UIC John Marshall Journal of Information Technology & Privacy Law

Volume 4
Issue 2 *Computer/Law Journal - Fall 1983*

Article 5

Fall 1983

Misappropriation of Computer Services: The Need to Enforce Civil Liability, 4 Computer L.J. 401 (1983)

Robbin Lynn Itkin

MISAPPROPRIATION OF COMPUTER SERVICES: THE NEED TO ENFORCE CIVIL LIABILITY

I. INTRODUCTION

Computers are becoming pervasive in modern society. Not surprisingly, the increased use of computers has been accompanied by an increase in the incidence of computer related crimes.[1] A great deal of scholarly writing has focused upon the problem of such crimes. Unfortunately, the vast majority of this literature fails to deal with the most ubiquitous computer related abuse—that of unauthorized, though legal, use of computer services.

Of the few states that have enacted "computer crime" statutes,[2] most have either failed to proscribe the type of computer abuse that is the subject of this Note, or have provided too severe a penalty for this type of misappropriation. In the latter case, the harsh penalties may account for the few instances of computer crime that are actually reported by the owners or lessees of computers that are used without authorization.[3]

This Note will survey the present law dealing with computer abuse, first, by discussing the appropriate applications of computer crime statutes, and second, by discussing, at length, the ineffectiveness of those statutes in treating the problem of unauthorized use of computer services. The Note then concludes with the proposition that a more appropriate and effective means of treating misappropriation of computer services is achieved through the increased imposition of civil liability. Remedial civil liability is more appropriate than criminal sanctions because it will require the abuser to com-

1. In 1978, 350,000 small businesses installed computer systems. Tunick, *Computer Law: An Overview*, 13 LOY. L.A.L. REV. 315, 316 (1980); McCartney, *Small Business Systems: They're Everywhere*, 24 DATAMATION Oct. 1978, at 91. For a discussion regarding the future increase in computer crime, see Dietz, *Computer Security; Not Just For Mainframes*, MINI-MICRO SYS. June 1982, at 251-55.

2. Only 12 states have enacted computer crime statutes: Arizona, California, Colorado, Georgia, Montana, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island and Utah. Howe, *Coping With Computer Criminals*, 28 DATAMATION, June 1982, at 118, 126.

3. *See generally* Dietz, *supra* note 1, at 251; A. BEQUAI, COMPUTER CRIME xiii (1978).

pensate the true victim of the misappropriation. Thus, compensation serves to make the injured party whole while simultaneously deterring the abuser from committing the wrongful behavior again.

II. SURVEY OF THE EXISTING LAW DEALING WITH COMPUTER RELATED ABUSE

One must be aware of the present treatment of computer abuse by state and federal statutes in order to truly comprehend the nature and severity of the existing problem. Further, this awareness will aid in understanding why the type of misappropriation referred to in this Note should be treated as a tort rather than as a crime.

Computer related crimes are actually a subpart of the larger, all encompassing activity known as "white-collar crime."[4] White-collar crime is defined as follows: "[A]n illegal act or series of illegal acts committed by non-physical means and by concealment or guile, to obtain money or property, or to obtain business or personal advantage."[5]

Numerous definitions exist as to what constitutes a "computer crime." The most simplistic definition currently in use is, "any incident associated with computer technology in which a victim suffered or would have suffered a loss, and a perpetrator by intention could have made a gain."[6] As of 1978, the annual cost of computer crime was estimated to be in excess of 40 billion dollars.[7]

Computer abuse is codified as a crime in the twelve states that currently have computer related statutes.[8] Misappropriation of computer services is presently included as one of the five distinct types of computer related crimes. It is commonly referred to as "theft of services."[9] A person is guilty of theft of services if "he obtains services which he knows are available only for compensation by *deception* or *threat* or by *false token* or other means to avoid payment for the service."[10]

There is a distinction between theft of services as defined above,

---

4. A. BEQUAI, *supra* note 3, at 1.

5. *Id.* at 6; 42 U.S.C. § 3791(a)(18) (Supp. V 1981).

6. *Computer Crime*, 18 AM. CRIM. L. REV. 370, 372 (1980).

7. A. BEQUAI, *supra* note 3, at 1.

8. *See supra* note 2.

9. The five areas of computer crime are classified as follows: financial, property, informational, theft of services, and vandalism. Tunick, *supra* note 1, at 326.

10. MODEL PENAL CODE § 223.7 (Proposed Official Draft 1962) (emphasis added). The Code defines "services" as "labor, professional service, telephone or other public service, accommodation in hotels, restaurants or elsewhere . . . ." For a further discussion of theft of services, see D. PARKER, S. NYCUM & S. OURA, COMPUTER ABUSE 57 (1973).

which is criminally sanctioned, and misappropriation of computer services as discussed herein to which civil sanctions most appropriately apply. Criminal sanctions are proper where the misappropriater of computer services harbors a criminal intent. Criminal intent has been defined as "a guilty or evil intent in performing an act prohibited by law and penalized as a crime."[11] For example, embezzlement, which has much in common with theft,[12] is a purely statutory offense defined as a "criminal breach of trust."[13] This offense generally entails a fraudulent or felonious conversion of property that has rightfully come into the possession of the converter.[14]

Where criminal intent is the basis for the misappropriation of computer services, criminal sanctions are necessary. Section 502 of the California Penal Code requires access to the computer systems with a devise or scheme to "defraud or extort" or to obtain services with "false or fraudulent intent" in order for the act to constitute a computer crime.[15] Severe sanctions may be imposed for violation of the California statute; violation constitutes a felony and is punishable by a maximum fine of $5000, imprisonment, or both.[16]

A few well known cases exemplify the type of computer abuse that constitutes computer crime as defined by statute and that necessitates criminal sanctions. In 1979, Stan Rifkin was a computer security consultant for Security Pacific Bank in Los Angeles.[17] Rifkin was found to have gained access to the wire transfer room of the bank, and, after memorizing the secret access code, he programmed the bank's computer to send $10.2 million to an account at the Irving Trust Co. in New York. He then purchased $8.1 million worth of diamonds with the stolen money. Rifkin was charged with stealing the $10.2 million.

