta, said that the "article" must be a tangible "article" to fall within coverage of the statute. Impulses transmitted over telephone lines are not tangible, according to the court. Thus, impulses do not constitute an "article."

Those who have pointed to this particular passage as an example of a shortcoming in criminal statutes note that probable cause existed only after it was believed that Ward made a (tangible) copy and carried it to his office.[163] This carrying to his office provided the necessary asportation, of a tangible item.[164] The proclaimed shortcoming is the requirement of a 1) tangible copy 2) carried somewhere. However, ths simple making of a copy, irrespective of any asportation, established a theft-of-trade secret violation.[164] Ward did not have to take a copy to his office for a violation to have occurred, as so many suppose was necessary. However, if Ward had simply displayed the source program on a Cathode Ray Tube (CRT) and made a program with significant modifications, no tangible copy would have needed to be made. Clearly, the transmitted impulses had value. This gap in the court's rational points to the need to midify the statute involved or the judicial thinking involved. However, this situation does not point to a need for broad "computer abuse"-type legislation.

U.S. v. Seidlitz is pointed to as an example of stretching existing law to meet the new demands on the legal system, resulting from burgeoning use of computer technology. Seidlitz involved a private firm's program rented to the Federal Energy Administration (FEA). The firm's source program was copied from the FEA's computer in Maryland by use of a remote terminal in Virginia. The fact is that Seidlitz was prosecuted and convicted of wire fraud.[165] Thus, the difficulty in prosecuting under federal law is overstated.

Taber notes that the federal prosecutor's real difficulty was jurisdiction.[166] There was ample evidence to support the finding that the program was "property".[167] Though similar programs existed, evidence that the private firm had 1) invested substantial sums to modify the program, and 2) that the firm enjoyed a multi-million dollar competitive advantage because of it, and 3) that the firm took steps to limit access to the program permitted a finding that the pilferred program was property of the firm.[168] These three characteristics could have easily been proof of the offense of theft of trade secret, a state offense.

Further criticism is that "wire fraud" was a roundabout way of prosecuting the offense. Section 641 of the U.S. Code forbids theft of public money, property or records.[169] Any misappropriation of software in the custody of the government is a violation of Section 641.[170] "The prosecutor erred in a couple of ways, and it isn't really fair of him to blame the computer for his errors."[171]

In addition to the Fourth Circuit in Seidlitz allowing software to be considered as property, several other courts have recognized computer software as "property". Prior to Seidlitz in 1967, the Fifth Circuit allowed the definition of property as a "thing of value".[172] This decision was ahead of its time. (Seidlitz was decided in 1978, when the novelty of computers had begun to wear off).

In 1978, two U.S. district courts upheld the "thing of value" definition.[173] In fact, one of the decisions specifically dealt with the use of computer time and computer capacity.[174] In 1979, the Second Circuit upheld a statute making unlawful the sale, without authority, of any "record or thing of value". The court declared this provision not unconstitutionally vague or overbroad.[175]

Thus, it can be seen that a trend is emerging. As familiarity with computers increases, the awe of such tools decreases. Familiarity with computers is a factor in the perspective one views computer technology from. Are computers a mysterious "black box" with unlimited powers, or a tool with the capacity to benefit mankind? Have computers been in existence only about twenty-five years, thus retaining status as a novelty, or have they been around over a quarter of a century, in existence longer than many humans? More than anything, the judicial response to computer technology has mirrored the changing perspective toward this technology. It is heartening to note that the judicial response reflects both a growing understanding of computer technology and the necessary flexibility to deal with the problems of this fast-evolving technology.

B. The Legislatures

There are over forty statutes establishing federal jurisdiction over various aspects of computers and crime.[176] Despite this vast array, many minimize such, saying that there is a need for specific statutory sanctions against "computer crime". The

fundamental flaw of those who desire specific sanctions lies in defining an abstraction computer "crime", "abuse", "fraud", etc. as a specific offense.

The case law, as noted in the prior section, demonstrates the effective use of criminal statutes already available. In fact, a broad federal statute intrudes in an area of law already governed by the states. The states have control over the prosecution of most such criminal acts already. The Legislative Resource Manual, published by Koba Associates, Inc., catelogues a vast array of statutes available to prosecute crimes involving computer systems.[177] The array includes both the federal and state levels of government.

One wonders why all this activity exists to push through the passage of broad "computer crime"-type bills. As the Chairman of the Board of National District Attorney Association, Lee Falke, pointed out, legislative efforts evidence of the government's "insatiable thirst for power."[178] Perhaps this "thirst for power" is what the whole spate of "computer crime"-type activity is really all about.

