

UNITED STATES SENTENCING COMMISSION
ONE COLUMBUS CIRCLE, NE
SUITE 2-500, SOUTH LOBBY
WASHINGTON, DC 20002-8002
(202) 273-4500
FAX (202) 273-4529

William W. Wilkins, Jr. Chairman
Julie E. Carnes
Michael S. Gelacak
A. David Mazzone
Ilene H. Nagel
Paul L. Maloney (ex officio)
Edward F. Reilly, Jr. (ex officio)



September 7, 1993

MEMORANDUM

TO: Chairman Wilkins
Commissioners
Senior Staff

FROM: Phyllis J. Newton *pin*
Staff Director

SUBJECT: Computer Fraud Working Group Report

Attached for your review is the Computer Fraud Working Group Report. Staff are prepared to discuss the report and receive advice as to additional work at the September 21st Commission meeting.

If you have questions regarding this report, please call Win Swenson.

Attachment

Computer Fraud Working Group Report

Win Swenson, Chair
Nolan Clark

Mary McDowell
John Scalia

September 8, 1993

TABLE OF CONTENTS

	<u>Page</u>
Executive Summary	iii
I. Introduction: Background and Overview of Report	1
II. Overview of Offenses Under 18 U.S.C. § 1030	2
III. Rationale for and Overview of the Proposed Amendment	3
IV. Public Comment on Proposed Amendment	5
A. Need for Guideline	5
B. Specific Offense Characteristic Categories	5
C. Undue Punitiveness	6
V. Discussions with Interested Parties	7
A. Discussions with Non-DOJ Officials	7
B. Discussions with DOJ/CCU Officials: The Current Position	7
VI. Overview of Legislative History of 18 U.S.C. § 1030	9
VII. Hotline Calls	12
VIII. Case Law	13
IX. Empirical Study of Cases Sentenced Under 18 U.S.C. § 1030	14
A. Types of Cases Prosecuted	16
1. Subsection of 18 U.S.C. § 1030 Charged	16
2. Nature of Victim	17
3. Relationship of Offender to Victim	18
4. Authorization to Access the Computer System	18
5. Nature of Cases Where Access to System Was Unauthorized ..	18
6. Offender's Motivation	18
7. Types of Risk or Harm Created by Offense	19
8. Magnitude of Pecuniary Loss	20
B. Offender Characteristics	21

1.	Age Distribution of Defendants	21
2.	Educational Background of Defendants	21
C.	Sentences Imposed	21
X.	Survey of the Literature	22
XI.	Analysis of Options	23
A.	Option I: Creating a New Computer Guideline	23
B.	Option II: Adding Loss Commentary and Amending the Statutory Index to Reference Guidelines Other Than §2F1.1 for Some Computer Crimes	26
C.	Option III: Taking No Action Now But Continuing to Monitor Cases	27
XII.	Conclusion	28
Appendix A -- Proposed Amendment on Computer Fraud and Abuse		
Appendix B -- Purpose Statement		
Appendix C -- Survey of the Literature on Computer Crime		

Executive Summary

Over the last decade, Congress enacted offenses codified at 18 U.S.C. § 1030 under the caption "Fraud and related activity in connection with computers." The statutory index in the Guidelines Manual references the fraud guideline (U.S.S.G. §2F1.1) for most of the computer-related offenses that are established by this statute.

The Department of Justice (DOJ) advised the Commission that computer crimes can involve harms that are not adequately accounted for under §2F1.1. At DOJ's request, the Commission published an amendment during the last amendment cycle that would establish a new guideline (proposed U.S.S.G. §2F2.1) to govern § 1030 computer crimes.

Following publication of the proposed amendment, the Computer Fraud Working Group (working group) reviewed a variety of information sources to assess the proposal's merit. Public comment on the proposal was generally critical. Personnel from DOJ's Computer Crime Unit (DOJ/CCU) consulted with the working group at various stages and, upon reviewing the public comment, advised the working group that they believed a better approach might be devised. DOJ/CCU suggested redrafting the proposed amendment to avoid concerns raised by public comment that the proposed amendment's specific offense characteristics swept too broadly.

As an alternative to redrafting a new guideline proposal, the working group asked DOJ/CCU how it would view an approach that would seek to address the relevant concerns by adding appropriate commentary following §2F1.1. DOJ/CCU indicated it was open to considering the possible merit of this less far-reaching approach.

However they are addressed, DOJ/CCU believes that there are a number of harms that are both unique to computer crimes and important in assessing their seriousness for sentencing purposes. Invasion of privacy and consequential system recovery costs are examples of these kinds of harms. An examination of relevant legislative history indicates that Congress created 18 U.S.C. § 1030 for reasons that are entirely consistent with DOJ's position, namely that computer crimes 1) can be serious, 2) can involve unique harms, and 3) deserve heightened public awareness as to their potential seriousness.

The working group reviewed a number of information sources and found that the incidence of the ostensibly unique computer crime harms is not well established. An empirical study of cases in which a conviction was obtained under 18 U.S.C. § 1030 revealed few examples of cases involving such harms and, moreover, found that the typical kinds of computer crime cases that have been sentenced under the guidelines involved economic loss that appears to be comfortably accommodated by the current guideline regime.

On the other hand, DOJ/CCU has indicated that there are a relatively high number of "pending" computer crime cases. When these cases are prosecuted and convictions obtained, it may be that the profile of computer crime cases sentenced under the guidelines will change to include more examples of the harms about which DOJ is concerned. In addition, two hotline calls and one unreported sentencing decision provided modest support for DOJ/CCU's concern that the guidelines more directly should account for consequential loss stemming from computer crimes.

There appear to be three basic approaches the Commission might follow at this juncture: 1) pursue the promulgation of a separate computer fraud guideline, as DOJ initially proposed; 2) pursue a "middle approach" of adding new loss commentary to U.S.S.G. §2F1.1 and exploring whether existing guidelines, other than §2F1.1, might better address computer-related harms that occur in connection with certain §1030 offenses; and 3) change nothing now but monitor the development of sentencing practices to see if changes are warranted in the future. Options one and two are not necessarily mutually exclusive, especially in the short term.

The difficulties of defining and ascribing sentencing weight to such harms as invasion of privacy may favor the more flexible approach of adopting expanded loss commentary rather than attempting to create a new guideline. The fact that few cases surveyed have involved harms of the kind that are of concern, may also caution against writing a new guideline at present. This is especially so since DOJ/CCU has advised the working group that it appears there could soon be an increase in the rate of cases prosecuted under 18 U.S.C. § 1030.

The third option would be to continue to monitor sentencing information from computer crime cases but make no immediate changes. In light of limited data to date and the prospect of increased cases in the future, the Commission could elect to hold off on any changes at present.

On the other hand, there is no doubt that 18 U.S.C. § 1030 does include harms that are not well covered by the current loss commentary to §2F1.1. Although the working group found little incidence of most of these harms in the case survey it conducted, to the extent these harms will show up in the future -- and DOJ/CCU believes they will -- the guidelines do not presently offer any guidance as to how they should be treated. Revised loss commentary would provide general guidance as the courts develop a sentencing data base that the Commission could later assess should it wish to address computer harms in a more binding fashion. The working group believes that revising the loss commentary would not be a difficult undertaking, especially in contrast to the more ambitious alternative of drafting a new guideline.

Moreover, discussions between the working group, Senior Staff, and DOJ/CCU shortly before the deadline for this report suggest that a "middle approach" -- i.e., an approach between writing a new guideline for computer crimes and making no changes

to the Guidelines Manual -- need not entail substantial revision to §2F1.1's loss commentary. As of this writing, consensus appeared to be developing among these three groups that *existing guidelines, other than §2F1.1*, may better address some of the computer harms about which DOJ/CCU is concerned than does §2F1.1.

Because 1) the case for a new computer fraud guideline does not appear strong, and 2) the guidelines do not deal with harms that, while not typical, can occur in connection with computer crimes, the working group proposes to pursue the "middle approach" described above.

I. Introduction: Background and Overview of Report

Beginning in 1984 -- and through statutory amendments enacted over the succeeding six years -- Congress established six new criminal offenses relating to the use of computers. These new offenses are codified at 18 U.S.C. § 1030 under the caption "Fraud and related activity in connection with computers." The Commission did not write separate guidelines to govern the new 18 U.S.C. § 1030 offenses. Rather, in 1988, it amended¹ the guidelines' statutory index to refer the user of the Guidelines Manual to existing Chapter Two guidelines for § 1030 offenses. The statutory index refers the user to the fraud guideline (U.S.S.G. §2F1.1) for convictions of five of the six substantive offenses under 18 U.S.C. § 1030, and to U.S.S.G. §2M3.2 for violations of § 1030(a)(1), involving national security data. (Violations of § 1030(b), involving attempts, are referred to U.S.S.G. §2X1.1.)

During the last amendment cycle, the Department of Justice (DOJ) requested² that the Commission publish for comment an amendment³ that would create a separate guideline, at U.S.S.G. §2F2.1, to govern computer fraud and abuse. The Commission agreed to publish the proposed amendment,⁴ and the Computer Fraud Working Group (hereafter working group) convened thereafter. Because the working group was in the unusual position of having a specific DOJ proposal and related public comment available for analysis at the outset of its work, the working group proposed in its Purpose Statement⁵ that the published amendment provide the principal focus for the working group's work.

Since publication of the amendment, the working group has 1) met with interested parties, 2) reviewed public comment, legislative history, case law, relevant literature and hotline calls, and 3) conducted an empirical analysis of cases sentenced under 18 U.S.C. § 1030. After describing the key features of the relevant statute and the proposed amendment, this Report summarizes the working group's findings in each of these areas and concludes with an analysis of what appear to be the Commission's three primary options in light of the information gathered.

¹U.S.S.G. Appendix C, amendment 60.

²See Letter from Paul L. Maloney, Member (ex officio), U.S. Sentencing Commission, to Judge William W. Wilkins, Jr., Chairman, U.S. Sentencing Commission, 7-8 (October 15, 1992).

³See Appendix A.

⁴See 57 Fed. Reg. 62832, 62855-56 (1992).

⁵See Appendix B.

II. Overview of Offenses Under 18 U.S.C. § 1030

The caption for 18 U.S.C. § 1030 aptly indicates that the conduct prohibited by this provision extends beyond traditional notions of fraud to other "related activity in connection with computers." Indeed, while all of the offenses established under § 1030 *could* involve fraud, only two provisions (subsections (a)(4) and (a)(6)) *necessarily* involve the elements of fraud.

In general terms, the statute establishes the following six offenses:

<u>Offense</u>	<u>Applicable Guideline⁶</u>	<u>Maximum Term of Imprisonment⁷</u>
• Subsection (a)(1) -- knowingly accessing a computer without authorization to obtain national security data;	§ 2M3.2	10 years
• Subsection (a)(2) -- intentionally accessing a computer without authorization to obtain certain confidential financial information;	§ 2F1.1	1 year
• Subsection (a)(3) -- intentionally accessing a government computer thereby "affect[ing] the use of the government's operation of such computer";	§ 2F1.1	1 year
• Subsection (a)(4) -- accessing a computer with intent to defraud and thereby obtaining anything of value;	§ 2F1.1	5 years
• Subsection (a)(5) -- intentionally accessing a computer without authorization to, among other things, alter information thereby causing a loss of at least \$1,000; and	§ 2F1.1	5 years

⁶Guideline to which user of the manual is referred by the statutory index.