Another incident of computer crime involved a graduate student at the University of California.[18] The student was arrested for stealing $1 million in supplies from the Pacific Telephone and Telegraph Co. He had used a telephone and the company's secret access code to instruct the computer to deliver the supplies to a remote ware-

11. BALLENTINE'S LAW DICTIONARY 291 (3d ed. 1969).

12. *See* 26 AM. JUR. 2D *Embezzlement* §§ 2, 4 (1966).

13. *Id.* § 1.

14. *Id.* Fraudulent intent is the requisite element for embezzlement, although states do use varied language to define the crime. *See, e.g.*, CAL. PENAL CODE § 503 (Deering 1983), which defines embezzlement as the "fraudulent appropriation of property by a person to whom it has been entrusted."

15. CAL. PENAL CODE § 502(b) (Deering 1983).

16. *See id.* at § 502(b)-(e) regarding specific sanctions imposed.

17. *Computer Crime*, *supra* note 6, at 370, 371.

18. *Id.* at 370, 372.

house. After the crime was discovered by an associate, the student was arrested and spent forty days in a minimum security facility for grand theft.

Both of the above cases involve criminal intent accompanied by the anti-social conduct that our justice system proscribes. Such criminal action is deemed harmful to the entire society,[19] and is considered conduct against the state rather than against any individual owner of the property.[20] Note that because of the severe sanctions that can be imposed for criminal conduct, the prosecution in a criminal case must prove the defendant's guilt "beyond a reasonable doubt."[21]

Where criminal intent is not harbored by a person who misappropriates computer services, that person can neither be justly charged for committing a crime nor punished with criminal sanctions. Where a person misappropriates computer services for legal, but personal benefits, a crime is not committed. A more appropriate classification for the conduct would be a tortious conversion, which entails the use of property in a "[m]anner exceeding the authorization."[22] When a person authorized to use a computer for specified work-related purposes uses the computer to trace the geneology of his horses, no *felonious intent* exists.[23] The action is purely one against the lessee of the equipment, for it is he who would be charged for the services wrongfully used. Thus, an appropriate sanction would be to require the abuser to compensate the lessee for the unauthorized services used. Due to the lessened severity of civil sanctions as compared to criminal sanctions, the plaintiff has a lower standard of proof by which to find the defendant guilty, that of a "preponderance of the evidence."[24] Because of the lower standard of proof, more abusers could be found guilty and more deterrence would therefore be achieved. Further, civil liability involves actions between individual citizens and civil remedies require that the victim be made whole, i.e., compensated for the computer services wrongfully used by the abuser.

The failure of states to codify computer crime or, if they do, the failure of their statutes to distinguish between criminal and civil liability, creates inequities in our justice system. An example of an unsuccessful prosecution against a computer misappropriater is the

19. A. BEQUAI, *supra* note 3, at 5.

20. 26 AM. JUR. 2D *Embezzlement* § 8 (1966).

21. *Id.* § 48.

22. *See* RESTATEMENT (SECOND) OF TORTS § 228 (1965). *See also id.* § 222A.

23. New York v. Weg, 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (N.Y. Crim. Ct. 1982) (a school employee used the school computer to trace the geneology of his horses).

24. 18 AM. JUR. 2D *Conversion* § 160 (1965).

case of *Lund v. Commonwealth*.[25] In *Lund*, the defendant, a graduate student, was accused of stealing school keys, computer cards and computer printouts, and using the school computer without authorization. The defendant had failed to seek proper authority for access to the computer on which he was conducting research for his dissertation. He obtained access by using keys from friends in other departments and those departments were billed for the defendant's access time. Faculty members testified that if the defendant would have properly requested access to the computer for his research, he would have received authorization.[26] Nevertheless, the defendant did not make a proper request. The trial court found the defendant guilty of grand larceny. The appellate court reversed the lower court's decision on the grounds that unauthorized use of computers is not the subject of larceny; nowhere in Virginia's criminal code does the word "use" appear as a form of larceny. The court found that the printouts had no more value than that of scrap paper. Furthermore, Virginia had not enacted a computer crime statute that made it a crime to obtain labor or services by means of false pretense. In conclusion, the court found that the evidence was insufficient to convict the defendant of grand larceny.[27]

Lund is a significant case because it demonstrates that the misappropriation of computer services can cause serious financial loss. The Director of the Computer Center testified that the cost of the defendant's unauthorized use of the computer was estimated to be $26,384.16. The defendant in *Lund* received no punishment or penalty because no computer abuse statute existed in Virginia, and the alleged wrongful conduct was not included in any criminally proscribed statute. In effect, there was no deterrent to committing such abusive acts, and the university was forced to absorb the $26,384.16 loss. This demonstrates the fact that institutions are likely to be very adversely affected by the lack of civil remedies for computer abuses.