FOOTNOTES

[1] A. Solzhenitsyn, Solzhenitsyn at Harvard (Berman, Ronald, editor) (1980). From the Harvard commencement speech: A World Split Apart.

[2] C. Alexander, "Crackdown on Computer Capers," TIME February 8, 1982. When one should use the term "computer abuse," "computer crime," or "computer-related crime." This author uses the term "computer-related crime" to denote what others have been calling "computer abuse," "computer crime," "computer fraud," etc. In other words, any criminal act involving a computer, however tangential the involvement, is "computer-related crime." "Computer crime" is defined by this author as those criminal acts perpetrated by a computer, where the computer, itself, has "criminal intent." See Jafin, note 152. A warning: as noted in the text, these same terms are used loosely by many to mean a host of different things. "Computer abuse" is considered a "fuzz word" with no real meaning. The term does conjure up images of a demented programmer wearing leather pants, whipping a main frame IBM computer with a shiny chain.

[3] G. Rivlin, "Computer Crime," Student Lawyer vol. 10 no. 6 (Feb. 1982) (Hereinafter cited as Student Lawyer)

[4] L. Tell, "Firms Face Computer Theft Issue," National Law Journal vol. 4 no. 24 (Feb. 22, 1982).

[5] P. Hilts, "Computer 'Break-in' Method Poses Big Crime Risk," Washington Post sec. A page 13 (March 4, 1982). Science magazine had a similar article; Kolata, Gina, "Students Discover Computer Threat," Science vol. 215 no. 4537 (March 5, 1982).

[6] L. Becker, "Computer Crime and Security," Library of Congress Congressional Research Service Issue Brief #IB80047 (originated April, 1980, updated March, 1982) (Hereinafter cited as CRS Issue Brief).

[7] GAO, Federal Information Systems Remain Highly Vulnerable to Fraudulent, Wasteful, Abusive and Illegal Practices, Masad-82-18 (April 21, 1982) (Hereinafter cited as GAO Report '82).

[8] of 1982. (Hereinafter cited as CBEMA 2nd Report).

[9] This is published by CBEMA (the Computer and Business Equipment Manufacturers Association) 5 times a year. (Kaufman, Lloyd S., editor, Bush, Cheryl, associate editor), at 1. No page numbers are printed. For the purposes of this paper, this author counts the pages sequentially starting from the first page inside the front cover.

[10] H.R. 3970, introduced June 18, 1981—to amend title 18 of the U.S. Code.

[11] CBEMA 2nd Report, supra notes 8, 9, at 8.

[12] ACLR is the quarterly-published journal of the Criminal Justice Section of the American Bar Association (ABA). It is the third most widely circulated legal periodical in the country. For the past several years, in the fall white-collar crime issue, a section on "computer crime" has been included.

[13] L. Terray, Les Conquerants De L'Inutile (The citation for this source was missing at the time of printing).

[14] J. Taber, "A Survey of Computer Crime Studies," 2 Computer/Law J. 275, 287. (Hereinafter cited as Taber Survey).

[15] D. Parker, S. Nycum, & S. Oura, Computer Abuse 7, 77-80. (Stan. Research Institute Report 1973); D. Parker Computer Abuse Assessment 15 (Stan. Research Institute Report 1975); D. Parker Computer Abuse perpetrators and Vulnerabilities of Computer Systems (Stan. Research Institute Report 1975). Also, in 1979, SRI (Stanford Research Institute) prepared Computer Crime for the U.S. Department of Justice (hereinafter Crim. Just. Manual).

[16] The Taber Survey did likewise. The reason this author does so is because of the continuous use of SRI's files by Parker over the years. The data base used in the 1973 study has simply been built upon. (see p. 288 Taber Survey and p. vi of the Crim. Just. manual supra note 15. Also, D. Parker, "Computer Abuse Research Update," 2 Computer Law 3 329 (1980) (Hereinafter cited as 1980 Update).

[17] Crim. Just. Manual, supra note 15; see also Hearing Before the Subcommittee on Criminal Justice of the Committee on the Judiciary U.S. Senate 96th Congress, 2nd Session, on S. 240 (Feb. 28, 1980). (Hereinafter cited as SB 240 hearings). The Taber Survey, supra note 14 at 287, indicates that there are other reports by SRI. Also, Parker has written the popular press book Crime by Computer (1976) (Hereinafter cited as Crime by Computer).

