COMPUTER ABUSE AND COMPUTER CRIME AS ORGANIZATIONAL ACTIVITIES

ROB KLING

Reprinted from
COMPUTER/LAW JOURNAL
Volume II, Spring 1980, Number 2

COMPUTER ABUSE AND COMPUTER CRIME AS ORGANIZATIONAL ACTIVITIES

By ROB KLING*

INTRODUCTION

"Computer abuse," "computer crime," and "computer fraud" are sensitizing concepts; they suggest that unsavory practices differ in significant ways from "usual" events when a computer is employed as a critical instrument. For example, individual thefts may more easily be in hundreds of thousands or even millions of dollars because of the volume of funds accessible in computerized accounts.[1] Frauds may be more difficult to uncover, since computerized files are often substantially more complex and difficult to audit than their manual precursors.[2] The overcharging of supermarket customers may become more common with product scanners and the disappearance of individually marked prices on each item, since custom-

* Professor, Department of Information and Computer Science, University of California, Irvine, California. The author wishes to acknowledge the helpful comments of Jay Becker, Robert Bigelow, Sharon Davis, Elihu Gerson, Donn Parker and Susan Strom on earlier drafts of this article.

1. Most analysts of computer crime emphasize the extent to which automated data systems are vulnerable to large scale thefts. *See, e.g.,* Allen, *The Embezzler's Guide to Computer Systems*, 53 HARV. BUS. REV., July-Aug. 1975, at 75; Kling, *EFTS: Social and Technical Issues*, 7 COMPUTERS & SOC'Y, Fall 1976, at 3; Kling, *Value Conflicts and Social Choice in Electronic Funds Transfer System Developments*, 21 COM. ACM 642 (1978); D. PARKER, CRIME BY COMPUTER (1976); Parker, *Vulnerabilities of EFTs to Intentionally Caused Losses*, 22 COM. ACM 654 (1979); T. WHITESIDE, COMPUTER CAPERS: TALES OF ELECTRONIC THIEVERY, EMBEZZLEMENT AND FRAUD (1978). However, there is some good evidence that the "typical" reported computer crime entails losses of several thousands of dollars, rather than several hundreds of thousands of dollars. *See* Taber, *A Survey of Computer Crime Studies*, 2 COMPUTER/L.J. 275 (1980); C. Sartorius & S. Lam, Computer Crime and Abuse: Sources of Data and the Magnitude of Reported Events (Mar. 1980) (unpublished manuscript).

2. *See* L. KRAUSS & A. MACGAHAN, COMPUTER FRAUD AND COUNTERMEASURES (1979).

ers will be less easily able to double-check their bills.[3] Outside auditors may be unduly impressed by an organization which is extensively automated with particularly sophisticated, complex systems.[4]

Analysts of computer abuse are quick to point out that activities such as these fall under conventional criminal labels, *e.g.*, theft, fraud.[5] They also argue that employing a computer as a critical instrument alters the character of these crimes, since such abuses are particularly subtle and difficult to detect.[6] While most analysts of computer abuse devote some attention to the nature of computers that make these episodes special, little explicit attention is given to the conceptions of "abuse" and "crime," the manner in which these conceptions may vary across social contexts, and the social contexts in which they are most likely to occur.

Implicit images are, of course, employed in the selection and interpretation of illustrative cases—usually frauds and thefts such as embezzlement. Concepts of computer crime or abuse are normally elaborated through case examples, rather than conceptually. Partly

---

3. *See* Puzo, *The Pitfalls of Priceless Products, or How the Crackers Went Awry*, L.A. Times, Jan. 20, 1980, pt. V, at 3.

4. See the Equity Funding case reported in D. PARKER, CRIME BY COMPUTER, ch. 13 (1976) and T. WHITESIDE, *supra* note 1, ch. 2. *See also* Kling, *Automated Welfare Client-tracking and Service Integration: The Political Economy of Computing*, 21 COM. ACM 484 (1978).

5. *See* C. WAGNER, THE CPA AND COMPUTER FRAUD (1979). Wagner lists twenty-one synonyms for "computer abuse," "computer crime," and "computer fraud." *Id.* at 31-34.

6. Some analysts also argue that crimes associated with computer will shift from losses characterized by "high incidence, low loss per event" to "low incidence, high loss per event." *See, e.g.,* Parker, *Computer-Related White Collar Crime*, in WHITE COLLAR CRIME 199 (G. Geis & E. Stotland eds. 1980). This interpretation hinges both on a particular conception of "computer crime" and representative data on its incidence and the magnitude of associated losses. This article seeks to expand the prevailing conceptions of computer abuse and computer crime, and, as a byproduct, to change the character of incidents and losses associated with computer abuse.

Having a computer system "associated with" a loss may make no material difference in the nature of the event. If one party hits another with a desk-top computer, "computer battery" differs in no material way from simple battery with any other heavy object, *e.g.,* hammer, typewriter. A robbery conducted at a liquor store which uses an automated point-of-sale terminal is unlikely to differ from a robbery at a store with a manual cash register, except possibly for the amount of cash or negotiable paper on hand.

While these observations seem obvious, it would help to have a sharper conception of the particular role played by computers in "computer abuses" that merits distinction. Otherwise, "computer abuse" will become increasingly banalized as computer systems spread. Crimes and abusive practices will more frequently involve computer, not because some special feature of the computer is exploited (*e.g.*, remote access to financial records), but simply because computers are commonplace devices.

to persuade readers that computer abuses are significant, and partly to maintain interest, the cases selected for explication are mainly those where reported losses are in hundreds of thousands or millions of dollars, rather than in the hundreds of dollars. Often, examples are casually expanded. Stanley Mark Rifkin's famous $10.2 million theft from Security Pacific Bank in 1978 is usually treated as a computer crime and used to illustrate the magnitude of funds that can be stolen from electronic funds transfer systems, despite the fact that Rifkin's theft was accomplished through wire transfers and no computer system was directly employed.[7] Yet, such fine-grained concepts, such as the particular ways that computers are instrumental in "computer crimes," are important.

There is a growing body of literature about computer abuse and computer crime, which range from popular accounts, to handbooks for auditors[8] and criminal prosecutors,[9] computer specialists,[10] consumer advocates,[11] and federal policymakers.[12] Each audience has special needs and interests, but it is difficult to find accounts of computer abuse or computer crime which enumerate the important assumptions being made by the author or researcher. Much hinges on matters such as (1) whether one emphasizes "abuses," "crimes," or "frauds" that are married to computing; (2) the conceptions of "abuses," "crimes," or "frauds" that are adopted; and, (3) the particular role that computing plays in these events.

Despite the myriad choices about these matters which can be made in principle, there is substantial concensus over the social location of perpetrators and victims and the "conventional" nature of these events. First, most of the cases examined are those in which businesses are victims; the perpetrators are (ndividuals or small

---

7. Donn Parker, for example, identifies the case as a "computer abuse," not for the "transfer" act, but because Rifkin was not authorized access to the terminal area where he gained critical information about the transfer codes. Personal communications with Donn Parker (April 24, 1980). *See* the text accompanying notes 14-30 *infra* concerning the role that computer systems should play in an event for the term "computer abuse" or "computer crime" to be helpful. *See also* note 6 *supra*.