⁷Subsequent violations of these offenses carry higher maximum penalties that range from ten to twenty years.

- *Subsection (a)(6)* -- trafficking in a password or similar information through which a computer can be accessed without authorization, knowingly and with intent to defraud. § 2F1.1 1 year

III. Rationale for and Overview of the Proposed Amendment

The proposed DOJ amendment that the Commission published for comment is set out at Appendix A. The rationale for the amendment, provided by DOJ, was stated in the Federal Register as follows:

This amendment creates a new guideline applicable to violations of the Computer Fraud and Abuse Act of 1988 (18 U.S.C. § 1030). Violations of this statute are currently subject to the fraud guidelines at §2F1.1, which rely heavily on the dollar amount of loss caused to the victim. Computer offenses, however, commonly protect against harms that cannot be adequately quantified by examining dollar losses. Illegal access to consumer credit reports, for example, which may have little monetary value, nevertheless can represent a serious intrusion into privacy interests. Illegal intrusions in the computers which control telephone systems may disrupt normal telephone service and present hazards to emergency systems, neither of which are readily quantifiable. This amendment proposes a new Section 2F2.1, which provides sentencing guidelines particularly designed for this unique and rapidly developing area of the law.

To achieve DOJ's stated goal of accounting for a variety of potential harms -- many of them nonmonetary -- the proposed guideline builds on a base offense level of six with the following specific offense characteristics:⁸

⁸The proposed amendment's commentary provides definitions for most relevant terms. See Appendix A.

Harms Pertaining to the Reliability and Integrity of Data⁹

<i>Specific Offense Characteristic</i>	<i>Offense Level Increase</i>
• altering data	+2
• altering protected information or public records	+6
• obtaining protected information	+2
• disclosing protected information	+4
• disclosing protected information through a general distribution system	+6

Other Nonmonetary Harms¹⁰

<i>Specific Offense Characteristic</i>	<i>Offense Level Increase</i>
• interfering with the administration of justice	+6
• harming any person's health or safety	+6
• interfering with any facility or communications network serving public health or safety	+6

Monetary Harm

<i>Specific Offense Characteristic</i>	<i>Offense Level Increase</i>
• economic loss, including 1) costs of system recovery and 2) consequential loss from trafficking in passwords	+ amount from table in §2F1.1.

⁹Under the proposed amendment, the maximum allowable increase in the offense level for this category of specific offense characteristics is 8.

¹⁰Under the proposed amendment, the maximum allowable offense level increase for this category of specific offense characteristics is 6.

Malicious Purpose

<i>Specific Offense Characteristic</i>	<i>Offense Level Increase</i>
• committing offense for the purpose of malicious destruction or damage	+4

IV. Public Comment on Proposed Amendment

The Commission received comment on the proposed DOJ guideline from six sources. All of the comments received were largely critical of the proposal. Comments questioned, variously, the need for a separate guideline, the potential breadth and impact of specific offense characteristics, and the overall severity of the sentences that would result from adoption of the proposed amendment. A synopsis of the comment follows.

A. Need for Guideline

The Federal Public and Community Defenders stated that they were not aware of many prosecutions for computer fraud and abuse. They noted that the existing fraud guideline suggests an upward departure when monetary loss does not fully capture the harmfulness and seriousness of the conduct. Accordingly, the Federal Defenders concluded that "there is no urgent need for a separate guideline to cover a handful of cases."

The Practitioners' Advisory Group used similar reasoning to question the need for a separate computer fraud guideline to deal with the sorts of non-monetary harm the proposed amendment seeks to address. The Advisory Group pointed to U.S.S.G. §2F1.1, comment. (n.10), which authorizes upward departures when, among other instances, the primary objective of the fraud was non-monetary, the offense endangered national security or military readiness, false statements were made for the purpose of facilitating some other crime, and the offense caused physical or psychological harm.

Computer Professionals for Social Responsibility also questioned the need for a new guideline: "It is our view that the current guidelines are a reasonably fair articulation of the specific harms that might warrant additional stringency, at least in the area of computer crime." "In addition, promulgation of a sentencing guideline at the present time is premature, as there have been very few published opinions where judges have issued sentences for violation of the CFAA."

B. Specific Offense Characteristic Categories

The proposed amendment provides for an increase "[i]f the defendant altered information." This category was criticized as overly broad. The Society for Electronic

Access stated: "Alteration is defined to include all changes to data. Merely logging onto another computer changes the information in the computer's system logs." Similarly Computer Professionals for Social Responsibility commented: "Any user of a computer system 'alters' the data on the system."

The proposed amendment provides for substantial increases if the defendant obtained or altered "protected information." Categorizing information in this way drew criticism. Computer Professionals for Responsibility commented: "It has been the experience of the computer profession that efforts to create new categories of information restriction invariably have a chilling impact on the open exchange of computerized data." Thomas A. Guidoboni and David W. O'Brien posited in a joint statement that any increase should be limited to the categories of information expressly protected by 18 U.S.C. § 1030 (i.e., classified national defense, foreign relations and restricted atomic energy data; financial records of a financial institution or card issuer; consumer credit information; medical records; and passwords).

Regarding the proposed amendment's increases for "economic loss," Messrs. Guidoboni and O'Brien viewed such an increase as troublesome because the proposal includes unintentionally caused costs or damages: "Use of a computer is not equivalent to the use of an inherently dangerous instrument, and what constitutes 'unauthorized access' to another computer is not always clear-cut." Computer Professionals for Social Responsibility agreed that the proposed guideline does not adequately distinguish between acts where harm is intended and those where it is not.

Finally, the proposed amendment provides for an increase if "an offense was committed for the purpose of malicious destruction or damage," with malicious destruction or damage defined to include injury to business and personal reputations. The Society for Electronic Access commented that the proposal was too broad in that it would treat "copying and publicly posting materials from [a] person's account that simply make[s] the person look foolish" as equivalent to "[b]reaking into a person's computer account and publicly posting information which disrupts his or her ability to conduct business."

C. Undue Punitiveness

The Society for Electronic Access commented that the proposed six-level increase for disclosing protected information to the public by means of a general distribution system is grossly disproportionate to the severity of the offense: "Such an increase, merely for putting some information on an electronic bulletin board, would treat the offense as more serious than assault with a dangerous weapon, sexual abuse of a ward, or trespassing on government property with a firearm."

Mr. Guidoboni and Mr. O'Brien stated that the offenses covered by the proposed guideline were more akin to theft, trespass, and property damage and destruction and thus should start with a base offense level of four rather than six.

Electronic Frontier Foundation, Inc., commented that the proposed guideline "is much too harsh for first time offenders and those who perpetrate offenses under the statute without malice aforethought."

V. Discussions with Interested Parties

The working group met directly with Thomas A. Guidoboni, who represented a defendant convicted under 18 U.S.C. § 1030 in a highly publicized case involving a computer "worm," Shari Steele of the Electronic Frontier Foundation (EFF), and representatives of DOJ's Computer Crime Unit (DOJ/CCU). Discussions with non-DOJ officials tended to confirm views advanced in written submissions. Discussions with DOJ/CCU officials have occurred periodically during the course of the working group's work and have led to a shared view between DOJ/CCU and the working group that options beyond simple tinkering with the published amendment should be explored.

A. Discussions with Non-DOJ Officials

Mr. Guidoboni and Ms. Steele both had submitted comment on the proposed amendment and both underscored points made in their submissions. Mr. Guidoboni stressed two points in particular. First, he urged the Commission to resist treating offenses involving a computer differently from other violations of the same kind of offense merely because a computer happened to be involved. He suggested that in this area the guidelines should stay with their basic approach of treating offenses generically, i.e., frauds as frauds, thefts as thefts, etc., notwithstanding use of, or impact on, a computer.

Second, he proposed that if consequential loss is counted in calculating the sentence it be limited to "reasonably foreseeable" loss. He generally urged care in adopting a definition of countable loss to ensure that the definition not be so inclusive that it brings about unjustly harsh punishment.

Ms. Steele echoed Mr. Guidoboni's view that the guidelines should treat offenses, whether or not involving computers, in a consistent, and to the extent possible, generic manner. She also emphasized a concern highlighted in EFF's written comments, that there ought to be a showing of intent with respect to loss counted in the computation of a sentence.

B. Discussions with DOJ/CCU Officials: The Current Position

The working group engaged in ongoing discussions with representatives of DOJ/CCU during the course of its work. These discussions allowed the working group the benefit of DOJ/CCU's thinking as new information and tasks presented themselves. DOJ/CCU's analysis of the public comment the Commission received in response to the

published amendment was especially useful in helping the working group consider a course for further work.

In general, DOJ/CCU found much of the public comment the Commission received to be appropriate and valid. Specifically, DOJ/CCU agreed that some specific offense characteristics and related definitions might be too broad and that while consequential loss should be counted in determining the sentence for computer crimes, further definition of this concept may be justified to avoid undue punishment.

The working group's early empirical work confirmed that there have been relatively few defendants convicted under 18 U.S.C. § 1030.¹¹ Partly due to this finding, the working group raised with DOJ/CCU the option of addressing its concerns in some manner other than through a guideline amendment, such as with expanded loss commentary in U.S.S.G. §2F1.1.

In light of the public comment and our back and forth discussions, DOJ/CCU's current position can be summarized as follows:

- The proposed amendment that was published for comment was an initial attempt to highlight important issues and can be improved upon.
- DOJ/CCU does not have a definite view at this point on whether a new *guideline* is needed to address what it believes are unique harms that can occur under 18 U.S.C. § 1030, but it does believe that some accommodation should be made in the Guidelines Manual to better account for computer-offense harms. DOJ/CCU is open to considering whether additional commentary might serve that purpose, and it is willing to work toward redrafting a separate guideline as well.
- In any case, the Guidelines Manual should, in DOJ/CCU's view, account for the following general categories of harms in some appropriate manner:
 - 1) Conscious or reckless risk of harm to a person's health or safety.
 - 2) Conscious or reckless risk of interference with the conduct of foreign relations or the national defense.
 - 3) Conscious or reckless risk of interference with the administration of justice.
 - 4) Interference with a communications network providing communication service to the public.
 - 5) Significant invasion of a person's privacy.

¹¹See Section IX of this Report.

- 6) If the offense involved economic loss,
 - a) the economic loss deriving from system recovery costs that were reasonably foreseeable.
 - b) the economic loss deriving from consequential losses caused by trafficking in passwords.
- 7) Malicious (i.e., intentional) destruction, damage, or injury.

VI. *Overview of Legislative History of 18 U.S.C. § 1030*

As noted, DOJ/CCU's current position is that the Guidelines Manual should, at least in some manner, more directly address computer offense-related harms. The legislative history to 18 U.S.C. § 1030 can be said to support this general view in two ways. First, the legislative record indicates a conscious decision by Congress to increase public awareness that computer-related crimes can be serious. This decision is explicitly stated in the legislative history and implied by Congress' separate treatment of these offenses in Title 18. Second, Congress appears to have wanted the criminal code to proscribe in a more direct fashion the kinds of misconduct and harms that can occur in connection with computers than existing fraud and theft offense provisions were deemed to do. Providing greater focus in the Guidelines Manual on computer crimes and the harms they cause arguably would serve these two legislative purposes.