[18] see supra note notes 2, 3, 5.

[19] see Computer Abuse 7 supra note 15, at 3. See also Federal Computer Systems Protection Act: Hearings on S. 1766 before the Subcommittee on Criminal Law and Procedure, Senate committee of the Judiciary, 95th Congress, 2nd Session (1978) (testimony of Donn B. Parker.).

[20] Computer Abuse 7, supra note 15, at 4.

[21] Id.

[22] Taber Survey, supra note 14, at 288.

[23] Crime by Computer supra note 17, at xi.

[24] Taber Survey, supra note 14, at 289 (footnote 62).

[25] Id. at 259. "Apparently, SRI's interest was crime, but its researchers were not formally qualified to conduct criminological studies." Id.

[26] "Such as in its seminar and consulting advertisements, its press releases and newspapers." Id.

[27] Id.

[28] Abuse was defined by SRI as any "intentional act in which one or more victims suffered or could have suffered a loss and one or more perpetrators made, or could have made a gain. The incident must be associated with computer technology or its use." Computer Abuse Assessment, supra note 15, at 3.

[29] Crim. Just. Manual, supra note 15, at 3.

[30] Taber Survey, supra note 14, at 288. In fact, as noted in Part B of this section, the factual foundation for classifying some cases as "computer crimes" is without basis in fact, even under Parker's broad definition.

[31] see infra Part B, at 7.

[32] Taber Survey, supra note 14, at 289. Also, 1980 Update, note 16, at 329. "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." (emphasis added). The title of the Crim. Just. Manual is "Computer Crime," yet, within the manual, Parker distinguishes "computer crime" from "computer-related crime," and says the Manual is about the latter. Crim. Just. Manual, supra note 15, at 3.

[33] Crime by Computer, supra note 17, at 294.

[34] 1980 Update, supra note 16, at 333.

[35] see infra Part B, at 7. Also, the section on the "Tool" perspective, infra, at 19, and the "Management" perspective, infra, at 22. It is sufficient to note, at this point, that the problem with SRI's work is not limited to the problem of defining the criteria used to identify the crime problem associated with computers. The arbitrary inclusion and exclusion of "cases" also must be considered in evaluating the SRI study.

[36] Crim. Just. Manual, supra note 15, at 370.

[37] 1980 Update, supra note 16, at 334. Also, Taber Survey, supra note 14, at 297.

[38] 1980 Update, supra note 16, at 333.

[39] Taber Survey, supra note 14, at 297. Also, Parker gains recognition and financial renumeration from the various publications and derivative congerences. This introduces the possibility of bias.

[40] It is difficult to decide whether to use "SRI" or "Parker." Often, Parker has cited to SRI's work, as if he were not associated with SRI. The interplay has helped to cloud the credibility of both. This monograph will use the names interchangeably, since by all appearances one has equaled the other after the first Computer Abuse report.

[41] U.S. Chamber of Commerce, A Handbook on White Collar Crime 4-6 (1974).

[42] Crime by Computer, supra note 17, at 29-30. This figure is based on several assumptions: that one hundred cases will be reported each year, that these reported cases constitute 15% of all computer-related crimes per year, and that there is an average loss of $450,000 per case.

[43] Many, adhering to the school that says "computer crime" exists, also adhere to the school that says what is known about losses represents only a tip of the iceberg. Parker inserts in the second paragraph of the 1980 Update the sentence, "The United States Chamber of Commerce estimates that losses from business, economic, and white-collar crime may cost more than $40 billion per year." 1980 Update, supra note 16, at 329. The Congressional Research Service published an issue brief which ties the $40 billion loss figure to "computer abuse." CRS Issue Brief, supra note 6, at 1. The CRS Issue Brief draws the inference of "computer abuse" as a subspecies of white-collar crime, despite the fact that many non-criminal matters fall within the parameters of "computer abuse." One author writes that it is believed that "computer crime" costs the public at least $10 billion annually. D. Tunick, "Computer Law," 13 Loyola L.A. Law Rev, at 326. It is interesting to note that the context of Parker's statement (above) did not focus on white-collar crime. Instead, it focused on the purposes of the SRI study. Yet, sandwiched between two sentences mentioning "computer crime" is this irrelevant sentence on white-collar crime losses of $40 billion, which becomes tied to "computer abuse"-caused losses.

[44] "Computer Crime" 18 ACLR 370, 371 (1980) (part of the "White-Collar Crime Survey"). ACLR defines "computer crime" as "the intentional use of a computer for fraudulent or illegal purposes." Id. at 372.