8. *See, e.g.*, L. KRAUSS & A. MACGAHAN, note 2 *supra*.

9. *See, e.g.*, SRI INT'L, COMPUTER CRIME: CRIMINAL JUSTICE RESOURCE MANUAL (1979) [hereinafter cited as RESOURCE MANUAL].

10. *See, e.g.*, Sterling, *Consumer Difficulties with Computerized Transactions: An Empirical Investigation*, 22 COM. ACM 283 (1979).

11. *See* Budnitz, *The Problems of Proof When There's a Computer Goof: Consumers Versus ATMs*, 2 COMPUTER/L.J. 49 (1980); Budnitz, *The Impact of EFT Upon Consumers: Practical Problems Faced by Consumers*, 13 U.S.F.L. REV. 361 (1979) [hereinafter Budnitz]; Broadman, *Electronic Fund Transfer Act: Is the Consumer Protected?, id.* at 245; Sterling, *Computer Ombudsman*, 17 SOC'Y, Jan.-Feb. 1980, at 31.

12. *See, e.g.*, Laudon, *Privacy and Federal Data Banks, id.* at 50.

groups acting in relative isolation and pursuing idiosyncratic criminal ventures. Cases in which computer systems are instruments of businesses acting against their clients, *e.g.*, consumer fraud, are largely ignored. Second, these events are typically removed from the social worlds in which they occur and simply labelled as "abuses" or "crimes," *e.g.*, invasions of privacy, fraud.

These two factors are not merely academic concerns, since "computer crime" is increasingly becoming subject to special legislation. Laws directed specifically at improper activities related to computers have been enacted in numerous states, and similar legislation is now pending in several states and in the United State Congress.[13]

Some of these practices are legally "crimes," since they violate existing statutes. However, the "criminal" label cannot be taken for granted when existing laws must be stretched for the acts in question to be defined as "crimes." For example, the use of "spare" computer time for private, recreational purposes by a computer programmer may be viewed as a theft of private property, or merely as a job perquisite akin to using a company telephone for limited personal calls. People differ over whether a particular act should be labelled as an "abuse," and furthermore, even if labelled an abuse, whether it should be prohibited by law.

If "unauthorized use of computer resources" is legislated as a criminal offense, an informal, but often accepted work practice would suddenly be rendered illegal. Similarly, there is considerable debate about which procedures for handling personally sensitive data should be considered fair business practices, and which are so unfair and intrusive that they abuse individual rights of privacy and should be made illegal.

The literature about computer abuse and computer crime is skewed by emphasizing white collar crimes in which businesses are the primary victims of thefts and abuses of trust, such as embezzlement, while neglecting business crimes and abuses, such as consumer fraud, invasions of personal privacy, and contractual violations in the computer industry. Moreover, the labels "abuse" and "crime" are usually taken for granted as objective properties of the acts in question, rather than as the signposts of conflict over rights and obligations.

A major goal of this article is to expand the prevailing conceptions of computer abuse to include this wider class of activities. This article will also examine the etiology of these events. Should they

13. There are currently eleven computer crime statutes. For the text of these statutes, see the Appendix in the next issue of the Journal.

be viewed as the idiosyncratic acts of individuals or as routinized occurrences in "criminogenic" environments? Finally, the article will examine the social contexts in which computer abuses are likely to occur, and will emphasize those computer abuses and computer crimes that may be viewed as organizational actions, insofar as the organizations which employ the perpetrators also gain from their actions.

I. Computer Abuse and Computer Crime

"Computer abuse" connotes a wide range of unsavory practices which can be married to computing, *e.g.*, fraud, theft, invasions of privacy. Selecting "computer abuse" as a sensitizing concept in contrast with "computer crime" or "computer fraud" offers two advantages. First, it allows a larger variety of problematic practices to be addressed, since the "criminal" status of many acts involving computers is unclear. Some of these activities, such as invasion of personal privacy, or swamping consumers with individually addressed junk mail, may not violate existing statutes. However, much is gained in the discussion by providing a covering term under which these acts may be examined.

Second, since the term "computer abuse" is more transparently a label whose appropriateness is not "given" but negotiated, it is easier to examine a wider array of actors who participate in and "define" computer abuses and computer crimes than just the perpetrator and the victim. These additional actors include "moral entrepreneurs," who define particular acts as abusive or criminal, such as security specialists, auditors and law enforcers.[14]

The larger social world in which computer abuse is defined is easily obscured by identifying "computer crime" with the transgression of existing statutes. This larger world is most apparent when definitions have not been agreed upon. Currently, "privacy practices" and the use of organizational computer resources for game playing and other minor personal perquisites by computer specialists are the subjects of serious controversy. A fortiori, the definition and legislation of computer crime bills is an important arena in which actors other than identified perpetrators and victims can identify themselves and articulate their interests.

For these reasons, the term "computer abuse" will be emphasized. Since some of the activities carried out with computer assistance violate existing legal statutes or are technically frauds, the narrow terms "computer crime" and "computer fraud" will still be

14. *See* H. Becker, Outsiders: Studies in the Sociology of Deviance (1963).

used where appropriate. Even when the activity is a "near crime," similar to statutory abuses but technically different in some minor respect, the appellation "computer crime" may still be used.

Most analysts rely upon implicit conceptions of computer crime or computer abuse. Donn Parker has been most explicit in this area by defining "computer abuse" as "any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator by intention made or could have made gain."[15] Unfortunately, this definition allows too broad a connection between computing and some abusive act, and emphasizes loss too strictly. It is important to amplify the meanings of the terms "associated with computers," "loss," and "intentional" if "computer abuse" is to be differentiated from other events.

A. Incidents Associated with Computer Technology

Computer systems must be a critical handmaiden to the loss or abuse. If computers are merely "used" incidentally, little is gained by drawing special attention to "computer" abuse. If an extortion attempt is made by long distance telephone, a computer is "associated with" the act, since direct, long-distance dialing is automated, but nothing is gained by treating long-distance extortion aided by the telephone as a "computer crime."

If an embezzler falsifies paper records, which are then fed into a properly operating, computerized information system, the special features of computing come into play less than when the software is altered or the complexity of computer-related procedures materially mask the deception.

The extent to which computer-based technologies are in some way essential to carrying out abuses in which they are employed as instruments must be resolved on a case-by-case basis, rather than by some sweeping and astute definition. For the purposes of this article, computer technologies are "associated" with abuses or crimes by being instrumental and essential in fostering the loss, or by being the object of the loss.