The *Lund* case is interesting to analyze with regard to the intent of the defendant. The facts of the case appear to evidence that the defendant did not have a criminal intent at the time of accessing the computer. The faculty members testified that if Lund had appropriately requested the access time, it would have been granted to him.[28] It is questionable, however, whether or not the actual services used by Lund exceeded the amount he would have been au-

25. 217 Va. 688, 232 S.E.2d 745 (1977).
26. *Id.* at 690, 232 S.E.2d at 747.
27. *Id.* at 692-93, 232 S.E.2d at 748.
28. *Id.* at 690, 232 S.E.2d at 747.

thorized to use if he had made a proper request. Since the facts state that the school departments leased the computer services,[29] it is doubtful that all dissertation students are entitled to use $26,000 worth of computer time. If the unauthorized access time exceeded the amount of time that Lund would have been allowed to use the computer had he received proper authorization, a civil, rather than criminal, action should have been brought by the school for the cost of the computer services excessively used.

There is an alternative theory of liability in *Lund*. If Lund knew he was not authorized to use the computer services to the extent that he did, and, in an effort to conceal his wrongful use of the services, he input the identification of departments other than those that should have been properly billed, he committed fraud.[30] Another example of the type of situation that constitutes fraud is where a law clerk attempts to conceal his personal use of Lexis or Westlaw by plugging in the name of a client who is then billed for services that appear to have been rendered for its benefit. These actions are perpetrated by false pretenses. A false pretense involves the "deprivation of another of a right, money, or property by artful and deceptive words and acts which, when the facts are known, were more or less obviously said or done with the intent to defraud."[31] The fraudulent intent categorizes the computer misappropriator as a criminal, and he should be sanctioned as such. As discussed, it is this sort of criminal intent that distinguishes acts giving rise to criminal liability from acts giving rise to civil liability (e.g., where a person misappropriates computer services for legal, but unauthorized purposes).

Another case exemplifies the inequities that may result from the broad interpretations often given to criminal statutes by prosecutors in order to sanction as criminal conduct that which is purely a civil wrong. In *New York v. Weg*,[32] a computer programmer employed by the Board of Education of the City of New York was charged with misdemeanor theft of services for allegedly using his employer's computer, without permission, for the purpose of tracing the geneology of his horses. The prosecution rested its case on section 165.15 of the Penal Law, which prescribes that one is guilty of "theft of services" where:

> obtaining or having control over labor in the employ of another person, or of business, commercial or industrial equipment or facilities of another person, knowing that he is not entitled to the use

29. *Id.* at 689, 232 S.E.2d at 746.

30. *See* Nycum, *The Criminal Law Aspects of Computer Abuse*, 5 RUT. J. COMPUTERS & LAW 271, 276, & 286 n.112 (1976).

31. 37 AM. JUR. 2D *Fraud and Deceit* § 26 (1968).

32. 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (N.Y. Crim. Ct. 1982).

> thereof, and with intent to derive a commercial or other substantial benefit for himself or a third peson, he uses or diverts to the use of himself or a third person such labor, equipment, or facilities.[33]

The judge stated that the central issue in the case was whether or not the computer was "business, industrial or commercial" equipment as stated in the statute.[34] The judge held that the available evidence, including statutory language and legislative history, was proof that the statute was to:

> apply only to unauthorized use of equipment that is offered for use as a service in a commercial setting, such as for lease or hire, *and was not designed to make it a crime for a public or private employee to use his employer's internal office equipment without permission*.[35]

Judge Juviler made an interesting comment in his opinion when he spoke about the varied existing interpretations of the words "business" and "facilities" as quoted in the statute, and stated that if these words were given the broad meaning asserted by plaintiff, then the Penal Code would make criminals out of "[t]he thousands of employees in government and the private sector who make unauthorized use of their employers' computers, word processors, calculators, copying machines, telephones, typewriters, and other equipment or facilities for personal benefit."[36] Most significantly he added, "[t]he Legislature could not have intended such a dramatic change in the criminal law of this state, transforming 'basically civil' wrongs to misdemeanors punishable by a year in jail, without giving clearer indication of its novel purpose."[37]

It is worthy of note that Judge Juviler expressed his recognition of the problem inherent in trying to classify as criminal that which under traditional principles of liability is a tort. The judge alluded that criminal statutes fail to set forth specific elements by which one may be accused of misappropriating computer services. Computer crime statutes are so broadly written that a wide area of discretion is given to the prosecution in which to classify the abuser's conduct as criminal. Thus, there is a need for criminal statutes that specify the distinction between the behavior that comprises criminal and civil computer abuse. Criminal statutes must be precisely written so that they are capable of narrow interpretation. They must also

---

33. *Id.* at 1018, 450 N.Y.S.2d at 958.

34. *Id.* at 1019, 450 N.Y.S.2d at 959.

35. *Id.* at 1019-20, 450 N.Y.S.2d at 960 (emphasis added); Judge Juviler granted the defendant's motion to dismiss on two grounds: failure to state a crime, and failure to allege facts in support of each element of the alleged crime.

36. *Id.* at 1023, 450 N.Y.S.2d at 963.