The current version of 18 U.S.C. § 1030 derives primarily from two separate statutory enactments: the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984¹² and the Computer Fraud and Abuse Act of 1986.¹³ Enactment of these federal statutes coincides with the enactment on the state level of a wave of computer crime laws, starting with the 1978 statutes enacted by Florida and Arizona.¹⁴

¹²Public Law 98-473

¹³Public Law 99-474.

¹⁴The emergence of computer crime laws is documented and analyzed in Hollinger & Lanza-Kaduce, "The Process of Criminalization: The Case of Computer Crime Laws," 26 *Criminology* 101-126 (1988). The development of the 1986 Act is covered in "The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem," 43 *Vand.L.Rev.* 453-490 (1990).

Growing publicity over computer abuse¹⁵ appears to have provided an impetus for federal legislative proposals, which were introduced as early as 1978. Representative Bill Nelson, who had been the principal author of Florida's computer crime act while in the state legislature, became the chief advocate for a federal computer crime statute. Much of the wording of his proposed legislation was incorporated into another bill dealing with credit card fraud and the abuse of credit information. The combined legislation was ultimately enacted as the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.

A House Report to this legislation described Congress' rationale for computer fraud legislation.¹⁶ The perceived problem was that intangible property in the form of magnetic impulses did not fit well into the traditional theft/larceny statutes. This problem was compounded, the Report continued, by "the advent of . . . so-called 'hackers' who have been able to access (trespass into) both private and public computer systems, sometimes with potentially serious results."¹⁷ Finally, the Report noted a "tremendous attitudinal problem": "People can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about taking information by use of a device called a computer even if it costs the economy millions now and potentially billions in the future."¹⁸

The 1984 Act made the unauthorized use of or access to a computer illegal in three comparatively narrow areas: (1) obtaining classified defense or foreign relation information with intent or reason to believe that the information would be used to harm the United States; (2) obtaining information contained in a financial record of a financial institution or in a consumer file of a consumer credit reporting agency; and (3) using, modifying, destroying, or disclosing information in a federal government computer if such conduct would affect the government's use of the computer.

Perhaps because of its narrowness, the 1984 Act appears to have been seldom used by prosecutors. In any case, DOJ lobbied for legislation that would both broaden the criminal provisions of the 1984 Act and create new criminal provisions covering fraud

¹⁵In late August and early September 1983, *Newsweek*, *People*, and *Time* all featured stories on juvenile hackers and the threat of computer crime. See Hollinger and Lanza-Kaduce, p. 107.

¹⁶House Report No. 98-894 is reprinted at 4 U.S. Code. Cong. Admin. News 3689-3711 (1984).

¹⁷*Id.* at 3695.

¹⁸*Id.* at 3697.

and destruction of property.¹⁹ Others wanted even broader federal legislation. The National District Attorney's Association, for example, favored a federal statute that would preempt state law and cover all computer crimes nationwide.²⁰

Congress agreed to broaden the scope of 18 U.S.C. § 1030 in 1986, but rejected the call for preemptive legislation. The Senate Report explained: "The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature."²¹

The 1986 Act modified the scope of subsections (a)(2) and (a)(3) and also defined three new offenses: (1) accessing a "Federal interest" computer with intent to defraud; (2) accessing a "Federal interest" computer and altering or destroying data that thereby causes a loss of more than \$1,000 or potentially impairs medical treatment; and (3) trafficking in passwords with intent to defraud.

The legislative history of the 1986 Act indicates that the Senate Judiciary Committee was primarily concerned with the use of "computers to steal, to defraud, and to abuse the property of others."²² The Senate Report makes clear that the Committee was mindful that abuse of property included harms that are "not solely financial in nature," citing the "414 Gang" break-in of the Memorial Sloan-Kettering Cancer Center.²³ Finally, the Committee concluded that knowing trafficking in other people's computer passwords should be directly proscribed.²⁴

The legislative history indicates that the overall purpose of the federal computer crime statute was to deter and educate. The Senate Judiciary Committee agreed with the ABA Computer Crime Task Force that increased computer security was the most effective means of preventing and deterring computer crime. The Committee also agreed that education programs were needed to "make young people and others aware of the ethical and legal questions at stake in the use of computers and to deflate the myth

¹⁹See generally "The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem," 43 Vand.L.Rev. 453, 466-470 (1990).

²⁰*Id.* at pp. 471-73.

²¹Senate Report No. 99-432, reprinted in 4 U.S. Code Cong. Admin. News, 2479, 2482 (1986).

²²*Id.* at 2480.

²³*Id.*

²⁴*Id.*

that computer crimes are glamorous, harmless pranks."²⁵ At the same time, the Senate Judiciary Committee found "that Federal criminal penalties for computer crime are an appropriate punishment for certain acts and can serve to deter would-be computer criminals and to reinforce education and security improvement programs."²⁶

VII. Hotline Calls

The Commission's hotline for probation officers and judges has received two calls concerning defendants who have engaged in unauthorized use of a computer. The fact that only two calls have been received suggests that application questions in this area are not yet a major problem for the field. On the other hand, the questions raised in the two cases are generally of the kind that the DOJ proposal seeks to answer.

The first hotline call involved a defendant in a well publicized case who introduced a computer "worm" into the INTERNET computer system. The defendant went to great lengths to conceal the nature and source of his intrusion. The probation officer's central questions were 1) Why does the statutory index reference §2F1.1 when there was no fraud involved? 2) Can the offense loss be based on the cost of detection and eradication of the worm and the loss of computer time? and 3) Is the enhancement for abuse of a special skill (§3B1.3) appropriate? A more specific treatment in the Guidelines Manual of § 1030 offenses might well obviate a question like the first one. The second question, dealing with consequential loss from computer offenses, is of the kind that DOJ believes the guidelines should explicitly address. The third question, while not answered by DOJ's proposal, does raise an issue touched on in public comment to the proposed guideline. Comment has raised the concern that application of both a new computer fraud guideline and U.S.S.G. §3B1.3 could lead to double counting.

The second hotline call involved a defendant who "improved" the credit histories of individuals for a fee. The defendant illegally gained access to the computer files of a credit reporting agency and altered his "customers" credit histories. The probation officer questioned whether the offense loss could be based on 1) the cost of reprogramming the credit reporting agency's computer system and 2) the value of the loans improperly granted to the defendant's customers. While DOJ would like to see greater clarification in the guidelines regarding computer-offense loss, this case demonstrates an additional technical issue that would require consideration if a new computer fraud guideline were adopted. In this case the defendant was convicted of wire fraud, not a § 1030 offense.²⁷ Thus a new guideline for computer fraud and abuse

²⁵*Id.* at 2481.

²⁶*Id.*

²⁷It appears that this is not an unusual occurrence with respect to computer-related misconduct. See Section IX.

would not resolve the questions in this case unless the fraud guideline contained a cross reference to the computer guideline, or the statutory index for fraud counts listed the new computer guideline as potentially applicable.

VIII. Case Law

The working group reviewed court opinions reported in traditional reporters (e.g., F.2d) and electronic data bases (e.g., LEXIS) that involved computer crimes. None of the six cases reviewed raised issues that appeared particularly relevant to this Report.²⁸ DOJ/CCU provided the working group with the transcript of a sentencing hearing and court decision involving a computer case in Denver that did contain relevant information, however.

The case²⁹ involved a young hacker who apparently gained unauthorized access into a government computer system. The prosecution agreed that it "would be a major mistake for both him and society" to send the defendant to prison.³⁰ Nevertheless, the prosecution wanted to establish -- for the purpose of "making good law" on the issue -- that certain consequential costs to the government in bringing the system back into sound and secure operating condition should count as "loss" under U.S.S.G. §2F1.1.³¹ The prosecution conceded that the Sentencing Commission had not expressly taken "into account this unique potential for damages."³²

The defense opposed considering the consequential loss. It countered that the Commission had recently adopted new commentary on loss and that the commentary limited consideration of consequential loss to certain enumerated kinds of offenses, computer fraud not being one of them.³³

²⁸The six cases reviewed were: *United States v. Riggs*, 967 F.2d 561 (11th Cir. 1992); *United States v. Demonte*, 961 F.2d 1579 (6th Cir. 1992); *United States v. Rice*, No. 91-5786 (4th Cir. 1992); *United States v. Carron*, 928 F.2d 1137 (9th Cir. 1991); *United States v. Morris*, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991); and *United States v. Lewis*, 872 F.2d 1030 (6th Cir. 1989).

²⁹*U.S. v. Wittman*, No. 91-327, Sentencing Hearing (D. Colo., March 16, 1992).

³⁰*Id.* at 12.

³¹*Id.* at 18-19.

³²*Id.* at 18.

³³*Id.* at 19.

The court agreed with the defendant's position but went on to state:

[T]he Court is of the view that more explanatory information should be set forth by the sentencing guidelines, and in the application notes in regard to the interpretation of computer activity. I think it's a great big void right now with computerization exploding at a very rapid pace. They should receive a high level degree of activity, and I do appreciate the fact that we have someone from the Department of Justice, no doubt, who will take this up with their colleagues in an effort to make the sentencing guidelines just a little more exacting than it is [sic] right now.³⁴

IX. Empirical Study of Cases Sentenced Under 18 U.S.C. § 1030

The working group conducted a study of cases sentenced under the guidelines that involved computer fraud and abuse. Practical problems, however, made it infeasible to review all potentially relevant cases. Discussions with DOJ/CCU confirmed that some cases involving computer fraud and abuse are prosecuted under statutes other than 18 U.S.C. § 1030. Indeed, computer fraud cases can be brought under approximately 40 different statutes. Because it would be something of a needle-in-the-haystack exercise to, for example, pull all of the thousands of U.S.S.G. §2F1.1 cases looking for those involving computers, the working group limited its study to cases with counts of conviction under 18 U.S.C. § 1030. These cases were readily identifiable.

Commission data for the period January 19, 1989, through April 30, 1993, indicate 76 cases in which the statutes of conviction included 18 U.S.C. § 1030. Of these 76 cases, 50 were available for inspection. The remaining 26 had been sent to archives. Accordingly, the working group examined the 50 cases sentenced under 18 U.S.C. § 1030 for which sentencing documents were available.³⁵

The working group examined these cases to determine, among other matters, the incidence of the factors 1) targeted for sentence enhancement in DOJ's proposed amendment and 2) subsequently identified by DOJ/CCU in discussions as important for consideration at sentencing. Overall, we found that most offenses involved economic harms

³⁴*Id.* at 24-25.

³⁵As a general rule, the 26 archived cases were older than the non-archived cases. Given the resources required to pull the archived cases, it was therefore decided to focus on the readily available, non-archived cases in which the information would be most current.

of the kind now addressed by §2F1.1 and infrequently involved other harms specified by DOJ as important.³⁶ More specifically, we learned the following:

- 1) 90 percent of the cases involved some form of fraud, theft, or embezzlement;
- 2) in 76 percent of the cases, the victim was the federal government, a financial institution, or a credit institution;
- 3) in 50 percent of the cases, the offender was a current or former employee of the victim;
- 4) in 64 percent of the cases, the offender or a co-conspirator was authorized to access the computer system;
- 5) none of the cases involved a conscious or reckless risk of harm to health or safety;
- 6) none of the cases involved a conscious or reckless risk of interference with the conduct of foreign relations or the national defense;
- 7) none of the cases involved interference with a communication network providing communications service to the public;³⁷
- 8) none of the cases involved economic loss from system recovery costs;³⁸

³⁶Because the empirical study did not, as noted, examine all cases that might have involved computer crimes, our study may understate the occurrence of some of the harms about which DOJ is concerned. See the next three footnotes.