A second kind of "association" between computer technology and an abuse can occur when computerized products or services are deceptively represented or contracted for. Because of the complexity of computer-based products (*e.g.*, mainframes, system software), data analyses (*e.g.*, simulation models), and services (*e.g.*, payment systems), a loss may occur simply by misrepresentation of a product to a "reasonable" but inexperienced agent, such as a customer

15. D. PARKER, *supra* note 4, at 12.

or auditor.[16]

B. *Intentionally Caused Losses*

Not all "intentionally caused losses" can be viewed as abuses. For example, if two parties set up a cash competition in which they use a computer system. such as a programming contest or a game played by two computerized chess programs which they wrote, each may intent the other to lose, but neither party will feel abused. It is not sufficient that a party suffer a loss, but that the party suffering the loss actually feel unfairly treated or the object of illegitimate actions—genuinely a victim.[17]

"Computer abuse" is a sensitizing concept which is difficult to define sharply. It helps to focus attention on the ways in which computerized technologies may cause problems for computer-using organizations or the public. If, for example, one wonders whether electronic funds transfer systems will be more subject to theft, large or small, than their manual precursors, computer abuse may be a useful point of departure.

II. The Construction of "Computer Abuses"

Analysts of computer abuse often illustrate important principles through exemplary cases. For example, to steal from a computerized record system, one might only need to manipulate normal transaction cards, and need not understand the software; a computer theft may be accomplished by employing a data entry clerk as an accomplice; computer frauds can survive standard audits and are often found only through accidental occurrences.[18]

Knowledge of patterns like these is important to those seeking to diminish the volume and frequency of loss by designing different

16. Because of their complexity, computer-based products are often not well understood in detail by their developers, vendors, users or other participants. Consequently, descriptions of computing products or computer-based services may include unintentional misrepresentations. Such misrepresentations should, on the average, serve no particular interest, since errors may equally serve the vendor or the vendee. In this acticle, negligent or intentional misrepresentations are emphasized.

17. The conception of "victims" as used in this article is entirely subjective. Nonetheless, difficulties remain, since not every party who suffers a clear loss in the eyes of others will feel victimized. Some battered wives feel that they "deserve" their ill treatment; some patients who have been crippled by the malpractice of doctors feel gratitude rather than anger, since they believe that their lives were saved, even if they were needlessly paralyzed in the opinion of other physicians.

18. The more serious compendia each include over a dozen cases. *See* Allen, note 1 *supra*; D. Parker, note 4 *supra*; T. Whiteside, note 1 *supra*; L. Krauss & A. MacGahan, note 2 *supra*.

computer systems, altering organizational procedures, or enacting and enforcing laws. The literature on computer abuse has been largely developed to draw attention to the peculiar properties of computer systems that make them more complex. Many analysts of computer crime view themselves as demythologizing or debunking "conventional" images, which attribute extensive security to automated systems, or which treat crimes with computers as no different in kind, strategy, or consequence from crimes without a computer.

Theoretically, the illustrative, reported cases would span the range of actual and potential abuses. In actuality, they form a peculiarly biased collection.[19] The lion's share of the attention is turned to episodes of theft or fraud where the victim is a computer-using organization and the identified perpetrator is an individual or small group engaged in clearly illegal acts.[20] These cases (or "capers"[21]) are briefly presented in most reports, and are similar to formula detective stories sans the detective.[22] Much of the attention focuses on the scheme used by the perpetrators, and possibly on the organizational practices which allowed them to continue undetected. Typically, these incidents are large frauds or embezzlements in which the loss to the victimized business is in the hundreds of thousands or millions of dollars. The sheer scale of these frauds and/or thefts helps the analyst dramatize their importance.

---

19. There is no way to obtain an "unbiased" sample, and the critical questions of "bias" revolve around the particular biases in any sample. All samples are marred by underreporting and the happenstance manner in which investigators learns about cases through professional contacts and friends. In addition, case collections like Parker's, which depend upon newspaper articles as a critical resource, are also subject to the biases of the news reporting, which emphasizes sensational events and world views consistent with the preferences of elite institutions. Newspaper stories serve as a rich and efficient resource for obtaining leads for some kinds of cases, but they must be supplemented by other sources. For an accounting of the structural biases in newsmaking, *see* G. TUCHMAN, MAKING NEWS: A STUDY IN THE CONSTRUCTION OF REALITY (1978).

20. *See* note 2 *supra*. The primary exception is in D. PARKER, *supra* note 4, ch. 4.

21. *See* T. WHITESIDE, note 1 *supra*.

22. One might suspect that computer abuses would conform more aptly to the formulas of crime novels than detective stories, since attention is directed at the deceptions of the perpetrator and the logical sequence of events, rather than the forensic powers of the investigators. In fact, since many computer aubses are discoverd by accident or when a perpetrator confesses on his own initiative, the absence of "detection" is even more characteristic of computer abuse. Symon contrasts "crime novels" with "detective novels" and argnes that detective novels emphasize a plot based upon deception, while crime novels depict relatively straightforward crimes and focus on the circumstances and interactions of the characters. J. SYMON, MORTAL CONSEQUENCES: A HISTORY FROM THE DETECTIVE STORY TO THE CRIME NOVEL (1972). *See also* J. CAWELTI, ADVENTURE, MYSTERY AND ROMANCE: FORMULA STORIES AS ART AND POPULAR CULTURE (1976).

In order to understand the social and technical conditions under which different acts are likely to be defined as computer abuses and are likely to occur, it is useful to have a set of categories to situate the major actors and their relationship to one another. In the special case of while collar crime, Edelhertz suggests a useful classification for situating "perpetrators" and "victims":

> 1. Crimes by persons operating on an individual, *ad hoc* basis, for personal gain in a nonbusiness context (hereinafter referred to as "personal crimes");
> 2. Crimes in the course of their occupation by those operating inside businesses, Government, or other establishments, or in a professional capacity, in violation of their duty of loyalty and fidelity to employer or client (hereinafter referred to as "abuses of trust");
> 3. Crimes incidental to and in furtherance of business operations, but not the central purpose of such business operations (hereinafter referred to as "business crimes");
> 4. White collar crimes as a business, or as the central activity of the business (hereinafter referred to as "con games").[23]

While organizations may be victims of white collar crimes in any of these categories, individual clients are most likely to be victimized by business crimes and con games.[24] While technically, all of these crimes are perpetrated by "individuals," as one moves from personal crimes to con games, the social scale of the collusion helpful for success increases. In Edelhertz's terms, most of the cases of computer crime which appear in the literature illustrate personal

---

23. H. EDELHERTZ, THE NATURE, IMPACT AND PROSECUTION OF WHITE-COLLAR CRIME (1970), *quoted in* S. REID, CRIME AND CRIMINOLOGY 223 (1976).