37. *Id.*

provide the constitutionally required notice of exactly what conduct constitutes criminal behavior.[38]

Federal attempts to codify computer related crimes have so far been just as unsuccessful as state attempts.[39] Model Penal Code section 223.7,[40] which deals with theft of services, provides that "anything that can be classified as a service that the actor knows is available only for compensation" falls within the purview of that section. The code prescribes that punishment for the theft of services offenses will be graded according to the amount of damages involved, which is the way that the code generally treats theft offenses. The minimum penalty under this section relating to the *smallest sum* involved invokes a maximum term of imprisonment for thirty days. Thirty days imprisonment may be too harsh a penalty for a person who, on one occasion, uses his employer's computer without authorization to balance his checkbook. Furthermore, the Code does not provide for reimbursement to the person responsible for paying for the computer time abused. Thus, by providing neither a penalty commensurate with the damage caused, nor a means by which the victim of the damage is to be made whole, the Model Penal Code fails to effectively deal with misappropriation of computer services.

Perhaps the harshest penalty yet provided for misappropriation of services, which ironically does take into account misappropriation for personal benefit, is set forth in the proposed Senate bill 240.[41] In 1979, Senator Ribicoff introduced S. 240, entitled the "Federal Computer Systems Protection Act of 1979."[42] The bill, which was overbroad and imposed unusually harsh penalties,[43] was never adopted. The problems of S. 240 were common problems of computer crime statutes. The act would have made it a crime to use, for fraudulent or other illegal purposes, any computer that was either owned or operated by: (a) the United States, (b) certain financial institutions, or (c) other entities that affect interstate commerce. The bill contained the following two-pronged test; if a person's conduct satisfied the elements of either prong, then that conduct would constitute fraud

38. "Fundamental fairness requires that no person be held criminally responsible for conduct which he could not reasonably understand to be proscribed." 21 AM. JUR. 2D *Criminal Law* § 16 (1981).

39. *See* Note, *Addressing Computer Crime Legislation: Progress and Regress*, 4 COMPUTER/L.J. 195 (1983).

40. For further discussion of the Code, see *supra* note 14.

41. S. 240, 96th Cong., 1st Sess. § 1028 (1979).

42. *Id.* at 1.

43. Note, *supra* note 39, at 203. For a more detailed discussion of S. 240, see Comment, *Computer Crime—Senate Bill S. 240*, 10 MEM. ST. U.L. REV. 660 (1979-80).

and abuse as defined in the bill:[44]

> (a) Whoever knowingly and willfully, directly or indirectly accesses, causes to be accessed or attempts to access any computer, . . . for the purpose of:
>
> (1) devising or executing any scheme or artifice to defraud, or
>
> (2) obtaining money, property, or services, for themselves or another, by means of false or fraudulent pretenses, representations or promises, *shall be fined a sum not more than two and one-half times the amount of the fraud or theft or imprisoned not more than fifteen years or both.*
>
> (b) Whoever intentionally and without authorization, directly or indirectly accesses, alters, damages, . . . any computer system, . . . *shall be fined not more than $50,000 or imprisoned not more than fifteen years, or both . . . .*[45]

The type of misappropriation of computer services dealt with in this article may logically be seen as constituting computer fraud and abuse under either of the two tests set forth in S. 240. For example, if an employee represents to his employer that he is in the office on a Saturday for the purpose of completing a research project assigned by his employer, but in reality he is using the employer's computer for personal economic purposes, then he may be held to have made false representations for the purpose of obtaining computer services. In that case, the first part of the test has been met. Likewise, the same employee may be held to meet the second prong of the test if he accesses the computer for an unspecified purpose without authorization. In either case, the penalties provided for by the bill are extreme in relation to the relatively harmless, although inappropriate, use of the employer's computer service.[46]

III. CIVIL CAUSES OF ACTION ARE NECESSARY TO EFFECTUATE THE REDUCTION OF MISAPPROPRIATION OF COMPUTER SERVICES

Before discussing the available civil remedies for misappropriation of computer services, it is important to note the following. There are numerous actions that constitute misappropriation of services for personal benefit where even civil remedies may be too

---

44. S. 240, *supra* note 41, § 1028 at 3.

45. For the complete tests, see S. 240, *supra* note 41, § 1028 (emphasis added). For further criticisms of these tests, see Comment, *supra* note 43, at 660, 665.

46. Comment, *supra* note 43, at 666. For a further discussion of the severity of such penalties and a proposal for penalties more commensurate with the true damages, see Letter from Harlan I. Ettinger, Staff Liaison for ABA, Section of Criminal Justice, To Members, Economic Offenses and Complex Litigation Problems Committee (Apr. 11, 1979).

harsh. This conduct consists of actions that have been knowingly going on for years, with nothing ever being done about them. For example, employees use their employer's xerox machine, make personal phone calls on the company phone, or use the company stationery for personal correspondence.[47]

In the cases mentioned above, the costs involved in bringing charges against an individual abuser would most likely outweigh the costs of the misappropriation of services that took place. For instance, when an employer owns a xerox machine, the only cost to the employer for an employee's personal use of the machine, unless the use was outrageously excessive, would be the minimal paper cost. When an employer fails to explicitly set forth the rules regarding an employee's use of the xerox machine, company phones, etc., the employer may be thought of as impliedly consenting to this minimal personal use of services. Similarly, in the situation where an employee improperly uses his employer's computer services on one occasion for a very short period of time, the cost of bringing an action against that employee for the misappropriated computer time would far exceed the cost of the misappropriation. This is especially true, as mentioned, where the employer owns the computer equipment rather than leasing it. When an employer does own the equipment, there also may be an implied consent by the employer that employees may use the equipment for their personal use during nonproductive working hours, such as during lunch.