[45] Crim. Just. Manual, supra note 15, at 1, 3-16, among others. This type of fraud, also called the "salami technique," has been reported to the point of being considered the gospel truth. The actual threat of such a threat is minimal, at best. See Taber Survey appendix, supra note 14, at 311.

[46] Student Lawyer, supra note 3, at 16.

[47] The list of those who do is legion. For a truncated list see infra main text, at 14-15.

[48] Taber Survey, supra note 14, at 288.

[49] General Accounting Office, Computer-Related Crimes in Federal Programs (1976) (Hereinafter cited as GAO Report) at 20, 24 (note A). The median was $6,749. Taber Survey, supra note 14, at 282.

[50] Taber Survey, supra note 14, at footnotes 38 and 42.

[51] GAO Report, supra note 49, at 20.

[52] "Computer-related" crime was defined as "acts of intentionally-caused losses to the Government or personal gains to individuals related to design, use, or operation of the systems in which they are committed." *Id.* at 1.

[53] Practicing Law Institute, Computer Abuse 1976, at 9.

[54] See supra section I. A., The "Computer Abuse" School (page 3). The SRI study includes noncriminal matters.

[55] Taber Survey, supra note 14, at 292. Other incidents involve offenses where precisely the lack of a computer is the "offense."

[56] 18 ACLR 370, at 371. The concentration of assets, the speed of the transaction, the ease of transborder removal of assets, and the special manipulability of the assets by a computer are pointed to as a characteristic of computer technology which warrant concern.

[57] U.S. District Court, Central District of California, *U.S.* v. *Stanley Mark Rifkin,* Criminal Action #78-1050-WMB, Reporter's Transcript of Proceedings (February 22, 1979) (Honorable Wm. Matthew Byrne, Presiding), at 35, 36. (Hereinafter cited as Ct. Transcripts).

[58] J. Taber, "On Computer Crime (Senate Bill S. 240)", 1 Computer/Law 517, at 518-519 (footnote 8) (hereinafter cited as Taber S 240).

[59] Ct. Transcripts, supra note 57, at 24, 25.

[60] Id. at 38, 39. $10 million was the principal for buying the diamonds. $200,000 was the broker's commission. Rifkin had used the name Mike Hanson, a non-existent bank officer. Another myth which has been popularized is that the diamonds were "russian" diamonds. This notion conjures up cloak-and-dagger action, adding to the mystique of Rifkin's theft. In actuality, the seller's name was Russalmaz, a diamond seller in Zurich, Switzerland. Id. at 30, 31.

[61] Taber Survey, supra note 14, at 218, 219.

[62] Id. at 219, and footnote 13.

[63] CRIME BY COMPUTER, supra note 17, at 114.

[64] See Taber Survey, supra note 14, at 294 and entire Appendix. Taber proves mathematically the impossibility of stealing the large amounts claimed to have been lost to the "roundoff" scame.

[65] D. Parker, Computer Abuse Assessment (1975), at 10.

[66] 1980 Update, supra note 16, at 335.

[67] In the Crim. Just. Manual, Parker makes the statement that "based on a study of 669 cases of computer-related crime over the past 20 years, the incidence of computer-related crime is increasing rapidly." Crim. Just. Manual, supra note 15, at vi. (Contra: "A study of 669 reported cases of computer abuse over the past 8 years. . . ." Id. at 3) (emphasis added). Taber voices the suspicion that SRI uses the term "computer abuse" strictly on formal occasions, such as reports to the NSF. Other terms are used glibly in SRI's more public appeals, such as press releases, and conferences. Taber Survey, supra note 14, at 289. The loose usage of terminology appears to carry over to the loose usage of the SRI data base.

[68] See supra page 8.

[69] 1980 Update, supra note 16, at 336. This author has deliberately noted the "possibleness" of such case. Too often they are readily accepted as "fact."

[70] Id.

[71] Id.

[72] Id. at 337. "We have loosely called the computer abuse file 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."

[73] From the chapter, "Extreme Climbing," at 115.

[74] S. 240 sec. 1028. This bill is a good point of focus since it is the grandfather of all of the existing "computer crime" legislation. The "tool" use of a computer is concerned with schemes or artifices to defraud or obtain money, property or services. These must be accomplished through the data manipulation capability of the computer. See supra footnote 56. The "target" side involves altering, damaging, or destroying any element of a computer system. S. 240 sec. 1028(A)(B). See infra footnote 159.