24. Individuals can be victimized by abuses of trust and businesses can be victimized by others engaged in business crimes, such as consumer fraud. These are relatively gross generalizations. Books written for auditors either assume that the computer-using organization is acting ethically or argue that it should be. *See* L. KRAUSS & A. MACGAHAN, *supra* note 2, at ch. 3; C. WAGNER, note 5 *supra*. Parker devotes an entire chapter to consumer fraud (D. PARKER, *supra* note 4, ch. 22, but neglects consumer fraud as a possibility in his analysis of consumer losses from electronic funds transfer systems. Parker, *Vulnerabilities of EFTs to Intentionally Causes Losses*, 22 COM. ACM 654 (1979). Oddly, he also neglects Sterling's study of consumer difficulties with computerized billing systems, which was reported in a prior issue of the same journal. Sterling, note 10 *supra*. Parker also analyses "business crimes" in that same article, but these are clearly personal crimes and abuses of trust. Business crimes, in the sense that that term is used in this article, are ignored. Moreover, Parker's analysis of "computer abuse perpetrators" only treats people who have engaged in personal crimes or abuses of trust, not in business crimes or con games.

August Bequai devotes a chapter to "consumer-related frauds" and a chapter to "crime by computer" in A. BEQUAI, WHITE COLLAR CRIME: A 20TH-CENTURY CRISIS, chs. 7, 12 (1978). However, the analysis of consumer fraud does not mention computer use, and the chapter on computer crime examines only personal crimes and abuses of trust.

crimes and abuses of trust; "business crimes" are typically excluded from attention, though that is perhaps the most important category for a variety of consumer frauds.[25] One con game, the Equity Funding case, is often cited in the accounts of computer crime.[26]

Much of this article is directed to business crimes. The concept of "business crime" has been best defined by Shover, who employed the label "organizational crime" to denote:

> criminal acts committed by individuals or groups of individuals, thus including conspiracies, during the normal course of their work as employees of organizations, which they intend to contribute to the achievement of goals or other objectives thought to be important for the organization as a whole, some subunit within the organization, or their own particular job duties.[27]

When criminal activities are common to an occupation, and not just to an organization, *e.g.*, kickbacks from laboratories to doctors, the term "occupations crime" is a useful designation.[28] Business crimes (or organizational crimes) include price-fixing, false advertising, and consumer fraud. When restricted to the cases where computing technology is instrumental, "business computer crimes" are most likely to be consumer fraud and contractual fraud. When these conceptions are extended to include "computer abuse" as previously defined,[29] "business computer abuses" would include invasions of privacy, misleading sales practices in the computer industry, and deceptive presentations of computerized data analyses. Both individuals and organizations may be the "victims" of these practices.[30]

III. Individuals as Victims of Business Computer Abuse

As computerized information systems spread throughout the economy, and are used as a medium to record transactions between organizations and their individual clients, the opportunities for com-

---

25. In this respect, the literature of computer crime parallels much of the crime literature, which neglects organizational and occupational crimes. *See, e.g.*, CRIME AT THE TOP: DEVIANCE IN BUSINESS AND THE PROFESSIONS (J. Johnson & J. Douglas eds. 1978).

26. *See* note 4 *supra.*

27. *See* Sover, *Defining Organizational Crime*, in CORPORATE AND GOVERNMENTAL DEVIANCE: PROBLEMS OF ORGANIZATIONAL BEHAVIOR IN CONTEMPORARY SOCIETY 37 (M. Ermann & R. Lundman eds. 1978).

28. *See* Quinney, *The Study of White Collar Crime: Toward a Reorientation in Theory and Practice*, in WHITE COLLAR CRIME: OFFENSES IN BUSINESS, POLITICS, AND THE PROFESSIONS 283 (G. Geis & R. Meier eds. rev. 1977).

29. *See* text accompanying note 14 *supra.*

30. This is not to minimize the importance of personal crimes or abuses of trust. Simple abuses of trust, like embezzlement, receive the lion's share of attention.

puter-related abuses and crimes are likely to increase. These acts may occur in any of several ways. Customers of organizations using electronic billing, funds transfer, or calculating aids (*e.g.*, supermarket scanners) may simply be defrauded. As the data collected in these systems increases in richness, it is likely to be used for other purposes, such as identifying "good customers" or locating debtors, which intrude on the privacy of the individual customer.

If individuals who elect to use computerized financial services are mislead as to the attendant risks and liabilities by service providers, they will suffer unexpected and unfair losses. These losses include a broad range of activities—consumer fraud, invasion of personal privacy, and false advertising—and range from practices that some parties feel are abusive, but are well within the bound of legal business practices, to those that clearly violate current laws.

Civil libertarians argue that routine organizational practices unduly invade personal privacy. For example, computer-using organizations have begun using their data files for new purposes, such as market surveys, matching payroll records against welfare files to identify "cheaters," and using business records for the Parent Locator Service.[31] Supporters of these practices emphasize their efficiency in helping an organization conduct its business or a public agency carry out its legislated obligations. Civil libertarians advocate maximum individual liberty as a competing value, which should not be easily compromised.[32] Jeremiah Guttman, for example, asserts:

> As valuable to the business and scientific communities as such research might prove, the use of data acquired and maintained by an electronic funds transfer system for any purpose other than transfer of money would be *to misuse the system, to abuse it, to betray a reasonable anticipation of privacy to which the consumer is entitled.*[33]

---

31. *See* PRIVACY PROTECTION STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977).

32. *See* Kling, *Value Conflicts and Social Choice in Electronic Funds Transfer System Developments*, 21 COM. ACM 642 (1978).

33. J. Gutman, Observations of a Civil Libertarian on Electronic Funds Transfer 2 (May 1979) (unpublished manuscript); emphasis added. Some uses of financial record systems for other purposes, such as the Parent Locator System, are mandated by law. Personal communications with Robert P. Bigelow, May 19, 1980. To civil libertarians, the abusiveness of a practice and its legality are independent. One may hope that laws will not permit or even mandate "abusive" practices, but legality is no insurance that a practice is not harmful. First, there must be a language of discourse about the character and consequences of proposed statutes in which attributes such as the "interests they serve," their constitutionality, their efficacy, their enforceability, and their abusiveness can be analyzed and discussed. Second, laws are often the product of legislative compromises between conflicting interests which may even

An analyst of computer abuse with civil libertarian sympathies would concentrate on a different set of episodes than one who accepts prevailing "legitimate," organizational record-handling practices as unabusive by definition.

Advertising and complex contracts that mislead or confuse consumers about the nature of computerized financial services is a second example of business computer abuse. Evidence about these practices is scant and usually anecdotal. For example, Mark Budnitz carefully examined the case of one pay-by-phone service, whose advertising misled customers about its convenience and liabilities.[34] Usually, legal remedies are employed to ameliorate problems like these. While laws such as the federal EFT Act[35] and the New York consumer contract law [36] require that contracts "be written in a clear and coherent manner using words with common and everyday meanings,"[37] business practices may not comply. There is little evidence about the extent to which actual contracts for EFT services meet these criteria. One recent survey of EFT contracts and advertising by fifteen New York state-chartered banks suggests that there are serious discrepancies between the intent of these laws and routine practices.[38]

> Some banks took greater care to insure that their contracts were able to be easily read and understood . . . . However, even when customer contracts of the more conscientious banks are compared to promotional contracts used by all the banks to entice new EFT customers, the shortcomings of the contracts are clear and the potential for readable contracts becomes obvious. The banks artfully designed the promotional materials . . . . When compared with the contracts, the promotional materials were printed in more simplified language and with more effective use of large and bold print . . . . Furthermore, none of the promotional materials we reviewed described all the terms and conditions written into the customer contracts. The most important omission from the promotional materials was the provision on the customer's liability for unauthorized use of his debit card.[39]

These practices certainly leave substantial room for abuse.