It is not the above sort of computer use for personal benefit that requires civil sanctions. Civil remedies are appropriate when more than minimal abuse takes place and where it is clear that, due to the extreme costs involved, someone misappropriated the computer services without implied consent. In such situations it is economically feasible for an employer to pursue a civil action rather than merely firing the employee. When an employer or private party leases computer equipment and thus is responsible for paying for each minute that the equipment is used, a scheme of civil remedies will resolve the problem of misappropriation of computer services in a fair and equitable manner.

In order for a scheme of civil remedies to be effective, the scheme must require that restitution be made to successful plaintiffs.[48] Victims of abused computer services would, therefore, be encouraged to initiate action; unlike the victims in a successful

47. For a discussion of those actions that are carried out "by thousands of employees", see New York v. Weg, 113 Misc. 2d 1017, 450 N.Y.S.2d 957 (N.Y. Crim. Ct. 1982).

48. 1 AM. JUR. 2D *Actions* § 43 (1962).

criminal action, they would be compensated for the losses incurred. Also, civil actions generally receive less publicity and take less time than criminal actions. Thus a victim who is concerned about economy of time and publicity will be more likely to commence a civil—as opposed to criminal—suit against an abuser.[49] In effect, increased civil remedies will deter wrongdoers from carrying on abusive behavior while more fully compensating the victims of the abuse. A discussion of the proposed civil remedies that will most effectively treat the misappropriation of computer services problem follows.

A. Tort Liability

1. Conversion

Conversion is defined as "an intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."[50] "One who is authorized to make a particular use of a chattel, and uses it in a manner exceeding the authorization, *is subject to liability for conversion to another* whose right to control the use of the chattel is thereby seriously violated."[51] This definition of conversion illustrates the primary method by which one misappropriating computer services commits the tort.[52]

Computer services are intangible property.[53] In order to know if computer services may be the subject of a tortious conversion, it is necessary to determine if intangible property constitutes personal property.[54] A controversy has long existed over whether or not intangible property may constitute personal property. This controversy continues to be active in the area of trade secrets.[55] Whether or not trade secrets constitute personal property has not been ultimately decided. When the issue arises, however, the authority most

49. Victims who actually report computer crimes are "only at the tip of the iceberg." Dietz, *supra* note 1, at 251. Victims of computer abuse are reluctant to admit losses publicly or to "introduce such cases into the public domain at court." Howe, *supra* note 2, at 118, 124.

50. Restatement (Second) of Torts § 222A (1965).

51. *Id.* § 228 (emphasis added). *See* 18 Am. Jur. 2d *Conversion* § 48 (Supp. 1983).

52. Restatement (Second) of Torts § 222A (1965), defines conversion as "[a]n intentional exercise of dominion or control over a chattel which so seriously interferes with the right of another to control it that the actor may justly be required to pay the other the full value of the chattel."

53. Intangible property is defined as "[p]roperty that is a 'right' rather than a physical object." Black's Law Dictionary 726 (5th ed. 1979).

54. *See* Note, *supra* note 39, at 198.

55. *See* A. Seidel & R. Panitch, What The General Practitioner Should Know About Trade Secrets and Employment Agreements 11-12 (1973).

often cited in support of protecting trade secrets as personal property is the following dictum written by Justice Holmes in *E.I. Du-Pont de Nemours Powder Co. v. Masland*:

> Whether the plaintiffs have any valuable secret or not the defendant knows the facts, whatever they are, through a special confidence that he accepted. The property may be denied, but the confidence cannot be. Therefore the starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs, or one of them.[56]

In applying this dictum, most courts tend to avoid the issue of property altogether and instead concentrate on public policy regarding fair dealing in business relationships.[57]

Public policy concerning fair dealing and justice should also prevail where a misappropriation of computer services occurs. As the doctrine of unjust enrichment prescribes, equity requires a person who converts property by using it without authorization to fully compensate the person at whose expense the use was performed.[58] Notwithstanding the importance of public policy as stated by Justice Holmes in *Masland*, case law and other authority do allow the classification of intangibles as personal property. In addition, personal property has been defined broadly to mean "the right or interest which a person has in things personal."[59] Thus, computer services are a proper subject for the tort of conversion,[60] and employers or private parties who have legal title to computer equipment have a protected interest in such property that is deemed to be personal to them.[61]

Recent state supreme and appellate court decisions provide further support for treating misappropriation of computer services as a tort of conversion rather than as a crime of theft. The Alabama Supreme Court held that a computer program can be the subject of conversion. In *National Surety Corp. v. Applied Systems*,[62] the court stated that even though the defendant, an employee of the plaintiff, developed the subject computer program for the plaintiff employer, he did not have any property rights or interests in the program. The court found that his job was to develop the program

56. E.I. Du Pont de Nemours Powder Co. v. Masland, 244 U.S. 100, 102 (1917); A. SEIDEL & R. PANITCH, *supra* note 55, at 11.

57. A. SEIDEL & R. PANITCH, *supra* note 55, at 11-12.

58. *See* RESTATEMENT OF RESTITUTION § 1 comment a (1936).

59. Reese v. Qualtrough, 48 Utah 23, 30, 156 P. 955, 958 (1916).

60. 18 AM. JUR. 2D *Conversion* § 9 (1964).

61. Title is evidence of one's ownership and is the "[m]eans whereby the owner is enabled to maintain or assert his possession and enjoyment." 63 AM. JUR. 2D *Property* § 31 (1972).