³⁷DOJ/CCU has advised the working group that several defendants have been convicted of crimes involving interference with a communications network but the cases did not surface in our study because the statute of conviction in these cases was not 18 U.S.C. § 1030. The defendants in these cases reportedly engaged in conduct ranging from disconnecting the phones of Hollywood celebrities to seizing control of phone lines to win radio station call-in contests.

³⁸We know from a reported decision of at least one case in which system recovery costs appeared to be at issue. *United States v. Morris*, 928 F.2d 504 (2d Cir.), *cert. denied*, 112 S. Ct. 72 (1991). This case did not surface in the empirical study because the sentencing documents in that case had been archived. In another unreported decision provided by DOJ/CCU, system recovery costs were clearly a central issue. See Section VIII.

- 9) invasions of privacy have not played a significant role; four cases involved a possible privacy interest, but none were deemed to involve a significant invasion of privacy;³⁹
- 10) on average, the cases did not involve extremely large pecuniary losses; the median loss was between \$10,000 and \$20,000; 78.3 percent of the cases involved a loss of \$70,000 or less;
- 11) only one of the 50 cases appeared to involve a hacker;
- 12) at least 78 percent of the defendants were 26 or more years old;
- 13) at least 38 percent of the defendants had at most a high school education;
- 14) the mean sentence imposed in the 50 cases was 6.8 months;
- 15) the four defendants whose motivation appeared to be to browse data, demonstrate computer prowess, or commit vandalism were placed on probation (None of these cases involved significant loss amounts.); and
- 16) the longest sentences were imposed on the defendants who were involved in industrial espionage or interference with the administration of justice (These cases involved relatively large loss amounts.).

A further breakdown of the working group's findings follows.

A. Types of Cases Prosecuted

1. Subsection of 18 U.S.C. § 1030 Charged

The distribution of cases by subsection charged was as follows:

<i>Subsection</i>	<i>Nature of Offense</i>	<i>Number</i>	<i>Percent</i>
(a)(1)	Effect on national security	0	0
(a)(2)	Access to financial information	12	24
(a)(3)	Affect government use of computer	5	10
(a)(4)	General impact of fraud	27	54
(a)(5)	Alteration of information	1	2
(a)(6)	Trafficking in passwords	6	12

³⁹DOJ/CCU also advised the working group that several hacker cases, although not surfacing in the study, have involved significant invasions of privacy. In one case, the conspirators reportedly had 176 credit reports in their possession.

The percentages total to more than 100 percent because one defendant was charged under subsections (a)(2) and (a)(4).

a) *Nature of cases charged under subsection (a)(2).* Following are brief characterizations of the types of cases charged under subsection (a)(2) -- obtaining information in a financial record:

8 cases	credit card fraud
3 cases	altering credit histories
2 cases	financial company theft or embezzlement

b) *Nature of cases charged under subsection (a)(3).* Following are brief characterizations of the types of cases charged under subsection (a)(3) -- affecting use of government's operation of computer:

2 cases	obtaining criminal record information
1 case	resigning employee left "time bomb" in computer software designed to delete personal information
1 case	IRS employee kept track of tax investigation of a friend
1 case	ex-employee used mother's password to access system and use E-mail

c) *Nature of cases charged under subsection (a)(5).* Following are brief characterizations of the types of cases charged under subsection (a)(5) -- altering computer information:

1 case	hacker claimed he accidentally accessed system; he then set up system so that he could access at will and then browse data
--------	--

d) *Nature of cases charged under subsection (a)(6).* Following are brief characterizations of the types of cases charged under subsection (a)(6) -- trafficking in access codes or passwords:

6 cases	use of telephone access codes
1 case	use of counterfeit credit card information

2. Nature of Victim

The distribution of cases by nature or type of victim was as follows:

<i>Type of Victim</i>	<i>Number</i>	<i>Percent</i>
U.S. government	15	30
Financial institution	14	28
Credit organization	9	18
Other for-profit organization	11	22
Other	1	2

3. Relationship of Offender to Victim

The distribution of cases by the relationship of the offender to the victim (at the time of the offense) was as follows:

<i>Type of Relationship</i>	<i>Number</i>	<i>Percent</i>
Current employee	22	44
Former employee	3	6
No relationship	25	50

4. Authorization to Access the Computer System

The distribution of cases based on whether the offender or a co-conspirator was authorized to access the computer system was as follows:

<i>Presence or Absence of Authorization</i>	<i>Number</i>	<i>Percent</i>
Authorized to access system	32	64
Not authorized to access system	17	34
Missing	1	2

5. Nature of Cases Where Access to System Was Unauthorized

Following are brief characterizations of the types of cases in which access to the computer system was unauthorized:

5 cases	improper use of telephone access codes
3 cases	obtaining data for credit card frauds
1 case	claimed accidental access; system then set up to allow repeated access; defendant appears to have merely browsed data
1 case	use of counterfeit credit card
1 case	alteration of cellular phone to be identified with fraudulent codes
1 case	use of credit card fraudulently claimed to have been stolen
1 case	use of stolen credit cards to make purchases

6. Offender's Motivation

The distribution of cases based on the offender's motivation was as follows:

<i>Motivation of Offender</i>	<i>Number</i>	<i>Percent</i>
Obtain free use of communications facility	6	12
Obtain use of computer	3	6
Other fraud, theft, or embezzlement	35	70

Demonstrate computer prowess	1	2
Browse data	2	4
Commit vandalism	1	2
Industrial espionage	1	2
Interfere with administration of justice	5	10
Access NCIC for criminal record data	4	8
Alter credit history (to accommodate boyfriend who received payment for alteration)	1	2

The percentages total to more than 100 percent because some offenders were coded as having more than one motivation.

Dual motivation cases. The distribution of cases involving more than one motivation was as follows:

1 case	browse data & obtain use of computer
4 cases	commit fraud & interfere with administration of justice
1 case	demonstrate computer prowess & commit vandalism
1 case	browse data & obtain free use of communications facility

7. Types of Risk or Harm Created by Offense

The percentages of the cases that involved certain types of risk or harm identified as priority areas by DOJ/CCU⁴⁰ were as follows:

<i>Type of Risk or Harm</i>	<i>Number</i>	<i>Percent</i>
Conscious/reckless risk of harm to health/safety	0	0
Conscious/reckless risk of interference with conduct of foreign relations or the national defense	0	0
Conscious/reckless risk of interference with administration of justice	6	12
	<i>Number</i>	<i>Percent</i>
Interference with a communications network providing communications service to the public	0	0
Invasion of privacy	4	8
Economic loss from system recovery costs	0	0
Consequential loss from trafficking in passwords	0	0
Malicious destruction, damage, or injury	1	2

⁴⁰See Section V.(B).

Nature of interference with administration of justice. Following are brief characterizations of the cases that involved a risk of interference with the administration of justice:

1 case	IRS employee accessed information to monitor tax investigation of an acquaintance
2 cases	IRS employee deleted data on friend's tax liability
1 case	IRS employee submitted false return and monitored whether any CID request was placed on the account; skipped town when CID request was placed
1 case	INS employee accepted bribe to issue fraudulent "green cards"

Nature of privacy interest. Following are brief characterizations of the cases that were coded as involving an invasion of a privacy interest:

3 cases	obtaining criminal record information from NCIC
1 case	gaining access to credit histories to commit a credit card fraud

In each case coded as involving a privacy interest, the coder questioned whether the case actually involved a privacy interest. In each of these cases, invasion of the privacy interest was not deemed to have been "significant."

Nature of Malicious destruction, damage, or injury. Following is a brief characterization of the case involving malicious destruction, damage, or injury:

1 case	defendant designed a "time bomb" that destroyed personal files after his resignation from a government contractor; defendant described "time bomb" as "remember me."
--------	--

8. Magnitude of Pecuniary Loss

The distribution of cases by pecuniary loss ranges was as follows:

<i>Loss Range</i>	<i>Number</i>	<i>Percent</i>	<i>Cumulative Percent</i>
\$2,000 or less	10	21.7	21.7
More than \$2,000	6	13.0	34.8
More than \$5,000	6	13.0	47.8
More than \$10,000	4	8.7	56.5
More than \$20,000	6	13.0	69.6
More than \$40,000	4	8.7	78.3
More than \$70,000	3	6.5	84.8
More than \$120,000	1	2.2	87.0
More than \$200,000	2	4.3	91.3

More than \$350,000	2	4.3	95.0
More than \$500,000			
More than \$800,000	2	4.3	100.0

B. Offender Characteristics

1. Age Distribution of Defendants

The distribution of cases by age-ranges of defendants was as follows:

<i>Age-Range</i>	<i>Number</i>	<i>Percent</i>
18-25	9	18
26-34	16	32
35-80	23	46
unknown	1	4

2. Educational Background of Defendants

<i>Education Level</i>	<i>Number</i>	<i>Percent</i>
up to high school	19	38
college	26	52
unknown	4	10

C. Sentences Imposed

Mean Sentence, By Motivation

The mean sentence, in months, for defendants who had various motivations were as follows:

<i>Motivation</i>	<i>Number</i>	<i>Mean Sentence</i> ⁴¹
Free use of communications facility	6	0.2
Use of computer	3	0.3
Other fraud, theft, or embezzlement	33	8.9
Demonstrate computer prowess	1	0.0
Browse data	2	0.0
Vandalism	1	0.0
Industrial espionage	1	18.0
Interference administration of justice	5	17.2
Other	4	5.0
Overall	50	6.8

⁴¹In months.

X. *Survey of the Literature*

An extensive body of literature devoted to computer-related crime has developed over the last twenty years or so. The working group reviewed this literature in some detail to determine if more could be learned with respect to the following questions: 1) What is the nature of computer crime? 2) Who commits computer crime? 3) How much computer crime is committed and how much loss results from such crime? 4) What explains the relative paucity of computer crime prosecutions? 5) What sentences are appropriate for computer crimes?

A full discussion of the working group's literature survey is set out at Appendix C. In brief, the working group was able to draw the following conclusions from the literature that are potentially relevant to sentencing under 18 U.S.C. § 1030:

- *What is computer crime?*

Computer crime has evaded a solid definition. While some types of *computer abuse* are unique and would be difficult to prosecute under traditional criminal statutes (e.g., unauthorized access of a computer to "browse"), there is no clear demarcation between *computer fraud* and other types of fraud. Typically, there is no impediment to prosecuting computer frauds under the general fraud statutes of title 18.

- *Who commits computer crime?*

Most computer crimes are committed by employees and involve taking of something of value from the employer. Contrary to an early view, many computer crimes are committed by persons who have only rudimentary computer skills.

- *How much computer crime is committed and at what cost?*

Reliable statistical evidence regarding the incidence and cost of computer crime is not available. Prosecutions of computer crimes reportedly have risen in recent years; it is not clear, however, whether this increase in prosecutions indicates an increase in the incidence of computer crime. Loss estimates from computer crimes vary widely.