---

hold conflicting values. In the case of data collected for one purpose being made available for other purposes, one must weigh the value of personal privacy against the values of efficient state investigations and the profitability of private enterprise. *See* Kling, note 1 *supra*; PRIVACY PROTECTION STUDY COMM'N, note 40 *supra.*

34. *See* Budnitz, note 11 *supra.*

35. 15 U.S.C. §§ 1692 *et seq.* (1978).

36. *See* Abrahamson & Martin, *The Impact of the Federal EFT Act on Consumer Contracts in New York State*, 13 U.S.F.L. REV. 467 (1979).

37. *Id.* at 469. *See* N.Y. GEN. OBLIG. LAW § 5-702 (McKinney Supp. 1978).

38. *See* Abrahamson & Martin, note 36 *supra.*

39. *Id.* at 469-71.

Stronger regulations for fair and complete advertising as well as simple contracts may ease these difficulties. As Budnitz notes:

> [i]t is unrealistic to expect financial institutions voluntarily to describe what may go wrong if they use EFT, or to provide more complete disclosure than the law requires. However, it is equally unrealistic to pretend that consumers who lack this information truly understand the consequences of agreeing to use EFT.[40]

Unfortunately, the ease of disclosure is made difficult by complex or ambiguous laws sich as the EFT Act, where the very conditions of liability are incomplete. For example, Broadman observes that the EFT Act may be read as limiting a consumer's liability to $0, $50 or $500, when he informs a bank of a lost debit card within two days, depending on how one reads the text.[41]

The third class of abusive activities, computer-related consumer frauds, are also poorly treated in the literature on computer crime.[42] Reports of "consumer difficulties" with computerized billing and payment systems are easy to find, though episodic. While the transitions from "consumer difficulties" to "consumer abuse" to "consumer fraud" are neither direct nor simple, evidence of systematic consumer difficulties is the most likely indicator of fraud. Many people have had difficulties with errors in computerized systems and in correcting errors once they are found. There is no reason to suspect that such errors are necessarily intentional, rather than accidental.

Even the better automated record systems are not entirely free of data and software errors. Since imperfection is the rule, the practical questions hinge on the quality of the data and software, and the extent to which an organizaton is attentive to correcting data and software errors. While the boundaries between "accident," "negligence," and "criminal negligence" may be clear in principle, they are difficult to specify in practice in automated data systems.

All computer systems of any scale are likely to suffer from system design flaws and data entry errors. The presence of errors detected, in say, disputed billings, only suggests the possibility of abuse or crime rather than "commonly accepted" and "acceptable" difficulties. Much depends upon the rate of errors found in specific systems, the extent to which design flaws are corrected over time, and the ease that consumers have in bringing errors to the attention of organizational staff and having them resolved. Despite the widespread and increasing use of computerized systems in business

40. Budnitz, *supra* note 11, at 369.

41. *See* Broadman, *supra* note 11, at 256.

42. For example, they are ignored in the recent prosecution manual. RESOURCE MANUAL, note 9 *supra.*

transactions, little systematic data is publicly available on these matters.

There are indications, however, that consumers have had difficulties in correcting computerized errors. Consumer-oriented centers set up to investigate consumer complaints attributable to computer errors shed some light on the presence of consumer difficulties. Theodor Sterling has reported on a variety of cases of computer "billing errors" that were referred to a "Computer Ombudsman Office" administered by a society of computer specialists.[43] One trade newspaper, Computerworld, routinely reports computer errors which are brought to the attention of a special contributor, Alan Taylor, by individual complainants. While only a few episodes are published each year, these are relatively "hard cases," since they are brought by complainants who typically have persisted in seeking to correct an error without success.[44]

Victimization surveys could shed light on the occurrence of untoward errors and abuses, if not consumer crimes, which are associated with computer systems. Sterling recently conducted a mail survey of five hundred households in British Columbia about their experiences errors in such systems.[45] Approximately forty percent of those sampled reported at least one error in the preceding year, and about fifteen percent reported two or more errors. One hundred and five households reported specific problems and errors with computerized transactions.

Each of these reports was followed up with an extensive telephone interview. Of those people with errors, seventy-four percent were able to resolve them, though satisfactorily solution required several contacts with the computer-using organization. Some respondents found error-correcting to be a time-consuming activity.[46] Moreover, some respondents suffered additional costs, since they were unable to have the interest charges on disputed amounts re-

---

43. The office was sponsored by the Vancouver Chapter of the Canadian Information Processing Society. *See* Sterling, *The Computer Ombudsman: Rational for Setting Up a Permanent Service*, CAN. DATASYS., Aug., 1976, at 62; Sterling, *supra* note 11, at 31; Sterling & Laudon, *Humanizing Information Systems*, 22 DATAMATION, Dec. 1976, at 53.

44. *See, e.g.*, Taylor, *New Approach Combats Deceptive Trade Practices*, Computerworld, Aug. 6, 1979, at 21, col. 1; Taylor, *Two Problems Crop Up in Bankcard Procedures*, Computerworld, Aug. 20, 1979, at 15, col. 1. The second article illustrates a particular consumer complaint investigated by Alan Taylor. Taylor is known among computer specialists for these investigations, and receives complaints that would not be the basis of news stories in the daily, less specialized, press.

45. *See* Sterling, note 10 *supra*.

46. Twenty percent of those interviewed spent more than twenty hours attempting to resolve a single error.

moved, even when they were reimbursed or credited for the disputed amounts.[47] Seven percent of the respondents gave up trying to resolve their difficulties. Of the remaining households, eight percent never tried to resolve the computer errors and eleven percent were engaged in an ongoing, but uncompleted, effort to resolve their problems at the time of the interview.

Sterling's study indicates that correcting computerized errors is much more troublesome than conventional accounts of computer use suggest. Furthermore, it was quite clear to many of the respondents that their identification of errors and attempt to correct them were not appreciated by the staff with which they dealt. "In 16 percent of cases respondents reported that they were coerced in some way to pay a disputed amount, and in approximately 9 percent of the cases they were specifically urged to pay a disputed amount in order to protect their 'good credit rating.' "[48] Sterling's study underlines the way in which computerized transaction systems can intersect the contractual side of transactions between the public and computer-using organizations.