62. 418 So. 2d 847, 849-50 (Ala. 1982).

for his employer, who had a definite and protected property interest in the program.[63] In addressing the issue of whether intangibles can be the subject of conversion, the court stated, "[i]t would be inconsistent to say that intangible personal property can be subject to theft and yet not be subject to conversion."[64]

The California Court of Appeals stated in *Miller v. Rau* that there does not need to be a "manual taking of . . . property [to have a conversion], since any wrongful assumption of authority over chattels, inconsistent with another's right of possession, or subversive of his vested interest therein amounts to conversion."[65] Thus, if a person misappropriates computer services for personal, unauthorized purposes, he has wrongfully assumed authority over the intangible personal property of the person whose property such services comprise; a conversion has been committed and the perpetrator should be prosecuted for committing a tortious act.[66] Depending on the extent of the services converted and the willfulness of the defendant in carrying out the wrongful act, punitive damages may appropriately be considered and awarded.[67]

2. *Breach of Confidence*

The attention of courts and legal scholars has recently focused upon the tort of breach of confidence. A law review note entitled *Breach of Confidence: An Emerging Tort*,[68] advocates that a tort has been committed where there is "disclosure of information revealed in the course of a nonpersonal relationship of a sort *customarily understood* to carry an obligation of confidentiality."[69]

The cases dealing with breach of confidence all involve disclosure to a third party of information understood to be confidential between two parties. *Peterson v. Idaho First Natl. Bank*[70] involved a breach of confidence by a bank to its depositors and customers. *Doe v. Roe*[71] dealt with a psychiatrist's publication of a former patient's

63. *Id.* at 849.

64. Intangible personal property is subject to theft in Alabama. *Id.* at 850.

65. 216 Cal. App. 2d 68, 75, 30 Cal. Rptr. 612, 616 (1963) (quoting Pilch v. Miliken, 200 Cal. App. 2d 212, 224, 19 Cal. Rptr. 334, 341 (1962)).

66. For a further discussion regarding intangible property being the subject of conversion, see A & M Records, Inc. v. Heilman, 75 Cal. App. 3d 554, 142 Cal. Rptr. 390 (1971); Belford Trucking Co. v. Zaga, 243 So. 2d 646 (Fla. Dist. Ct. App. 1971); Miracle Boot v. Plastray, 84 Mich. App. 118, 269 N.W.2d 496 (1978).

67. 22 AM. JUR. 2D *Damages* §§ 80, 236 (1965).

68. Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426-68 (1982).

69. *Id.* at 1426, 1462-68 (emphasis added).

70. 83 Idaho 578, 367 P.2d 284 (1961).

71. 93 Misc. 2d 201, 400 N.Y.S.2d 668 (Sup. Ct. 1977).

intimate fantasies. These cases demonstrate that although the relationships of the parties may be quite varied,[72] each relationship "carries an implied assurance of confidentiality that the defendant held out and then violated."[73]

This implied assurance of confidentiality customarily exists between a person authorized to use computer services, such as an employee, and the person who authorizes that use, such as an employer. When an employee accesses computer services, acquires information about his employer or client, and then discloses that information to a third party, there has been a clear case of breach of confidence. Here the employee has obtained a personal benefit by accessing the computer to retrieve valuable information he then related to others. As stated by Justice Holmes in *Du Pont Powder Co. v. Masland*,[74] "[t]he starting point for the present matter is not property or due process of law, but that the defendant stood in confidential relations with the plaintiffs or one of them."[75] Where damages may be difficult to measure due to the inability of the employer to prove with certainty the amount of time that the employee improperly accessed the computer, a breach of confidence tort would be most successful in compensating the victim for the harm caused to him as a result of the breach.

B. Contracts Liability

Civil liability for breach of contract may be the simplest action to bring against a misappropriater of computer services. Where a contract specifies what sort of computer access is and is not allowed, any violation of the contractual terms may give rise to a cause of action for breach of contract. The breach requires that the non-defaulting party's restitutional interest be protected.[76]

A special type of contract may be required between a party authorized to use computer services and the party from whom such authorization must be obtained. Since a major problem in pursuing a cause of action in the area of misappropriation of computer services is the difficulty in proving with certainty the extent of services wrongfully used, a contract for agreed remedies or liquidated damages would assure that the sum stipulated in the contract be paid to the employer upon breach by the employee.[77] In order for a liqui-

72. *See* Note, *supra* note 68, at 1426-32.
73. *Id.* at 1434.
74. 244 U.S. 100 (1917).
75. *Id.* at 102.
76. 22 Am. Jur. 2d *Damages* § 46 (1965).
77. *Id.* at § 218.

dated damages clause to be enforceable, damages caused by breach of contract must be uncertain and difficult to ascertain or prove.[78] A liquidated damages claim will serve as a safeguard to the employer who fears the possibility of computer misuse and his inability to prove its occurrence with certainty.

An agreed remedy stipulation between an employer and an employee may at first appear to concede to the idea that an employee will necessarily breach the contract and misappropriate computer services for personal benefit. Viewed in this manner, the contract could be interpreted as encouraging misbehavior. At second glance, however, when the liquidated damages are greater than the actual cost of the accessed computer services, the stipulation actually serves as a deterrent to wrongful behavior. The liquidated damages agreement, with its specifications regarding conduct that will constitute a breach of its terms, enables the employer and the employee to know what to expect of each other. This may enhance communication and increase the amount of trust and confidence between the parties, and thus decrease the likelihood of an abuse of services.