- *Why do there appear to be relatively few prosecutions?*

Commentators seem to agree that the number of prosecutions of computer crimes under 18 U.S.C. § 1030 and other computer-specific criminal laws is low relative to the incidence of these crimes. However, because prosecutions of computer crimes under general fraud and other statutes are not fully accounted for, we do not know how many prosecutions of

computer crimes actually occur. A variety of explanations exist as to why general criminal statutes may be preferred by prosecutors over computer-specific statutes.

- *What sentences are appropriate for computer crimes?*

No consensus appears to exist regarding the relative seriousness of the nonfraud crimes that may occur under 18 U.S.C. § 1030. Studies reveal substantial public ambivalence over appropriate punishment levels, especially with respect to computer hackers.

XI. Analysis of Options

The Commission appears to have three basic options regarding DOJ's proposal to amend the guidelines to focus more directly on computer crimes. First, it can pursue the development of a separate computer fraud and abuse guideline as DOJ initially proposed. Second, it can pursue a "middle approach" such as amending the commentary to U.S.S.G. §2F1.1 to give courts additional guidance on how loss should be calculated, and other harms considered, in computer cases. Based on very recent discussions with DOJ/CCU, it appears this middle approach could include amending the statutory index to reference existing guidelines other than §2F1.1 that might better fit some §1030 offenses and the harms they can cause. Third, the Commission could elect to make no immediate changes to the guidelines but monitor sentencing practice with respect to computer crimes to see if a change in the future is warranted.

A. Option I: Creating a New Computer Guideline

On balance, the considerations that might favor creating a new computer guideline appear modest in comparison to the arguments for a less far-reaching alternative. On the one hand, Congress has signaled its view that computer crime is potentially serious and that it wishes to increase public awareness of that potential seriousness. Congress has also enacted a statute covering conduct that can, in some instances, differ from traditional notions of fraud. The working group has identified two hotline calls and has been provided with the transcript from one sentencing hearing that provide some support for the notion that the guidelines should address computer-related harms more directly. How to treat consequential loss in computer cases appears to be the most significant of these unaddressed harms.

On the other hand, while these considerations may argue for more focus in the Guidelines Manual on computer crimes, they do not invariably point to the need for a separate computer *guideline*. Beyond these considerations, moreover, the information gathered to date may well favor an approach that is less ambitious than creating a new guideline.

The following considerations appear to weigh against a new computer guideline at this juncture.

1. Definitional Problems. The public comment submitted on the published DOJ proposal raises concerns about the complexity of defining harms that may flow from computer misconduct. DOJ/CCU candidly recognized that its published proposal had problems of this kind and subsequently offered to draft a guideline that would measure harms somewhat more generically, *i.e.*, by defining categories of harm such as "significant invasion of a person's privacy."⁴² This approach might not solve the definitional difficulties, however. Working group coders attempting to assess whether privacy interests were implicated in computer cases found, for example, that the occurrence of this harm was especially difficult to agree upon.⁴³ None of this is to say that definitional hurdles are insurmountable. They do appear challenging, however.
2. Just Punishment Concerns. Once computer-specific harms were defined, determining how to sanction them would appear more difficult than has been the case with other offense-specific harms. As the literature makes clear, no public consensus yet exists regarding, for example, the seriousness of "hacking" or "browsing" that involves unauthorized access or use but does not involve any significant damage to computerized information. DOJ/CCU expressed this ambivalence itself by advising the working group that in cases involving youthful hackers, prosecution -- let alone imprisonment -- could be counter-productive.⁴⁴

Similarly, it appears difficult to assign punishment to harms involving privacy invasion since invasion of privacy can occur in a vast array of forms and degrees.

3. Structural Concerns. DOJ/CCU and the literature the working group has surveyed confirm that prosecutors can and do use general fraud statutes to prosecute computer crimes. A separate computer guideline would raise technical issues stemming from this charging practice. As noted earlier, the Commission might have to adopt the real offense sentencing device of

⁴²See Section V.(B).

⁴³Coders ultimately determined that no cases involved "significant" privacy interests. See page 33.

⁴⁴The view expressed was that for a youthful hacker a felony conviction might have the undesirable effect of diminishing prospects for productive future employment, whereas intervention but no prosecution could prevent further criminal conduct without this effect.

cross-referencing computer fraud cases from U.S.S.G. §2F1.1, or, alternatively, list the computer guideline in the statutory index as potentially applicable to general fraud counts. Otherwise, subjective charging decisions could lead to the application of different guidelines, with different sentencing outcomes, for similar computer crimes.

4. Lack of Empirical Support. The working group's survey of cases sentenced under 18 U.S.C. § 1030 provided little additional support for the creation of a separate computer guideline.

First, most of the cases sentenced involved the types of harms that are regularly dealt with under guideline sections 2B1.1 and 2F1.1. Ninety percent of the cases examined involved some form of fraud, theft, or embezzlement.

Second, harms that DOJ identified as inadequately measured by loss tables apparently do not arise very frequently. None of the cases examined involved: a conscious or reckless risk of harm to health or safety; a conscious or reckless risk of interference with the conduct of foreign relations or the national defense; interference with a communications network providing communications service to the public; economic loss from system recovery costs; or a significant invasion of privacy.

Third, in the cases that involved the kinds of non-economic harms about which DOJ is particularly concerned, courts have typically imposed relatively lower, not higher, sentences. For example, the four defendants whose motivations appeared to be either to browse data, demonstrate computer prowess, or commit vandalism were all placed on probation. These four cases seem to show that some courts have the kind of ambivalence about the need for punishment in computer crime cases when fraud is not involved that was generally described in the literature. Relatively longer sentences were imposed in cases that involved interference with the administration of justice, but these cases also involved significant loss amounts that appeared to account for the higher sentences.

Fourth, the profile of defendants sentenced under 18 U.S.C. § 1030 reflects the "democratization" of computer crime noted in the literature. In other words, the computer crimes surveyed seemed to have been committed by persons who happened to have access to computers, often in the work place, and do not typically involve some special category of young, bright "whiz kids," as popular lore might suppose. In 64 percent of the cases surveyed, the offender or a co-conspirator was authorized to access the computer system; in 50 percent of the cases the offender was a current or former employee of the victim. Indeed, the profile of defendants sentenced under 18 U.S.C. § 1030 is similar to that of other defendants

sentenced under §2F1.1 generally, with the exception that defendants sentenced under 18 U.S.C. § 1030 were slightly better educated: approximately 90 percent of the defendants sentenced under 18 U.S.C. § 1030 graduated from high school and 52 percent later attended college, while approximately 76 percent of defendants sentenced under §2F1.1 graduated from high school and 43 percent later attended college.

B. Option II: Adding Loss Commentary and Amending the Statutory Index to Reference Guidelines Other Than §2F1.1 for Some Computer Crimes

The arguments noted as possibly supporting a separate guideline -- a congressional desire to highlight computer crimes and the unique quality of some harms that may result from computer crimes -- could be addressed through a "middle approach" falling between writing a new guideline and taking no action (but continuing to monitor cases).

Following recent discussions with Senior Staff and DOJ/CCU, this middle approach could involve 1) some expansion of the loss commentary in U.S.S.G. §2F1.1, and 2) exploring whether certain existing guidelines, such as §2B2.3 (Trespass), might already cover the harms occurring under some subsections of 18 U.S.C. § 1030 better than §2F1.1. This middle approach could have general advantages over the creation of new guideline.

First, definitional and just punishment problems could be more easily dealt with in commentary. For example, commentary could describe harms that are difficult to define -- such as privacy interests -- somewhat generally and note that where such harms occur to a significant degree the court should consider a departure.

Amending §2F1.1's loss commentary might be an especially good method for addressing DOJ/CCU's desire to factor consequential loss into the sentencing equation in computer cases. The §2F1.1 loss commentary already contains commentary explaining the relevance of consequential loss in product substitution and procurement cases.⁴⁵ Adding a discussion of consequential loss in computer crime cases would therefore be a comfortable fit with the current structure.

The approach of using revised loss commentary to build into the Guidelines Manual more guidance on computer-related harms may be supported by another consideration as well. The approach would leave courts with more unguided discretion in this area than a separate guideline -- a result not generally favored. However, in this instance courts would be using their discretion to establish an experiential data base and would have had the benefit of the expanded loss commentary discussing the targeted harms. This data base could be helpful to the Commission should it choose to address these harms in a more binding fashion in the future.

⁴⁵See U.S.S.G. §2F1.1, comment. (n.7(c)).

This benefit seems particularly valuable in light of information DOJ/CCU provided the working group on pending cases. While the working group found only 76 guideline cases in which the statutes of conviction included 18 U.S.C. § 1030, DOJ/CCU advised the working group in June that there were some 215 computer crime cases "pending." According to DOJ/CCU, many of these cases are in an investigative stage and will not result in prosecution, but the high number of pending cases may suggest that the volume of computer crime sentencings will soon increase. If this is true, the Commission would be in a considerably better position to conduct empirical analyses in the not-too-distant future than it is today. This may further support holding off on adoption of a new computer fraud guideline at this juncture.

Because the loss commentary to §2F1.1 has undergone several revisions in recent years, there may be some concern about extensively expanding it now. As this Report was nearing deadline, there appeared to be a developing consensus between the working group, Senior Staff, and DOJ/CCU that the "middle approach" might be able to avoid this problem. Specifically, it appears that a number of existing guidelines might fit the harms that are likely to occur under certain §1030 subsections better than §2F1.1.

For example, §2B2.3, covering trespass, might be a better fit than §2F1.1 for §1030(a)(3) offenses, which involve accessing a government computer thereby "affecting [its] use." Similarly, §2B1.3, covering property damage and destruction, might be a better fit than §2F1.1 for hacking cases prosecuted under §1030(a)(5).

To the extent that guidelines other than §2F1.1 are deemed to better cover the unique computer harms about which DOJ/CCU has expressed concern, the need to amend §2F1.1's loss commentary would be lessened. Relatively straightforward amendments to the statutory index and perhaps modest changes to the newly referenced guidelines would achieve the desired result.

C. Option III: Taking No Action Now But Continuing to Monitor Cases

The relatively few cases sentenced, the larger number apparently "in the pipeline," and the definitional and just punishment concerns noted, could argue for the Commission holding off on any changes at present in favor of further monitoring of developments. Making no changes would have drawbacks, however.

There is little question that 18 U.S.C. § 1030 does include harms that are not well covered by §2F1.1 and its existing commentary. Although the working group found little incidence of most of these harms in the case survey it conducted, to the extent these harms will show up in the future -- and DOJ/CCU believes they will -- the guidelines do not presently offer any guidance as to how they should be treated. A new guideline or the "middle approach" would provide the missing guidance.

XII. Conclusion

Based on the foregoing, and absent contrary directions from the Commission, the working group proposes to pursue Option II, or the "middle approach," at this juncture. DOJ/CCU seems to recognize the validity of the working group's conclusion that the case for a new computer fraud guideline is not that strong. The middle approach -- revising §2F1.1's loss commentary and exploring whether guidelines other than §2F1.1 may fit some computer crimes better than §2F1.1 -- allows the working group to move forward in attempting to address DOJ/CCU's concerns.