Sterling's study, and "The Taylor Report" can only be suggestive of the extent of the problems facing consumers. Alan Taylor selects cases from an unspecified universe of consumer complaints. Sterling's study is but one investigation, based on a special sample, and does not track the complaints back to the computer-using organizations to examine their organizational etiology. Certainly the frequency of events reported by Sterling are likely to vary from sample to sample, place to place, and time to time. But the critical questions are whether this data is credible and whether it indicates likely consumer abuses where the clients of organizations are victimized.[49]

While consumer studies of this nature do not directly address the question of whether individuals are being subjected to intentional, abusive billing practices using computerized systems, they do indicate, at the very least, that many people are experiencing errors

47. Thirty-six percent of the households with errors had interest charged on the disputed amount. In nineteen percent of the cases, the interest was removed at the time the error in the charges was corrected. Another eleven percent required yet additional action to have the interest on the disputed amount removed. Six percent of the households paid interest in the disputed amount.

48. Sterling, *supra* note 10, at 286-87.

49. One of Sterling's rates, that of billing error, is similar to that reported by Ronald Anderson in a study of public perceptions of computing. Anderson, *Sociological Analysis of Public Attitudes Toward Computers and Information Files,* in PROC. AFIPS SECOND JOINT COMPUTER CONF. 649 (1972). In a random sample of Minnesotans surveyed in 1971, thirty-five percent reported having problems with a computerized bill in the preceding year.

with such systems, and that some of these errors prove so difficult to correct that people pay the amount rather than continuing to fight their cases. In none of the cases published in "The Taylor Report" or reported by Sterling could criminal intent be proved. It was simply not investigated, since the goal of the complaint bureaus is to investigate, negotiate and rectify individual complaints. In these negotiations, the ombusdman adopts a strategy which allows the organization's staff the greatest opportunity to correct the error without losing face. Consequently, the ombudsman is more likley to avoid blaming errors on intentional acts, or trying to pin down blame and motive, as would an investigator seeking evidence of criminal activity. Nor could a telephone survey of consumers provide data about the intent of the organization. One possible exception is the extent to which consumers were coerced into paying disputed bills.

Moreover, since the sample in a citizen survey is selected to represent a geographically defined population, rather than the clientele of a particular firm, it is impossible to draw conclusions about the consumer practices of any given firm. Suppose that consumers in a probability sample drawn from a large metropolitan area complained of problems with Bigmart five times as often as with Fastmart in a study of consumer difficulties with computerized information systems. Bigmart's billing and error correction procedures could be seen as poorly developed, abusive, and possibly even fraudulent. However, if one knew that Bigmart has twenty times the number of customers as Fastmart, one should conclude that its procedures are actually "cleaner." Nonetheless, it is hard to review Sterling's report and the occasional cases published in Computerworld and escape the suspicion that some businesses are systematically abusing their customers with automated transaction systems and their procedures for identifying and correcting errors.[50]

As consumer-oriented computer systems, such as electronic funds transfer systems and supermarket scanners, become more commonplace, it is likely that the incidence of losses related to computer errors will rise. Whether these losses are accidental, the result of negligence, or intentional, can only be determined empirically. But special attention needs to be given to consumer

50. There is some evidence that consumer abuses are infrequently reported to consumer protection agencies. While other forms of consumer abuse, such as home repair swindles and "bait-and-switch" sales practices may form the majority of larger consumer abuses, there is a paucity of evidence from which to draw strong conclusions about the incidence and importance of consumer-related abuses. *See* McGuire & Edelhertz, *Consumer Abuse of Older Americans: Victimization and Remedial Action in Two Metropolitan Areas*, in G. Geis & E. Stotland, *supra* note 6, at 266.

difficulties if they are investigated at all, since they are unlikely to be reported in the press or brought to the attention of lawyers or prosecutors without special support. Individual losses are likely to be small, even if they are large when aggregated over thousands of customers and transactions. It is most likely that individuals will simply seek to recover their own losses, and it is difficult to prove "intent" in most cases.

The three different kinds of computer-related activities discussed in this section (1) turning financial record-keeping systems into instruments of surveillance or research, (2) completeness and clarity of advertising and contracts of computerized services, (3) and procedures for correcting errors in computerized billing systems, illustrate the ways in which "computer abuse" is a socially-defined label, since the legitimacy of each of these activities is subject to debate. There is little evidence about the incidence or seriousness of each of these kinds of activities, but they usually are ignored by analysts of "computer abuse," even though they may constitute a large fraction of abuses.

IV. Organizations as Victims of Business Computer Abuse

Increasingly, computerized systems appear as instruments in the transactions between organizations: sales and payments are recorded, computer equipment and software is bought and sold, and organizational participants display their work to clients and auditors in other organizations using computer-based data analysis for insight and persuasion. Certainly, organizations can be the victims of con games that employ computerized systems as instruments. For example, if a firm is sending bogus bills to randomly selected businesses for services that were never rendered, the businesses may pay the bills as if they were routine expenses properly incurred. If the bogus bills are produced by a computer system—to increase their legitimacy and permit operations on a larger scale—this would be a computer fraud. Similarly, businesses are the identified victims in a variety of other computer crimes, such as fraud[51] and embezzlement.

Of interest in this section, however, are "routine" business practices which may be examples of computer abuse or computer crime, but which are ignored in the literature. There are three commonplace occupational activities involving computer technology, which can range from those that are clearly legitimate, to some that are

51. *See, e.g.*, Vaughan, *Crime Between Organizations: Implications for Victimology*, *id.* at 77.

questionable, to still others that are deemed abusive, unethical, and possibly criminal. These activities involve:

1. Selling computing equipment and services;
2. "Delivering" software which meets contractual specifications;
3. Employing complex or sophisticated computer technologies to persuade a client that a given course of conduct is appropriate.

All of these activities include legitimate practices. Salesmen are expected to place their wares in the best possible light. Software developers will produce products that resemble the contract specifications. Analysts, such as engineers, actuaries, and urban planners, are expected to utilize sophisticated means, including computer-based systems, to provide better insight or "analytic penetration" into complex problems.

However, the staff acting for the computer-using or computer-selling organization can also rely on strategems to advance the interests of their own organization, subunit or job, which "cause losses" to the client organization. Sales staff will certainly inform prospective buyers of software developed for their machine which meets the client's needs. Sometimes, however, the promised software is very remote from what the client actually requires.[52] Early delivery deadlines may be set to "beat the competition," even though they are unrealistic and turn out later to be unattainable. Similarly, vendors sometimes sell undersized equipment, since the lower price may better the competition; once the equipment is acquired, the customer is locked into upgrading from the same vendor.[53] Some misrepresentations are unintentional, but others which clearly serve the vendor's interest are likely to be negligent or intentional. Sales staff vary in the integrity with which they make promises, and in their sophistication in accurately assessing their own product lines and likely delivery schedule. Consequently, it is

52. *See* Crabtree & Kling, *DP Sales Ploys and Counterploys,* 24 DATAMATION, May 1978, at 194.

53. Undersizing computer systems may also serve the interest of the user. For example, there is one large, multi-division organization which has a policy about the level of scrutiny given to computer system acquisitions of different sizes. That organization has annual operating revenues of approximately one billion dollars and several thousand employees spread over several geographically dispersed divisions. Systems or components which cost less than $100,000 may be authorized by division directors without any evaluation of integrating the acquisition into the organization-wide computing plan. The staff of an operating department in one division wished to acquire a computer system which cost almost $175,000. With the support of the division director, they proposed a $95,000 system, which was too small for the intended task. The system, however, could then be approved at the division level, and expanded to its proper size in the following fiscal year.

difficult to clearly demonstrate that unreliable sales promises were intentionally misleading, except in the most blatant cases.