C. Restitution: Recovery for Tort and Contract Actions; Alternative Basis for Liability

A judgment for damages in a tortious conversion case is measured by the full value of the converted property.[79] Hence, where services are misappropriated or converted, the fair measure of damages would be the full value of the services wrongfully used. Such recovery parallels recovery based on the doctrine of restitution (i.e., the fair value of the benefit received). The remedial scheme of restitutional recovery for a tort fully compensates the victim at whose expense one has unjustly received a benefit. Similarly, where a breach of contract has occurred, the victim's restitutional interest has been impinged upon since it is at his expense that the abuser has wrongfully benefitted. Thus, in the breach of contract situation, restitutional recovery serves to make the victim of the breach whole.

Restitution itself may be an independent basis for liability. The Supreme Court of Colorado has recently awarded restitutional recovery to a cable television corporation for a harm characterized as

78. Restatement of Contracts § 339 (1932) requires the amount so fixed to be "a reasonable forecast of just compensation for the harm that is caused by the breach," and the harm must be one that is "incapable or very difficult of accurate estimation."

Restatement (Second) of Contracts § 370 (Tent. Draft No. 14, 1979) requires the liquidated damages to be "an amount that is reasonable in the light of the anticipated or actual harm caused by the breach and the difficulties of the proof of loss."

79. Restatement (Second) of Torts § 222A comment c (1965).

wrongful conversion of the plaintiff's subscription cable service. In *Cablevision of Breckenridge v. Tannhauser Condominium Ass'n*,[80] the plaintiff Cablevision Corporation, pursuant to an oral agreement with a representative of the owners of the defendant's condominium complex, installed the equipment necessary to provide Cablevision and F.M. radio service to thirty-three condominiums. After two years of properly servicing and billing all thirty-three units at the specified rate per unit, Cablevision was requested to serve and bill only three units. In addition, when a new, twenty-five unit complex was built, Cablevision was never requested to provide service. The new complex, however, was internally wired to the first building, and plaintiff's service was being provided to all twenty-five units without any payment being made to plaintiff. After discovering this, Cablevision filed suit against the condominium association for the unauthorized use of its subscription cable service. The court found as an undisputed fact that a representative of the owners had disconnected the plaintiff's amplifier from the cable entering the complex and had connected his own. In effect, the complex was receiving television and F.M. radio service for fifty-eight units, while only three units were being billed.

Rather than classifying the defendants' conduct as the crime of theft, the district court awarded damages for wrongful conversion of the cable television service. The court of appeals reversed on the grounds that the only issue to be decided by the court was whether or not the defendant breached any contract with the plaintiff. The court essentially evaded the issue of conversion. After granting certiorari, the supreme court upheld the judgment of the district court in favor of the plaintiff. The court failed, however, to resolve the conversion issue. Instead, the decision was based on a separate, alternative basis of liability—unjust enrichment.[81]

The *Tannhauser* case is significant in that it evidences the propensity of the courts to resort to traditional theories of civil liability, such as conversion, where misappropriation of services takes place. Furthermore, the supreme court decision acknowledges the importance of analyzing such cases in terms of civil liability in order to deal most effectively with the abuse of services. By finding unjust enrichment and then granting the plaintiff restitution, the court was able to both deter the defendant from engaging in similar wrongful behavior and compensate the plaintiff, Cablevision Corp., for the full value of its services. The scheme of remedial civil liability served to impose a penalty upon the defendant that was commensurate with

80. 649 P.2d 1093 (Colo. 1982).

81. *Id.* at 1096.

the harm caused. In comparison, the penalties prescribed by criminal statutes and proposed legislation are not only harsh and inappropriate, they also fail to compensate the one harmed by the misappropriation.

Public policy requires that a person who is unjustly enriched at the expense of another must make restitution.[82] As dictum in *Tannhauser* indicates, misappropriation of computer services is an appropriate occasion for application of the doctrine of restitution.[83] Invocation of the doctrine need not depend upon the existence of any contract. Rather, it is dependent upon *the need to avoid unjust enrichment*.[84] When a person authorized to use computer services for specific purposes uses them for personal, unauthorized purposes and does not properly pay for them, that person is unjustly enriched.[85] Hence, restitution must be made to the person at whose expense the services were obtained.[86]

Whereas in *Tannhauser* the unjust enrichment was the value of the services that the defendant received free of charge, based upon the prescribed rate per unit, the unjust enrichment in a computer services misappropriation case is the value of the computer services received by the defendant, based upon the cost to the plaintiff. As stated above, this measure of damages is commensurate to the actual harm caused by the defendant.

The civil remedy has been described as providing full compensation to the victim of a conversion. To avoid being misled, however, into believing that restitution *alone* is a "cure-all," one must be aware of the effect that the dilatory nature of the judicial system has on the attainment of equitable resolutions. When an individual has borne the burden of paying for services improperly obtained by someone else, a *later* judgment for restitution *will not* fully compensate that person for his expenses unless pre-judgment interest is also awarded.[87] This is especially important where a large amount

82. RESTATEMENT OF RESTITUTION § 1 (1936).

83. *Tannhauser*, 649 P.2d at 1096-97. *See* 66 AM. JUR. 2D *Restitution and Implied Contracts* § 11 (1973) (various situations to which the doctrine of restitution applies.)

84. *Tannhauser*, 649 P.2d at 1097.