[75] H.R. 3970 (Introduced by Rep. William Nelson, Fla.). Referred to the Judiciary Subcommittee on Civil and Constitutional Rights 6/18/81. Referred to the Subcommittee on Civil and Constitutional Rights 6/24/81.

[76] Senate Bill S. 240 (introduced by January 25, 1979) and the virtually indentical S. 1766 (introduced June 27, 1977) were both proposed by Senator Abraham Ribicoff of Connecticut.

[77] If one lights the definition of a "computer" to the central processing unit (CPU), then the input and output (in whatever forms), the software (i.e. source and user programs), terminals, user manuals and procedures, and support services (which are often included as part of the package when a "computer" is sold) are obviously excluded. Some state statutes define "computer" so broadly that even pocket calculators are included.

[78] C. WAGNER, THE CPA AND COMPUTER FRAUD (1979). They are: computer abuse, computer-assisted fraud, computer-based fraud, computer capers, computer crime, computer crooks, computer-directed fraud, computer embezzlement, computer fraud, computerized fraud, computer-managed fraud, computer-oriented, computer-related crime, computer-related fraud, computer swindler, computer theft, computer theft, embezzlement by computer, fraud in EDP systems, operator fraud, programmer fraud, stealing by computer, steal via computer, and theft by computer.

Id. at 32.

[79] J. Becker, The Investigation of Computer Crime (1980); A. Bequai, Computer Crime (1978); J. Becker, Computer Crime: Expert Witness Manual (1980); G. McKnight, Computer Crime (1973); D. Parker, Crime by Computer (1976); Practicing Law Institute, Computer Abuse (1975); Practicing Law Institute, Computer Abuse 1976 (1976); SRI (Stanford Research Institute), International, supra note 15; T. Whiteside, Computer Capers (1978).

Collateral publications include: Koba Associates, Inc., Computer Related Crime Legislative Resource Manual; C. Warner, The CPA and Computer Fraud (1979).

[80] ABA House of Delegates, Section of Criminal Justice Recommendation in Support of federal computer crime legislation (August 1979); "Computer Crime," 18 ACLR 370 (1980) (survey); "Computer Crime," 19 ACLR 499 (1981) (survey); L. Becker, "Computer Crime and Security," Congressional Research Service Science Policy Research Division, Issue Brief #IB80047 (3/17/82 Update); J. Bloombecker, "The Trial of a Computer Crime," Jurimetrics, Volume 21, Summer 1981, Number 4 (reprinted from Computer/Law J., Volume II, Spring 1980, Number 2); M. Gemignani, "Computer Crime: The Law in '80,"13 Indiana L. R. 681, (1980); C. Huston, "Computer in the Future: Evolutionary and Revolutionary Risks," Congressional Research Service Futures Research Division (reprinted from the Future of Risk, 1978); D. Parker, see supra note 15, 16 for all three; Student Lawyer; J. Roddy, "The Federal Computer Systems Protection Act," 7 Computers, Technology and L.J. 343 (1980); D. Tunick, "Computer Law," 13 Loyola L.A.L. Rev. 320 (1980); M. Volgyes, "The Investigation, Prosecution, and Prevention of Computer Crime: A State-of-the-Art Review," 2 Computer/Law J. 385 (1980); (see also S. Nycum, "Legal Sanctions to Computer Abuse," Assets Protection, Volume 2, Winter 1977, Number 2; Committee on Government Operations, United States Senate, Problems Associated with Computer Technology in Federal Programs and Private Industry—Computer Abuses, 94th Congress, 2nd Session (June 1976); Koba Associates, Inc., National Conference on Computer-Related Crime Summary Report (1980); Subcommittee on Criminal Justice, Committee on the Judiciary, United States Senate, Computer Systems Protection Act of 1979, S. 240 (hearings), 96th Congress, 2nd Session (February 1980); Subcommittee on Criminal Laws and Procedure, Committee on the Judiciary, United States Senate, Federal Computers Systems Protection Act, S. 1766 (hearings) 95th Congress (June 1977).

[81] For the sake of manageability, individual source cites are excluded. Further, the author reminds that the above listings are a limited sampling. The sampling is representative of a greater bulk of materials available. Also, it should be noted that several of the authors feed off of themselves, and the others listed. Parker, for instance, has written books, articles, spoken at conferences, and given testimony before several legislative bodies, including the U.S. Senate. Sometimes, he has referred to his own earlier writings as "by SRI," which has undoubtedly helped to cloud the waters.