Appendix A

Proposed Amendment on Computer

Fraud and Abuse

59. **Synopsis of Amendment:** *This amendment creates a new guideline applicable to violations of the Computer Fraud and Abuse Act of 1988 (18 U.S.C. §1030). Violations of this statute are currently subject to the fraud guidelines at §2F1.1, which rely heavily on the dollar amount of loss caused to the victim. Computer offenses, however, commonly protect against harms that cannot be adequately quantified by examining dollar losses. Illegal access to consumer credit reports, for example, which may have little monetary value, nevertheless can represent a serious intrusion into privacy interests. Illegal intrusions in the computers which control telephone systems may disrupt normal telephone service and present hazards to emergency systems, neither of which are readily quantifiable. This amendment proposes a new Section 2F2.1, which provides sentencing guidelines particularly designed for this unique and rapidly developing area of the law.*

Proposed Amendment: Part F is amended by inserting the following section, numbered §2F2.1, and captioned "Computer Fraud and Abuse," immediately following Section 2F1.2:

"§2F2.1. Computer Fraud and Abuse

- (a) Base Offense Level: 6
- (b) Specific Offense Characteristics
 - (1) Reliability of data. If the defendant altered information, increase by 2 levels; if the defendant altered protected information, or public records filed or maintained under law or regulation, increase by 6 levels.
 - (2) Confidentiality of data. If the defendant obtained protected information, increase by 2 levels; if the defendant disclosed protected information to any person, increase by 4 levels; if the defendant disclosed protected information to the public by means of a general distribution system, increase by 6 levels.

Provided that the cumulative adjustments from (1) and (2), shall not exceed 8.

- (3) If the offense caused or was likely to cause
 - (A) interference with the administration of justice (civil or criminal) or harm to any person's health or safety, or
 - (B) interference with any facility (public or private) or communications network that serves the public health or safety,increase by 6 levels.
- (4) If the offense caused economic loss, increase the offense level according to the tables in §2F1.1 (Fraud and Deceit). In using those tables, include the following:
 - (A) Costs of system recovery, and
 - (B) Consequential losses from trafficking in passwords.
- (5) If an offense was committed for the purpose of malicious destruction or damage, increase by 4 levels.

(c) Cross References

- (1) If the offense is also covered by another offense guideline section, apply that offense guideline section if the resulting level is greater. Other guidelines that may cover the same conduct include, for example: for 18 U.S.C. § 1030(a)(1), §2M3.2 (Gathering National Defense Information); for 18 U.S.C. § 1030(a)(3), §2B1.1 (Larceny, Embezzlement, and Other Forms of Theft), §2B1.2 (Receiving, Transporting, Transferring, Transmitting, or Possessing Stolen Property), and §2H3.1 (Interception of Communications or Eavesdropping); for 18 U.S.C. § 1030(a)(4), §2F1.1 (Fraud and Deceit), and §2B1.1 (Larceny, Embezzlement, and Other Forms of Theft); for 18 U.S.C. § 1030(a)(5), §2H2.1 (Obstructing an Election or Registration), §2J1.2 (Obstruction of Justice), and §2B3.2 (Extortion); and for 18 U.S.C. § 1030(a)(6), §2F1.1 (Fraud and Deceit) and §2B1.1 (Larceny, Embezzlement, and Other Forms of Theft).

Commentary

Statutory Provisions: 18 U.S.C. §§ 1030(a)(1)-(a)(6)

Application Notes:

1. This guideline is necessary because computer offenses often harm intangible values, such as privacy rights or the unimpaired operation of networks, more than the kinds of property values which the general fraud table measures. See §2F1.1, Note 10. If the defendant was previously convicted of similar misconduct that is not adequately reflected in the criminal history score, an upward departure may be warranted.
2. The harms expressed in paragraph (b)(1) pertain to the reliability and integrity of data; those in (b)(2) concern the confidentiality and privacy of data. Although some crimes will cause both harms, it is possible to cause either one alone. Clearly a defendant can obtain or distribute protected information without altering it. And by launching a virus, a defendant may alter or destroy data without ever obtaining it. For this reason, the harms are listed separately and are meant to be cumulative.
3. The terms "information," "records," and "data" are interchangeable.
4. The term "protected information" means private information, non-public government information, or proprietary commercial information.
5. The term "private information" means confidential information (including medical, financial, educational, employment, legal, and tax information) maintained under law, regulation, or other duty (whether held by public agencies or privately) regarding the history or status of any person, business, corporation, or other organization.
6. The term "non-public government information" means unclassified information which was maintained by any government agency, contractor or agent; which had not been released to the public; and which was related to military operations or readiness, foreign relations or intelligence, or law enforcement investigations or operations.
7. The term "proprietary commercial information" means non-public business information, including information which is sensitive, confidential, restricted, trade secret, or otherwise not meant for public distribution. If the proprietary information has an ascertainable value, apply paragraph (b) (4) to the economic loss rather than (b) (1) and (2), if the resulting offense level is greater.

8. Public records protected under paragraph (b) (1) must be filed or maintained under a law or regulation of the federal government, a state or territory, or any of their political subdivisions.
9. The term "altered" covers all changes to data, whether the defendant added, deleted, amended, or destroyed any or all of it.
10. A "general distribution system" includes electronic bulletin board and voice mail systems, newsletters and other publications, and any other form of group dissemination, by any means.
11. The term "malicious destruction or damage" includes injury to business and personal reputations.
12. Costs of system recovery: Include the costs accrued by the victim in identifying and tracking the defendant, ascertaining the damage, and restoring the system or data to its original condition. In computing these costs, include material and personnel costs, as well as losses incurred from interruptions of service. If several people obtained unauthorized access to any system during the same period, each defendant is responsible for the full amount of recovery or repair loss, minus any costs which are clearly attributable only to acts of other individuals.
13. Consequential losses from trafficking in passwords: A defendant who trafficked in passwords by using or maintaining a general distribution system is responsible for all economic losses that resulted from the use of the password after the date of his or her first general distribution, minus any specific amounts which are clearly attributable only to acts of other individuals. The term "passwords" includes any form of personalized access identification, such as user codes or names.
14. If the defendant's acts harmed public interests not adequately reflected in these guidelines, an upward departure may be warranted. Examples include interference with common carriers, utilities, and institutions (such as educational, governmental, or financial institutions), whenever the defendant's conduct has affected or was likely to affect public service or confidence."

Appendix B

Purpose Statement

3/9/93

AGENDA ITEM



March 2, 1993

MEMORANDUM

TO: Phyllis J. Newton
Staff Director

FROM: Computer Fraud Working Group
Win Swenson, Nolan Clark, David Rauma, John Scalia

SUBJECT: Purpose Statement

I. Introduction

In 1988, Congress enacted the Computer Fraud and Abuse Act of 1988. The Act established several new offenses that are codified at 18 U.S.C. § 1030 under the caption "Fraud and related activity in connection with computers." The Commission amended the guidelines' statutory index to indicate appropriate guidelines for the various subsections of this new statutory provision, but otherwise did not amend the guidelines in response to the Act. As amended, the statutory index refers the user to the fraud guideline, §2F1.1, for all but one of the violations established under 18 U.S.C. § 1030. The statutory index refers the user to U.S.S.G. §2M3.2 for violations of the statute involving national security data. See 18 U.S.C. § 1030(a)(1).

The caption for 18 U.S.C. § 1030 appropriately indicates that the scope of conduct prohibited by this provision extends considerably beyond traditional notions of fraud to other "related activity in connection with computers." In general terms, the statute prohibits:

- knowingly accessing a computer without authorization to obtain national security data (subsection (a)(1));
- intentionally accessing a computer without authorization to obtain certain confidential financial information (subsection (a)(2));

- intentionally accessing a government computer thereby "affect[ing] the use of the Government's operation of such computer" (subsection (a)(3));
- accessing a computer with intent to defraud and thereby obtaining anything of value (subsection (a)(4));
- intentionally accessing a computer without authorization to, among other things, alter information thereby causing a loss of at least \$1,000 (subsection (a)(5)); and
- trafficking in a password or similar information through which a computer can be accessed without authorization, knowingly and with intent to defraud (subsection (a)(6)).

The maximum penalties for these various categories of conduct range from one year to ten years imprisonment (and/or a fine).

Because some forms of the conduct proscribed by 18 U.S.C. § 1030 involve harms that are either nonmonetary (e.g., national security, privacy) or otherwise not covered by §2F1.1's loss definition (e.g., the consequential loss caused by various kinds of disruptions to computer security systems, software, data bases, etc.) the Department of Justice has suggested that a new guideline be drafted to address these harms with greater specificity than does §2F1.1. To that end, the Commission has agreed to publish, at the Department's request, a proposed new §2F2.1 in this year's published amendment package. See Proposed Guideline Amendment No. 59.

The Computer Fraud Working Group recommends that a detailed analysis of this proposal, including possible amendment and nonamendment alternatives to it, constitute the group's principal objective.

II. The Proposed Approach

A. *Public Comment*

~~Because the~~ Commission has already published and is in the midst of the comment period with respect to the Department's amendment proposal, the Working Group may be in the unusual position of having public comment to consider at the very outset of its work. The Working Group will study and evaluate any comment received.

B. *Empirical Study*

The Computer Fraud Working Group will conduct a special study of computer offenses involving convictions under 18 U.S.C. § 1030. The primary focus of this study will be to collect information about specific offense characteristics that are included in the Justice Department's proposed amendment. These characteristics include alteration of information, access to confidential information, costs of system recovery, and consequential losses to the victim. If other common offense/offender characteristics are identified through discussions with interested parties, case law, or a preliminary reading of guideline cases involving convictions under 18 U.S.C. § 1030, information about these characteristics will also be collected. At present, the number of sentenced cases appears to be quite low (less than 20 per year) and, as a result, all available cases will be included in the data collection effort.¹

C. *Consultation With Interested Parties*

In addition to consulting with appropriate representatives of the Justice Department, the Working Group will seek input from representatives of the defense bar and public interest groups that monitor computer crime and related issues.

D. *Case Law*

Reported court decisions involving computer crime -- both the construction of 18 U.S.C. § 1030 and the application of the guidelines to computer cases -- will be analyzed. The Working Group has been preliminarily advised that there are few reported decisions due to the newness of the relevant statute.

E. *Hotline and TAS*

The Working Group will consult with the Technical Assistance Staff to see what, if any, experience that unit has had with sentencing in computer crime cases.

¹According to officials at the Justice Department, computer-related crimes are also prosecuted under 18 U.S.C. § 2701 (Unlawful access to stored communications) and various commonly used fraud statutes. A preliminary review of cases indicates that prosecutions of computer crimes exclusively under § 2701 occur infrequently. Nevertheless, to the extent the Working Group identifies such cases, they would be included in the study. Because the general fraud statutes under which some computer crimes are prosecuted are so frequently used for unrelated kinds of cases, the Working Group does not propose to comb through the voluminous number of prosecutions involving these statutes to identify what, we are advised, should be a relatively small number of computer-related offenses.

F. *Legislative History*

The Working Group will analyze the legislative history to the Computer Fraud and Abuse Act to see if it provides additional guidance on appropriate approaches to sentencing in this area.

G. *Literature*

The Working Group will canvass any relevant literature for additional guidance.

III. *Timing*

At the Commission's direction, the Computer Fraud Working Group has been established as a two-year working group. Accordingly, the Working Group will adhere to the schedule established by the Staff Director for two-year groups.