85. RESTATEMENT OF RESTITUTION § 1 (1936) comment a, states that: "A person is enriched if he has received a benefit. A person is unjustly enriched if the retention of the benefit would be unjust." Section 1 comment b adds that: [One] [c]onfers a benefit not only where he adds to the property of another, but also where he saves the other from expense or loss. The word 'benefit,' therefore denotes any form of advantage. The advantage for which a person ordinarily must pay is pecuniary advantage."

86. *See Tannhauser*, 649 P.2d at 1096; 66 AM. JUR. 2D *Restitution and Implied Contracts* § 3 (1973).

87. *See generally* Hussey Range Div. of Copper Range Co. v. Letromelt Furnace Div., McGraw Edison Co., 417 F. Supp. 964 (1976) (discussion of pre-judgment interest

of money is involved and the plaintiff would have been able to invest or earn interest on the money had he been able to retain it.

The element of uncertainty has been mentioned previously; it is another factor that could drastically interfere with the success of a civil cause of action and the recovery of pre-judgment interest.[88] If a party billed for computer services initiates an action against another party for conversion of a portion of those billed services, but cannot distinguish the amount of converted time from the time that was properly used, then a suit for damages will probably fail due to the plaintiff's inability to prove actual damages with certainty. As will be discussed below, such uncertainty can be prevented by keeping track of the amount of authorized computer use and the reasonable amount of time in which projects assigned to others should be completed. Any excessive additional use of computer services, other than that properly recorded, may then be attributed to misappropriation of the services; hence the uncertainty problem is avoided.

IV. METHODS BY WHICH TO ASCERTAIN DAMAGES IN A CIVIL ACTION FOR MISAPPROPRIATION OF COMPUTER SERVICES AND TO PROVIDE SECURITY FROM COMPUTER ABUSE

The ideal means of ascertaining damages caused by misappropriation of computer services would be by a statutory formula. A codified civil remedy for computer abuse would serve to notify citizens of exactly (a) what conduct constitutes misappropriation of computer services for personal benefits and (b) what sanctions will apply. The statute should enumerate the various bases of civil liability as discussed herein (i.e., conversion, breach of confidence, breach of contract, restitution) and delineate the elements of each offense. The statute should also specify the type of conduct that justifies an award of punitive damages and the means of calculating such damages. Overall, the statutory formula should seek to fully compensate the victim of the abuse for the fair value of the services wrongfully used.

Currently, there is no statutory formula that provides a civil remedial scheme for the compensation of misappropriated computer services. Due to the increased use of computers throughout our society, however, state legislatures will soon be forced to deal head-on

---

and an illustration of the majority of the courts' failure to grant such interest to a plaintiff). With respect to pre-judgment interest granted upon breach of contract, see RESTATEMENT OF CONTRACTS § 337 (1932).

88. Damages must be proved with certainty. RESTATEMENT OF TORTS § 912 (1939).

with the problem of misappropriation. Until then, victims of computer abuse must realize that basic civil causes of action may successfully be brought against misappropriaters of their computer services. Nevertheless, as a means of preventing misappropriation from taking place initially, the following recommendations should be noted.

The first step for any employers or private parties responsible for paying for computer services should be to issue a policy statement to be read and signed by every authorized user of their computer equipment. The policy should set forth exactly what may or may not be done with the computer.[89] Specifically, these statements should (a) set forth the amount of time, if any, allowed for personal use of the computer, and (b) define, in exact terms, what constitutes *personal* use of the equipment.

Another important, but often overlooked, step would be to thoroughly investigate the individuals hired or otherwise authorized to utilize computer services.[90] Early detection of an irresponsible or dishonest person could later save a great deal of both time and money.

As a third step, access to the computer should only be available during certain hours (e.g., normal working hours). During other times, the services should only be accessible after properly complying with certain security procedures. Such security measures would prevent an otherwise authorized user from accessing the computer for unauthorized purposes during non-working hours (e.g., weekends or evenings), when he or she would be unobserved by others. Note that this type of abuse is often committed by using false identification, such as an access number that belongs to another person, in order to avoid being identified.[91]

To make sure that any unauthorized use of the computer can be proven with certainty, careful records of accessed computer time should be maintained, with accurate notations of the amount of computer time that each project should take, and actually does take, to complete. Who is entitled to use the computer, and for what purposes should also be documented. The importance of monitoring these records should be noted. Any unusual expenditure of computer time will be readily noticed under this system. Thus, any misuse may be rectified early. Also, the mere awareness by authorized

89. Howe, *supra* note 2, at 120.

90. For a brief discussion on the importance of investigating computer operators, see *id.* at 120.

91. *See* Nycum, *supra* note 30, at 285.

users of the measures taken to prevent computer abuse may serve to deter a potential abuser.

V. CONCLUSION

Action must be taken to deter the rapidly increasing problem of computer abuse. Parties that are the victims of misappropriation of computer services must be encouraged to initiate civil actions. Those civil actions will then serve to deter further abuse and to compensate the victims of the wrongful conduct.

Many states have either adopted, or are in the process of adopting, computer crime statutes. The application of those statutes is appropriate where criminal actions, such as embezzlement or fraud, occur. When the conduct constitutes conversion, breach of confidence, breach of contract or unjust enrichment, however, it should not be classified as criminally proscribed "theft of services."

When a person who is authorized to use computer services misappropriates the services by using them for personal, unauthorized purposes, a civil action will both penalize the wrongdoer in a manner commensurate with the harm caused and deter future wrongdoing. The remedial scheme will require restitution to be made by the wrongdoer to the victim of the misappropriation of computer services.

Robbin Lynn Itkin