[82] 1980 Update, supra note 16, at 336. The usual story is that exuberant boy scout troops have toured computer centers through the United States, waving their magnets and erasing tape records.

[83] The story usually is that some person has printed their own magnetic ink character recognition (MICR) account number on otherwise blank deposit slips. This person then places the slips in the bank's convenience bins. Customers without their own deposit slips use the doctored slips. The machine which then processes the MICR deposit slips reads the doctored MICR number and credits the person's account. After a few days, this person withdraws a large sum, and disappears into the mists forever. There are the usual variations on the theme.

[84] Fed. Computer Sys. Protection Act S. 1766 Hearings (1976), at 2. (Statement of Sen. Joseph Biden, Jr.); Id. at 18 (Statement of Sen. Charles Percy).

[85] 1980 Update, supra note 16, at 336. This was a "project finding."

[86] See supra pages 9-10 of the text.

[87] Taber Survey, supra note 14, at 395.

[88] Id.

[89] According to Whiteside, supra note 79, at 36, the deputy chief of a federal crime force investigating the incident concluded that the computer program had been manipulated to divert the box cars (another case of the "blame the computer" syndrome). How often it is heard that "the computer fouled up again," ignoring the role of the programmer or operator.

[90] Taber S240, supra note 58, at 519.

[91] See supra pages s. 8-9 of the text, dealing with Rifkin and Equity Funding.

[92] General Accounting Office, "Managers Need to Provide Better Protection for Federal Automatic Data Processing Facilities," reprinted in Committee on Government Operations, Problems Associated with Computer Technology in Federal Programs and Private Industry, "Computer Abuses," 94th Congress, 2d Session (June 1976), at 93, 97. (Hereinafter cited as Government Operations Report).

[93] GAO Report, supra note 49, at 8.

[94] In reference to SRI's figures, GAO stated that "we don't know why the average losses in detected government cases are similar than those in the private sector." Id. at 7. SRI reported 300 plus cases at the time, compared to GAO's 69. Further, GAO had an average loss per incident of $44,000 compared to SRI's $450,000.

[95] Id. at 2.

[96] As Taber notes, commentary in the GAO Report cites cases not on its list, including a $7 million loss borrowed from SRI's cases. Taber Survey, supra note 14, at 284. See also GAO Report, supra note 49, at 2. In reference to incidence rates, the report states that "they do not represent all the computer crimes . . . since agencies do not customarily differentiate between computer-related and other crimes," (emphasis added). It appears GAO's pairing of "computer crimes" to "computer-related" crime is much like SRI's coupling of "computer crimes" to "computer abuse."

[97] GAO Report, supra note 49, at 22-24 (see charts). Defining such acts by their instrumentalities would mean that one would have to provide for "file cabinet" crime, if a file cabinet were involved. Simply because the record-keeping is automated doesn't change the essential nature of the act.

[98] Id. at 23, 24. 8 involved such offenses exclusively.

[99] Id. at 7, 23, 24.

[100] Id.

[101] Id. Several others were mixed incidents involving more than one of the several types of incidents classifications.

[102] See Appendix, infra page 32, on the legal community's current handling of computer-related crime questions. It seems apparent that as the legal community becomes more familiar with computers, the anomalous decisions like U.S. v. Seidlitz (infra Appendix) become less of a problem.

[103] Because the "tool" segment of the "tool or target" school is so closely tied to such a weak factual foundation, it seems better to examine the possible, independent foundation upon which it can be based.

[104] T. Patey, One Man's Mountains (published posthumously, 1975).

[105] See supra footnote 56. The various works listed in section 3 list one or more of these factors.

[106] Taber Survey, supra note 14, at 298.

[107] Id.

[108] Id.

[109] Id.

[110] SRI case #77322. This case is well-documented independently of SRI.

[111] Id. Lax auditing prevented the dog track officials from detecting the loss. In actuality, the investigator solved the case within 3 days. See SB 240 hearings, supra note 17, at 40 (statement of John Taber).

[112] Taber Survey, supra note 14, at 297.

[113] See Appendix for a brief survey of the handling of computer-related questions, by various courts. The question which is repeatedly begged concerns the sentencing aspect. Should computer-related crimes be treated as special because of the special characteristics of computers? (See supra footnote 56). It has been suggested that this factor be given consideration at sentencing. SB 240 Hearings, supra note 17, at 55 (statement of Lee Falke).