IV. *Résources*

Because of 1) the small number of cases that will require inclusion in the Working Group's empirical study, 2) the apparently limited amount of reported case law and other experience (e.g., hotline) with these cases, and 3) the fact that the Working Group will have the benefit of considering an already-drafted, proposed amendment in this area, total resource demands should, relative to most working groups, be quite modest. It is expected that the four members of the group (perhaps in time augmented by Melissa Selick, an originally named member now on maternity leave) will be able to carry out the group's work without a substantial impact on the rest of their duties. Modest additional support staff resources (mostly secretarial) will also be required.

Appendix C

Survey of the Literature on Computer Crime

SURVEY OF THE LITERATURE ON COMPUTER CRIME

Computer-related crime has generated extensive literature. We have surveyed a portion of that literature, ascertaining its relevance to issues relating to appropriate sentencing for violations of 18 U.S.C. § 1030 (Fraud and related activity in connection with computers). The relevant information has been organized in terms of a number of questions:

- What is the nature of computer crime?
- Who commits computer crimes?
- How much computer crime is committed and how much loss results from such crime?
- What explains the relative paucity of computer crime prosecutions?
- What sentences are appropriate for computer crimes?

1. What is the nature of computer crime?

Computer crime "has evaded a solid definition."¹ Donn Parker, one of the earliest publicists of computer crime and abuse, used clippings to prepare a data base on all forms of computer misuse.² Rather than define computer crime, Parker instead classified the possible relationships that may exist between computers and crime. He claimed that all known and reported cases of computer crime involve one or more of four roles: object; subject; instrument; and symbol.³

Crimes in which the computer is a direct object of the offense include, sabotage, vandalism, arson, or physical abuse directed against the computer "hardware." Crimes in which the computer is used as an instrument include: "fraud, theft, robbery, arson, embezzlement, extortion, conspiracy, sabotage, espionage, and more."⁴ Computer crimes in which the computer is a symbol can involve using the computer "as a symbol for intimidation or deception," e.g., an "organization falsely claiming to use nonexistent computers."⁵

¹Barry J. Hurewitz and Allen M. Lo, "Computer-Related Crimes," 30 Am. Crim. L. Rev. 495 (1993).

²Donn Parker of Stanford Research Institute, in 1973, published his first survey, Computer Abuse, as a report, co-authored by Susan Nycum and Stephen Dura. This survey was followed by D. Parker, Crime by Computer (1976).

³Donn Parker, Computer Crime: Crim. Just. Resource Manual Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 2 (2d ed., Aug. 1989).

⁴*Id.* at 3.

⁵*Id.*

In addition, Parker identified techniques by which computer crime and abuse can occur. Initially, twelve techniques were identified.⁶ That list has since expanded and now includes: eavesdropping and spying; scanning; masquerading; piggybacking and tailgating; false data entry (data diddling); superzapping; scavenging and reuse; Trojan horses; computer viruses; salami techniques; trap doors; logic bombs; asynchronous attacks; data leakage; computer program piracy; computer and computer components larceny; and use of computers for criminal enterprise.⁷

This early, and somewhat unscientific, literature on computer crime and abuse was significantly affected by two critical articles by John Taber.⁸ As BloomBecker has stated: "Taber came out of nowhere and challenged [the] reigning computer security orthodoxy. He demonstrated how much of the statistical and anecdotal evidence of computer crime was myth and not scholarship."⁹

Taber defined computer crime as "a crime that, in fact, occurred and in which a computer was directly and significantly instrumental."¹⁰ Although Taber's definition has

⁶See Christopher D. Chen, Note, Computer Crime and the Computer Fraud and Abuse Act of 1986, 10 Computer/L. J. 71, 73 (1990).

⁷U.S. Department of Justice, *supra* note 3, at 9-25.

⁸John K. Taber, On Computer Crime, 1 Computer/L. J. 517-543 (1979); John K. Taber, A Survey of Computer Crime Studies, 2 Computer/L. J. 275-327 (1980).

⁹Buck BloomBecker, Spectacular Computer Crimes, 67 (1990).

¹⁰*Id.* at 68.

not been uniformly adopted, it has forced other analysts to be more careful. Parker, himself, responding to Taber, retreated to a narrower definition of computer-related crime as being "any illegal act where a special knowledge of computer technology is essential for its perpetration, investigation or prosecution."¹¹¹²

Other definitions for computer crime have been offered. One of the narrowest and most precise is that used by The National Center on Computer Crime Data (NCCCD). The NCCCD defines computer crime "as that which the law in a specific jurisdiction defines as computer crime in its computer crime law." Gemignani reserves the term computer crime "for traditional crimes which have acquired a new dimension or order of magnitude through the aid of a computer, and abuses which have come into being because of computers."¹³ Comer, in his book on corporate fraud,¹⁴ argues that "any financial dishonesty that takes place in a computer environment is a computer fraud."¹⁵ Mandell asserts that computer crime consists of two kinds of activity:

¹¹U.S. Department of Justice, *supra* note 3.

¹²In addition, Parker has used the term "computer abuse" -- defined as "any intentional act associated in any way with computers where a victim suffered, or could have suffered, a loss, and a perpetrator made, or could have made, a gain." BloomBecker, *supra* note 9, at 69.

¹³Michael C. Gemignani, What is Computer Crime, and Why Should We Care?, 10 U. Ark. Little Rock L. 55, 56 n.4 (1987-88).

¹⁴M. J. Comer, *Corporate Fraud* (2d ed. 1985).

¹⁵Martin Wasik, *Crime and the Computer*, 1 n.4 (1991).

(a) the use of a computer to perpetrate acts of deceit, theft or concealment that are intended to provide financial, business-related, property or service advantages; and (b) threats to the computer itself, such as theft of hardware or software, sabotage and demands for ransom.¹⁶

Some analysts have gone so far as to argue that computer crime is not unique, but rather traditional crimes committed in new ways. For example, Reimer has asserted: "Computer crimes are not new crimes, they are the same old crimes committed in fresh and inventive ways made possible by the high technology of today's computers and telecommunications."¹⁷

The argument that computer crime is not unique has some validity,¹⁸ but is overstated. Although many computer crimes could be prosecuted under traditional crime statutes,¹⁹ some types of computer abuse are unique, making it very difficult to

¹⁶*Id.* at 2 (quoting S. L. Mandell, *Computers, Data Processing and the Law*, 155 (1984)).

¹⁷Chen, *supra* note 6, n.7.

¹⁸For example, in 1980, Taber using his narrow definition of computer crime, "reviewed the 375 files in the data base maintained by Donn Parker at SRI in Menlo Park, California . . . and found only two he accepted as falling within this definition." BloomBecker, *supra* note 9, at 68.

¹⁹That is, crimes in which the computer is an object, a symbol, or an instrument are typically not new forms of criminal conduct. Indeed, Nycum has identified at least 40 federal statutes that could be applied to computer-related violations. See Richard C. Hollinger and Lonn Lanza-Kaduce, *The Process of Criminalization: The Case of Computer Crime Laws*, 26 *Criminology* 101, 103 (1988) (citing Susan Nycum, *The Criminal Law Aspects of Computer Abuse: Part II -- Federal Criminal Code*, 5 *Rutgers J. of Computers and L.*, 297-322 (1979)).

prosecute them under traditional criminal statutes. Such abuse typically is conduct in which the computer is the subject of the offense. Specifically, in the new "paperless office," proprietary information stored in a computer memory or on an electronic medium can be accessed, altered, stolen, and sabotaged without the perpetrator's being physically present or resorting to the use of force. Thus, it is the intangible, electronic-impulse nature of computerized information that has caused the greatest concern in the legal community over possible loopholes in criminal law."²⁰

In particular, legal questions existed with regard to three types of conduct:

(1) the copying of electronic data; (2) the unauthorized access or electronic "browsing" of sensitive or confidential material; and (3) the infliction of damage to computer programs or data held in a computer. To address these types of conduct, statutes were enacted at both state and federal levels creating new types of computer crimes.

2. Who commits computer crime?

Donn Parker, in his first book, Crime by Computer, characterized computer criminals as follows:

²⁰Richard C. Hollinger & Lon Lanza-Kaduce, The Process of Criminalization: the Case of Computer Crime Laws, 26 *Criminology* 101, 103 (1988).

Perpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the characteristics that make them highly desirable employees in data processing.²¹

This characterization of computer criminals, although not particularly helpful,²² has been adopted by journalists and by security consultants.²³ With the proliferation of computers, however, "the phrase 'computer people' must now be expanded substantially to take account of the increasing numbers of computer-aware employees who have legitimate access to desk-top micros."²⁴ This expansion renders Parker's characterization somewhat dated.

Two principal studies provide more detailed information regarding the nature of computer criminals in the United States. The first was a survey in 1984 by the American

²¹See BloomBecker, *supra* note 9, at 38.

²²BloomBecker, *supra* note 9, at 38.

²³This is because such a classification does not help to distinguish persons likely to commit crimes. Indeed, as Mandell has stated: "The popular view of the successful computer criminal is interesting and somewhat unsettling. Most companies would be eager to hire personnel who fit this description." See Wasik, *supra* note 15, at 60.

²⁴Wasik, *supra* note 15, at 61.

Bar Association.²⁵ The second is the compilation by the National Center on Computer Crime Data of cases prosecuted on computer-crime statutes.

In the ABA survey, nearly 40 percent of the perpetrators were not identified. Of the remainder, programmers tended to predominate, with a fairly even balance of executives, computer operators, supervisors, workers, outside consultants, and individuals having no prior link with the organization. The survey found, though, that more cases (125) came from within the organization suffering the loss than from outside it (73 cases).

The NCCCD data provides a more detailed breakdown: "programmer (21 per cent), student (14 per cent), input clerk (14 per cent), bank teller (10 per cent), accomplice (10 per cent), unskilled (7 per cent), unemployed (7 per cent), employee with access (6 per cent), computer executive (5 per cent), and miscellaneous (6 per cent)."²⁶

Reviewing cases involving "rogue computer programs," Anne Branscomb identified the following varieties of perpetrators: (1) employees; (2) software developers; (3) pranksters; (4) professionals ("those with criminal intent, those who are apprentices attempting to improve their skills, and those who are deliberately attempting to break

²⁵American Bar Association, Task Force on Computer Crime, Report on Computer Crime, Washington, D.C.: Government Printer, 1984.

²⁶Wasik, *supra* note 15, at 60.

into closed systems in order to test their vulnerability and increase awareness of the defects"); (5) cyberpunks ("computer skilled but anti-social individuals who deliberately disrupt computer systems merely for the joy and person satisfaction which comes from such achievement"); and (6) saboteurs or terrorists ("So far there have been no incidents of entries which have been publicly disclosed of deliberate destruction or interruption of service attributed to terrorists groups, although there have been incidents of voyeurism and espionage.")²⁷

The literature indicates that computer criminals and abusers, whatever their occupation, are typically either employees or ex-employees of the company that is the victim.²⁸ For example, the latest NCCCD survey as of 1990 indicated that employees committed 75 percent of the computer crimes prosecuted in the United States.²⁹ Moreover, the data also indicate that in many cases the perpetrators have rudimentary computer skills. For example, West German studies found that 90 percent of detected computer criminals were employees of the victim firm and that 60 per cent (typically in the field of input manipulation) did not have specialist skills.³⁰

²⁷Anne W. Branscomb, Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime, 2 Rutgers Computer and Tech. L. J. 1, 27-28 (1990).