Some sales practices are related to discrepancies between the usually vague contractual specifications for software, and the relatively concrete package that is actually provided to the customer. "Missing features" are common in contractually developed software. Estimating the costs of complex software is more art than science, and a poorly developed art for many. Since there are not particularly strong professional standards by which to compare software costing or scheduling strategies.[54] Consequently, it may be difficult to distinguish a good professional judgment which results in a poor outcome, from a poor professional judgment, and further, to distinguish either of these from rank deception, except in the most brazen cases.

One illustrative example concerns the case of a software firm, Softmix,[55] which developed a special system for a public agency, Govworks, on a fixed fee contract. The package did not meet all of the contractual specifications, but the computing specialists were encouraged to develop a "minimal" running system that could be turned over to Govworks at the earliest possible date. After Govworks' contracting officer accepted the minimal system, Softmix could be awarded a new "maintenance" contract, which would bring in the additional revenue needed to pay for the remaining development.

Even sharply defined contracts, however, may not be sufficient. One example concerns a major computer manufacturer, Byterite, that provides a FORTRAN language on its SUMMA machine series, which is suppose to meet ANSI[56] FORTRAN standards. A programmer was assigned to maintain Byterite's SUMMA FORTRAN by implementing enhancements, repairing errors, and issuing memos about new developments. Some of the error reports that she received from installations using SUMMA FORTRAN indicated subtle but important discrepancies between SUMMA FORTRAN and ANSI FORTRAN. FORTRAN programmers who believed that SUMMA

54. *See* Wolverton & Boehm, *Software Cost Modelling: Some Lessons Learned*, in PROC. OF SECOND SOFTWARE LIFECYCLE MANAGEMENT WORKSHOP 129 (IEEE Computer Soc'y 1978).

55. "Softmix" is a pseudonym for a particular software firm. The following discussion will identify other organizations by similar pseudonyms, *e.g.*, Govworks, Byterite.

56. The American National Standards Institute (ANSI) develops standards for various programming languages. These are voluntary standards in principle, but often compulsory in practice, since federal agencies usually specify that software must meet ANSI standards.

FORTRAN was compatible with the ANSI standard wrote programs which did not run "properly." SUMMA's programmer prepared a variance report which she planned to send to all sites using SUMMA FORTRAN. Her supervisor objected, arguing that Byterite could not acknowledge any discrepancy between the two versions of FORTRAN since it was contractually obligated to provide an ANSI-compatible language. She persisted, since she knew of the difficulties that the unexpected discrepancy was causing in the field. In face of threatened termination, she relented and did not publish the report.[57] The programmer was demoralized and later left her job. Data about matters such as this is, of course, scant and anecdotal. It appears that programmers resolve difficulties such as there privately—by compliance or departure. Those who complain loudly, or "blow the whistle," are likely to be penalized in their "efficiency reviews" or fired.

The use of computers to favorably impress clients or auditors is commonplace. One of the most frequently cited computer crimes, the case of Equity Funding,[58] illustrates a case of deception on a grand scale. Remarkably, the literature of computer crime and computer abuse chronicle few other cases where computerized information systems were used as instruments of impression management. Such cases, however, are reported by social analysts who examine computer use in organizations. Rob Kling reports the case of a welfare agency which used an automated client tracking system to favorably impress federal auditors,[59] and the case of an engineering firm which turned to complex data analyses to "snow" auditors hired by its client to review a slow moving project.[60]

The success of the Polaris missle project was often attributed to the use of PERT scheduling, which was specifically developed for it. However, Harvey Sapolsky persuasively argues that PERT was not used to manage Polaris schedule and costs.[61] The admiral in charge of Polaris development was not concerned how PERT was used, only that its presence be visible. PERT served to sufficiently enhance the image of the Navy teams managing Polaris development

57. *See, e.g.,* the case of Virginia Edgerton, as reported in 22 TECH. & SOC'Y (IEEE Soc'y Comm. on the Social Implications of Tech. [no date]). For a case of engineering design with similar dynamics, *see* Vandivier, *Why Should My Conscience Bother Me?*, in LIFE IN ORGANIZATIONS: WORKPLACES AS PEOPLE EXPERIENCE THEM (R. Kanter & B. Stein eds. 1979).

58. See the Equity Funding case, reported in D. PARKER, *supra* note 4, ch. 13; T. WHITESIDE, *supra* note 1, ch. 2.

59. *See* Kling, note 4 *supra.*

60. *See* Kling, *Social Analyses of Computing: Theoretical Perspectives in Recent Empirical Research*, 12 COMPUTING SURVEYS 67 (Mar. 1980).

61. *See* H. SAPOLSKY, THE POLARIS SYSTEM DEVELOPMENT (1972).

that they were relatively unburdened by the scrutiny and intrusive demands of external review boards. On other projects, PERT might well serve as an instrument of managerial control. But in its first, and most publicized use, it served primarily as an instrument of deceit.

These three kinds of activities—selling computerized equipment, delivering software to contractual specifications, and using computerized systems for impression management—can each entail abusive practices in the course of routine work for participants in organizations.

V. The Etiology of Computer Abuse

When analysts of computer abuse or computer crime consider the "causes" of these activities, they emphasize individual proclivities. Parker, for example, has identified profiles of "computer abuse perpetrators" based on interviews with people who engaged in personal crimes or abuses of trust. Mowshowitz criticizes this approach for neglecting the ethos of the organization which employs the "computer abuse perpetrator."[62] He believes that Parker's data supports the hypothesis that "computer abuse perpetrators" are acting in accord with the ethos of their employer, but have turned their behavior against the employer rather than performing on his behalf. Thus, a workplace principle that "customers can be deceived if they won't bear visible losses" can be modified to legitimatize embezzling sums that are not "visible" to the organization.[63] Mowshowitz's analysis shifts attention from characteristics of the individual—his background, motives, financial needs and opportunities—to the social context in which computer abuses take place.[64]

In the business computer abuses examined in this article, abusive sales practices, contractual frauds, or deceptive impression management techniques constitute the corrupt ethos which Mowshowitz employs as an explanation.[65] In the case of many business computer abuses or computer crimes, practices which entail com-

62. *See* Mowshowitz, *Computers and Ethical Judgment in Organizations*, in Proc. 1978 Nat'l ACM Conf. 675 (1978).

63. A Security Pacific Bank official reported that Rifkin's theft of $10.2 million was sufficiently small, given the bank's volume of transactions, that the sum was unlikely to have been missed or felt as a profound loss. While Rifkin was not an employee, and the theft was technically wire fraud, rather than computer theft, it is sufficiently close to illustrate the principle.

64. *See* Altheide, Adler, Adler & Altheide, *The Social Meaning of Employee Theft*, in J. Johnson & J. Douglas, *supra* note 25, at 90.