[114] See the ABA House of Delegates, Section of Criminal Justice Recommendation in Support of Federal Computer Crime Legislation (1979) (hereinafter cited as ABA Recommendation), at 5, where the justification for such legislation is for its deterrent effect. The "deterrence" concept has little value, especially if it is so difficult to detect "computer crime." cf. J. Carroll, Computer Security (1977), at 36.

[115] K. Rynne, "Prevention of Computer Crime," (seminar presentation; Georgetown University Law Center, April 14, 1982) (hereinafter cited as Rynne Presentation).

[116] Whiteside, supra note 79, at 19-25. Also, Student Lawyer, supra note 3, at 16, 17.

[117] Id. See also J. Carroll, Computer Security (1977), for an excellent overview of security management considerations.

[118] Rynne Presentation, supra note 115, .a.

[119] Actually, there are other aspects of prevention, such as password controls, encryption of data, limitation of physical access, etc.

[120] A trend for smaller businesses to combine resources, and buy their own "mainframe" computer. A single person is hired for the position of programmer/operator, for the entire consortium. T. Conover, Programmer, California State Universities system (February 21, 1982). Mr. Conover is also associated with South West Research Laboratories, Inc. (Hereinafter cited as Conover Interview).

[121] "Crime" is used here in the common, generic sense, of an actual offense, regardless of how the legal system disposes of it.

[122] Taber S240, supra note 58, at 523 (footnote 39).

[123] Whiteside, supra note 79, at 61. While the author is hesitant to use a "popular" source like Whiteside, independent documentation of this point is not liable at this time.

[124] C. Alexander, "Crackdown on Computer Capers," Time (February 8, 1981), at 61, 62. Several Accounting firms are moving into the auditing software field.

[125] Conover Interview, supra note 120.

[126] GAO Report 82, supra note 7.

[127] Id. at 23.

[128] Id. at 23.

[129] Taber S240, supra note 59, at 528. Examine, also, SRI's data in the various reports over the years.

[130] Id.

[131] Id. See also the various manuals put out by the Department of Justice, GAO, and others. See supra footnotes 79, 80.

[132] Id.

[133] Id.

[134] Id. at 529.

[135] Id. This apparently includes programming sensitive accounting applications. The Navy allows female convicts to perform data entry services (at Alderson, West Virginia and Terminal Island, California). The Navy's use of convicted persons also seems anomalous, especially since the GAO Report said that false data entries were the most prevalent type of offense by far.

[136] Id. at 530. A useful, meaningful well-paying skill has been learned.

[137] Taber Survey, supra note 14, at 309, 310.

[138] Taber S240, supra note 58, at 531.

[139] Id. See, especially, footnote 85.

[140] P. Hilts, "Computer Break-in Method Poses Big Crime Risk," Washington Post, sec. A page 13 (March 4, 1982); C. Alexander, "Crackdown on Computer Capers," Time (February 8, 1982); G. Kolata, infra note 142, at 1216-1217.

[141] Id.

[142] G. Kolate, "Students Discover Computer Threat," Science vol. 215, 1216 (March 5, 1982).

[143] Id. Admittedly, the Air Force and the NSA do not share possible vulnerabilities which they have discovered. However, just from the newspaper reports, this author had, independently, concluded that SRI's "new" threat was merely a variation on the old Trojan horse theme, at the most. This author makes no claims to being a programming expert, either.

[144] Taber Survey, supra note 14, at 310.

[145] Id. It has been reported that while executive-level employees were involved in only 5 percent of the company thefts, they were responsible for 85 percent of the total dollar loss to U.S. companies. S. Porter, "Theft by Employees: Tighten Screening," Washington Post (March 6, 1982), Clearly, the fear of an army of programmers is overblown.

[146] A perusal of the "computer crime" literature finds the theme of "not reporting" repeated ad infinitum.

[147] Taber Survey, supra note 14, at 288.

[148] A fourth, but highly unlikely, reason is that prosecutors are unable or unwilling to use the statute. Given that the Florida statute is very broad in scope (it can even reach pocket calculators) it would seem that prosecution would be easier to initiate. There may be the fear on the part of prosecutors of the law being voided for vagueness. See infra Appendix.

[149] Y. Chouinard, Climbing Ice (1978) (from the chapter: "Keeping Your Head About You").

[150] See infra Appendix for an example of how the legal system is dealing with the crime issue relating to computers.

[151] See infra Appendix.

[152] "Trade secret" and "copyright" are possible protections.