²⁸Wasik, *supra* note 15; BloomBecker, *supra* note 9, at 49.

²⁹BloomBecker, *supra* note 9, at 37.

³⁰Wasik, *supra* note 15.

3. How much computer crime is committed and how much loss results from such crime?

Most estimates concerning the amount of computer crime have been based on the newspaper clippings assembled by Donn Parker and the 1984 ABA survey. After these data sources were criticized by Taber, most analysts concluded that we do not know how much computer crime is committed.³¹

In 1973, Parker claimed, based on his clippings, that the annual world-wide loss from computer misuse was \$300 million, and that the average loss per case was \$450,000.³² In the 1984 survey by the ABA Computer Crime Task Force, 283 companies out of 1,000 responded. One hundred sixty of these companies stated that they had suffered from some form of computer crime. The Task Force estimated from this survey that total annual losses from computer crimes in the United States were somewhere in the range from \$145 million and \$730 million.³³

A 1984 survey by the American Institute of Certified Public Accountants (AICPA) provides a much lower estimate of the incidence of computer crimes. Their survey of 9,405 banks and 1,232 insurance companies indicated that only 2 percent of the banks

³¹See generally Wasik, *supra* note 15, at 34-41; BloomBecker, *supra* note 9, at 72-75; Holliger, Lanza-Kaduce, *supra* note 19, at 105-107.

³²Wasik, *supra* note 15, at 34.

³³*Id.* at 36.

and 3 percent of the insurance companies had found instances of computer fraud. After reviewing the cases, the AICPA concluded that only 85 of the cases submitted by the banks and 34 of the cases submitted by the insurance companies fit the study's working definition of computer fraud.³⁴

A more rigorous approach to the measurement of computer crime and abuse is to rely exclusively on "censuses" of cases prosecuted under computer-crime statutes. This approach has been used by the National Center for Computer Crime Data. The NCCCD estimated "only several hundred prosecuted computer crimes cases per year in 1986," as compared with "several thousand cases prosecuted per year" in 1989.³⁵ Thus, although prosecutions have increased, it is not clear whether the incidence of crime has increased.

With regard to magnitude of loss, the NCCCD census indicated that 60 percent of the prosecuted cases involved a loss of less than \$10,000, while 87 percent involved a loss of less than \$100,000.³⁶ Despite this data, BloomBecker concludes that the average loss is actually greater, based upon "surveys of computer security professionals [that] suggest that the average annual loss from computer crime is about one-half billion' and 'that

³⁴*Id.*

³⁵BloomBecker, *supra* note 9, at 74-75.

³⁶*Id.* at 75.

only about six percent of the serious computer security incidents were reported for prosecution." ³⁷

4. What explains the relative paucity of computer crime prosecutions?

Commentators generally agree that the volume of computer crime prosecutions is low relative to the estimated amount of computer crime. Although this assumed paucity cannot be documented, explanations have been offered for the assumed paucity.

Just as it is impossible to measure the magnitude of computer crime, so is it impossible to measure the magnitude of computer crime prosecutions. The NCCCD tallies the number of prosecutions under special computer-crime statutes. Although the literature indicates that prosecutors tend to rely on traditional criminal statutes, no one knows how many computer-related crimes are prosecuted under other statutes..³⁸ Accordingly, the actual volume of computer crime prosecutions may be much larger than reported.

In any event, relatively few defendants have been prosecuted under the federal computer-crime statute, the 1986 Computer Fraud and Abuse Act. A number of

³⁷*Id.* at 74-75.

³⁸*See, e.g.,* Carol C. McCall, Note, Computer Crime Statutes: Are They Bridging the Gap Between Law and Technology, 11 *Crim. Just. J.* 203, 215-16 (1988).

possible explanations have been given, such as "the relatively sparse reporting of computer crime, the difficulty of prosecuting computer crime, or the ease of prosecution under more traditional crime statutes."³⁹

A number of reasons have been given why victims may choose not to report computer crimes:

- reported losses may be embarrassing;
- bad publicity may reduce customers' confidence level;
- the cost of prosecution may outweigh the benefits;
- reporting may not lead to prosecution;
- prosecution is unlikely to result in restitution.⁴⁰

³⁹Cynthia K. Nicholson and Robert Cunningham, Computer Crime, 28 Am. Crim. L. Rev. 393, 397 (1991).

⁴⁰See Chen, *supra* note 6, at 82. Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem, 43 Vanderbilt L.Rev. 453, 485-86 (1990).

Another possible reason is that victims may have concluded, as did Congress,⁴¹ that internal security measures are the most effective means of deterring computer crime.

Finally, Hollinger and Lanza-Kaduce argue that the relatively few prosecutions under computer crime statutes is consistent with the underlying purpose of those statutes. Specifically, the computer crime laws "possess a significant symbolic component" . . . "in the sense that the laws communicated cultural normative messages about the use and abuse of the expanding computer technology."⁴² In other words, the computer crime laws are intended as much to heighten awareness about what is acceptable conduct as to punish for breaches of that code of acceptability.

If the primary function of the new computer crime statutes was to deter rampant abuse, one would expect the new laws to result in vigorous prosecutions. The number of prosecutions under the new computer crime laws, however, has been surprisingly low, especially when contrasted with the media-created images of rampant abuse by groups of hackers collaborating to share passwords to break into systems. From 1978 to 1986, fewer than 200 criminal prosecutions were initiated nationally. Under the nation's oldest statute, Florida's, fewer than a half-dozen prosecutions had been filed in its first 5 years. At the same time, some of the most visible offenders (e.g., the "414 hackers"), who could have become the

⁴¹S. Rep. No. 432, 99th Cong., 2d Sess. 3 (1986), reprinted in 1986 U.S. C. C. A. N. 2479.

⁴²Hollinger & Lanza-Kaduce, *supra* note 19, at 114.

clearest examples for general deterrence, have been dealt with leniently. This meager enforcement pattern might undermine direct utilitarian strategies like deterrence, but it is consistent with symbolic functions of law formation.⁴³

5. What sentences are appropriate for computer crime?

Some public ambivalence is evident regarding appropriate sentences for computer crimes. This ambivalence appears in a number of contexts: the enactment of computer crime legislation, police and prosecutor actions with regard to reported computer crimes, employer reactions to computer abuse, judicial sentencing for computer crimes, and attitudes of the general public regarding appropriate sentences for computer crimes.

Based on their study of the process of the criminalization of computer crime law, Hollinger and Lanza-Kaduce conclude that there was no public demand for criminalization:

Public opinion neither called for nor opposed the criminalization of computer abuse. In fact, there was very little direct pressure on legislators from any interest group -- moral or economic. Nor were there any "moral entrepreneurs" zealously seeking to legislate morality. Instead, individual state and federal lawmakers took the initiative. "Computer crime" presented activist

⁴³*Id.* at 117.

legislators with an ideal issue with which to maximize personal media exposure without offending any major constituency. To legitimize their campaign, the legislators enlisted technical experts on computer abuse, who also gained recognition for themselves and their work.⁴⁴

According to Gemignani, this ambivalence carries over to police and prosecutors:

The ambivalent attitude towards computer crimes is exemplified by the reluctance sometimes shown by police and prosecutors to pursue the computer criminal. The technology requires special expertise, with preparation of a case against a suspect time-consuming and tedious.⁴⁵

Further, it appears that employers are often reluctant to impose discipline upon employees who engage in computer misconduct. The ABA Report indicated that in "less than half of the cases did the employer take any disciplinary action against the perpetrator."⁴⁶

⁴⁴*Id.* at 113.

⁴⁵Gemignani, *supra* note 13, at 56.

⁴⁶*Id.* at 56 n.6.

In the view of Gemignani, "nowhere, however, is the ambivalence toward computer crime demonstrated more forcefully than in the courts."⁴⁷ Gemignani cites one case that allegedly involved the theft of more than a million dollars worth of equipment for which the defendant served four days and paid a \$500 fine, and a second case that involved a wire transfer of over \$10 million for which the defendant received a seven-year term, "but only because he tried the same trick again while awaiting trial."⁴⁸

Part of the ambivalence noted by Gemignani may be no more than the ambivalence regarding the appropriate sentencing of white-collar criminals. After all, in the case involving the wire transfer of over \$10 million, the defendant, himself, made no direct use of any computer.

However, some of the perceived ambivalence regarding sentencing of computer criminal is clearly real. In particular, public attitudes are split regarding the appropriate sentences for "hackers." This split was most evident with regard to the case involving Robert Morris -- the first person convicted by a jury of a felony under the Computer Fraud and Abuse Act of 1986.⁴⁹

⁴⁷*Id.* at 56.

⁴⁸*Id.* at 56 n.7.

⁴⁹A full discussion of Robert Morris and the Internet worm is contained in Katie Hafner and John Markoff, *Cyberpunk: Outlaws and Hackers on the Computer Frontier*, 253-341 (1991).

Morris was a graduate student at Cornell University, who was conducting research on the subject of computer security. Morris found some bugs in the sendmail program used on the Internet network system. One bug allowed him to enter through a "back door." A second bug let him run a program on a second machine without logging in. Through an MIT computer, Morris introduced a worm into the Internet system. The worm was designed to be as innocuous as possible. Morris, however, made an error in his programming, causing the worm to replicate itself very rapidly. As a consequence, about 600 computers on the Internet system went down. When Morris discovered that computers were crashing, he sent a message containing a fix. In the meantime, though, the entire Internet system was in a state of disarray.

After an eight-month deliberation regarding whether to prosecute, Robert Morris was indicted on one felony count of violating the Computer Fraud and Abuse Act of 1986. After a jury trial, Morris was convicted and then sentenced to pay a \$10,000 fine, serve three years' probation, and perform four hundred hours of community service.

The Morris prosecution and sentence imposed split both computer scientists and the larger community. Some viewed Morris as a brilliant kid whose experiment fouled up; others viewed him as a public menace. Some thought the sentence was fair; others thought that a jail sentence was necessary to send a message to other hackers.⁵⁰

⁵⁰The National Center for Computer Crime Data held an "If I Were the Judge in the Robert Morris Case" essay contest. The responses were "split between those stressing punishment and those favoring 'not wasting' Morris' computer expertise." BloomBecker,

The Robert Morris case appears to be the type of computer crime case that causes the greatest ambivalence. One on hand, Morris' conduct did not violate traditional criminal statutes, nor had Morris intended to cause harm. On the other hand, Morris had acted recklessly, and caused an estimated damage of \$160,000.

One law student analyst, assessing the Morris case from retributive and utilitarian perspectives, concluded: "Ultimately, neither of the traditional arguments for criminal punishment -- retribution and utilitarianism -- provide[s] a justification for criminal punishment of hackers."⁵¹ This argument, however, was applicable to a narrow set of cases:

the introduction of a computer worm might be included whereas the introduction of a virus -- a program that typically destroys or scrambles data -- would not. Innocuous forms of computer 'prowling' would not justify punishment, though we might be justified in sentencing the unauthorized use of information gathered in that fashion.⁵²

"Hang the Hacker of Honor Him?" Security 31 (June 1990).

⁵¹Brenda Nelson, Note, Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm, 11 Computer/L. J. 299, 304 (1991).

⁵²*Id.* at 319.