65. While these localized ethical orientations might be further explained by reference to the broader "ethos of capitalism," such explanations are ad-hoc.

puting may be similar to other work practices which are less related to computing. Of these activities, impression management strategies common in entrepreneurial and bureaucratic organizations may be widespread, with or without computing.[66]

However, different abusive practices may be the by-product of different social processes. One promising line of inquiry examines the social arrangements under which systematic abuses are most likely. Recent analyses of industries in which illegal practices are common have led sociologists to develop the conception of "criminogenic markets" and "conditioned" or "coerced" crime. Leonard and Weber, for example, have examined abusive and illegal practices adopted by automobile dealers, including "forcing accessories," "service gouging," "high finance [charges]," "parts pushing," and the "warranty sham."[67] While these activities are carried out by the sales and service personnel of new car dealerships, Leonard and Weber argue that they are "conditioned by" policies of the major automakers. The "criminogenic" policies which regulate the relations between the automakers and their dealers reward them for new car sales and implicitly penalize good service. They also provide dealers with meager markups for selling "stripped down" versions of new cars.

Farberman explicitly defines a "criminogenic market" as "the deliberate and lawful enactment of policies by those who manage economically concentrated and vertically integrated corporations and/or industries which coerce lower level (dependent) participants into unlawful acts."[68] He also notes that "[t]hose who set the conditions which cause others to commit unlawful acts remain non-culpable."[69]

If the sales staff of a contract software firm sets contract dates without consulting with the technical staff, or "lowball" the estimates to "beat the competition," the technical staff are unlikely to be able to deliver on the contract.[70] These arrangements would be criminogenic, and the technical staff is placed in the position of cov-

66. *See* R. GABRIEL & P. SAVAGE, CRISIS IN COMMAND: MISMANAGEMENT IN THE ARMY (1978); P. BLAU, THE DYNAMICS OF BUREAUCRACY (1955).

67. *See* Leonard & Weber, *Automakers and Dealers: A Study in Criminogenic Market Forces*, in G. Geis & R. Meier, *supra* note 28, at 133.

68. *See* Farberman, *A Criminogenic Market Structure: The Automobile Industry*, 16 SOC. QTRLY 438, 438 (1975), *reprinted in* SOCIAL INTERACTION 146, 160 (H. Robbey, S. Greenblatt & C. Clark eds. 1979).

69. *Id.*

70. Sometimes, the technical staff and marketing staff anticipate each other's actions. The technical staff will increase its deadlines or budgets by, say one hundred percent, and the marketing staff will, in turn, reduce their estimates by one-half.

ering up the areas where the product fails to meet specifications. Unfortunately, there is little systematic data about arrangements such as these, even though they are known to participants in the software industry and a source of dissatisfaction among software specialists.

It is difficult to understand the etiology of business crimes and abuses by reference to a profile of "abuse perpetrators," since business abuses are often "normal" occupational activities. To the extent that this is the case, perpetrators will be identical to other participants in the same organization or occupation. An alternative perspective shifts attention from the proclivities of individuals to the structuring of organizational worlds which make abusive or untoward activities more likely. Contractual frauds in the delivery of computer software may be a by-product of "criminogenic" organizational arrangements. This is a tentative explanation, and does not necessarily fit all forms of business computer abuse. It does, however, provide a promising starting point for serious investigation.[71]

VI. Conclusion

Computer uses are increasing in variety, and a larger fraction of socially and economically sensitive data are maintained on automated data systems. Questions concerning the vulnerability of these systems to abuse or their use as abusive instruments are becoming increasingly important. The audiences for investigations include computer specialists, technology assessors, auditors, law enforcement agents, prosecutors, lawyers, legislators and consumer advocates. These groups, however, have somewhat different orientations and interests in different forms of computer abuse or computer crime.

Much of the literature on computer abuse and crime is sensitizing, and is written to attract attention to the peculiar problems of computerization. Unfortunately, it also sensationalizes computer crimes and abuses to help attract attention. The labels "computer crime" and "computer abuse" have been overgeneralized. In this article, a broad range of activities which can be identified as computer abuses or computer crimes have been examined. But, in practice, these terms have denoted personal crimes and abuses of trust.

Spectacular wire frauds and embezzlements make interesting reading and capture popular imagination, but probably illustrate only a small class of important computer abuses and computer crimes. Occupational crimes are usually ignored, except insofar as

71. For one investigation, which uses the characteristics of organizational victims and interorganizational relations as a point of departure, *see* Vaughan, note 51 *supra*.

they are abuses of trust. As a consequence, the computer crime and abuse literature emphasizes the protection of computer-using organizations, rather than the public.

Fortunately, there are relatively few instances of verified computer abuses or crimes. Thus, most analyses draw strong conclusions from small collections of cases. These studies include claims about the nature and etiology of computer abuses, the nature of perpetrators and victims, the conditions under which these acts occur, and their social significance. That is to be expected at this time. But it is important to expand the common conceptions of computer abuse and crimes to include business and occupational activities.

It may not be prudent for all forms of abuse to be prohibited or remedied by legal actions. If, however, one is interested in reducing the frequency of "computer abuses," a serious approach cannot merely emphasize the "deviant acts" of ne'er-do-wells who engage in personal crimes or abuses of trust. To the extent that computer-related abuses and crimes are business or occupational activities, strategies for abatement will have to be altered. That means that programs to minimize computer abuse would emphasize matters other than the detection and prosecution of clever computer manipulators. They would attempt to inhibit contractual abuses of computer systems by providing some protection for "whistle blowers." Such programs aimed at minimizing computer-related consumer abuse would include a variety of measures, from laws such as the EFT Act to provide consumers with minimal protections in case of errors, through the establishment of consumer action agencies.

Lawyers and lawmakers are particularly concerned about activities such as "computer abuse" or "computer crime" insofar as they alter the lawful relationships between parties or merit changes of law. However, clear conceptions of the kinds of abuses or crime in which computerized technologies may be significant are useful for other purposes as well. In particular, they help policymakers, managers, consumers, legislators in their role as reviewers of administrative activity, and computer specialists to understand the opportunities and difficulties of different modes of computer development and use and the appropriateness of different strategies for resolving difficulties.

This article has sought to expand the prevailing conceptions of the nature of computer abuse and the conditions under which abuses are likely. It identifies the kinds of abusive activities in which organizations may be "perpetrators," as well as "victims." It also suggests some ways in which abusive practices in the development sale and provision of computer-based systems and services should not be viewed simply as "regrettable" events which are the

acts of a few misguided individuals. Rather, they should be viewed as routine organizational practices which are likely to occur under specifiable conditions. The vast majority of activities practiced in the development, sale or use of computing are neither abusive not criminal. However, the prevailing conceptions of computer abuse are simply too narrow and self-assured. Taken together, these points indicate that the current spate of computer crime bills are based on these narrow conceptions of computer abuse and computer crime, and fail to come to terms with the conditions under which computing may be most abusive for organizations or the general public.