[153] A. Solzhenitsyn, Solzhenitsyn at Harvard (R. Berman, editor) (1980). From the Harvard commencement speech, "A World Split Apart." "The center of your democracy and of your culture is left without electric power for a few hours only, and all of a sudden crowds of American citizens start looting and creating havoc. The smooth surface film must be thin, then, the social system quite unstable and unhealthy." Id. at 13.

[154] Id. at 11. (From the section "A Fashion in Thinking.").

[155] "Computer crime" is defined here as a criminal act actually committed by a computer.

[156] There are two types of criminal intent: 1) general, and 2) specific. "General" criminal intent is presumed to exist when one commits certain acts, such as robbery, theft, assault, etc. Criminal intent is imputed to the violator by virtue of the commission of the acts. "Specific" criminal intent must be proven to exist, by the prosecution. For example, the charge "intent to commit larceny" requires that the intention to steal actually be proved. If the person charged picked up someone's property, by mistake, thinking that it was his, no "specific" intent exists. G. Susteren, Esq. Attorney, Georgetown Criminal Justice Clinic (Interview June 1982).

[157] Popular science fiction films such as "2001: A Space Odyssey," and "Demon Seed" have suggested otherwise.

[158] The advent of Josefson (supercold) junctions, and, possibly, "bubble" memories presages this event. See Science Volume 215, Number 4535 (February 12, 1982) for an excellent overview of developments and future trends.

[159] Koba Associates, Inc., National Conference on Computer-Related Crime Summary Report (1980) (panel presentation of Hon. Judge Joseph Ryan). "Current statutes are not adequate." Id. at 31. Inquiry at Judge Ryan's chambers revealed that Judge Ryan, as with so many others of the Superior Court of the District of Columbia, was greatly overburdened with court obligations. His law clerk of the time did the underlying research. The definition of "computer crime" used reveals the "tool or target" roots of the clerk's research: "Any crime which either directly or indirectly involved a computer system as a means or target in the perpetration of a crime" (emphasis added). A good synopsis of cases involving computers, where existing statutes were applied, was written by D. Pomerance, "Case Digest," 2 Computer/Law J. 777 (1980).

[160] 3 CSR 206 (Cal. Super. Ct. County of Alameda, 1972).

[161] 589 F. 2d 152 (4th Cir. 1978), cert. denied, 441 U.S. 922 (1979).

[162] Ward, supra note 160, at 211.

[163] Id. at 209.

[164] Id.

[165] Id. see paragraph 1.

[166] Id. at 153.

[167] SB 240 hearing, supra note 17, at 51 (statement of John Taber).

[168] Seidlitz, supra note 161, at 160.

[169] SB 240 hearing, supra note 17, at 51.

[170] Id.

[171] Id.

[172] *Hancock* v. *Decker*, 379 F. 2d 552 (5th Cir. 1967) (per curiam).

[173] *United States* v. *Lambert*, 446 F. Supp. 890 (D. Conn. 1978), cert. denied, 444 U.S. 871 (1979); *United States* v. *Sampson*, 6 CLSR 879 (N.D. Cal. 1978).

[174] Sampson, supra note 173, at 880 (the other case dealt with records). "The uses of the computer and the product of such uses would appear to the court to be a 'thing of value' within the meaning of 18 USC subsec. 641, sufficient upon which to predicate a legally sufficient indictment." Computer time and computer capacity were considered by the court to be inseparable from the physical identity of the computer itself.

[175] *United States* v. *Girard* 601 F. 2d 69 (2nd Cir. 1979).

[176] SB 240 hearing, supra note 17, at 6 (statement of J. D. MacFarlane).

[177] A. Bequai was associated with Koba Associates, Inc., the contractor of the project, at the time. Bequai was project director then, consultant to Koba Associates, Inc. Koba, under a single contract, wrote the Computer Related Crime Legislative Resource Manual and the Computer Crime: Expert Manual. In addition, Koba surveyed prosecutors and investigators, held 6 training conferences in various locations throughout the country, and published two newsletters. C. Williams, Koba Associates, Inc. (phone interview June 10, 1982). Interestingly, the Legislative

Resource Manual surveys the vast array of federal and state statutes available, yet, minimizes their coverage of the many facets of computer technology. Similarly, ACLR minimizes the criticism of specialized "computer crime" legislation. ("Ironically, in an era when the growing awareness of computer crime demands more specialized legislation, the Federal Systems Protection Act has received much criticism." "Computer Crime," 19 ACLR 499, 505 (footnote 2897) (1981). The real irony is that the facts weigh in the critics' favor.

[178] SB 240 hearings, supra note 117, at 51 (statement of John Taber).

○