The John Marshall Journal of Information Technology & Privacy Law

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

Article 20

1980

On Charging Computer Crime, 2 Computer L.J. 429 (1980)

Donald G. Ingraham

ON CHARGING COMPUTER CRIME

By DONALD G. INGRAHAM*

INTRODUCTION

The first myth about computer crime is that it exists; the second is that it does not matter. The advent of the computer did not create a new crime, any more than the development of the automobile created a new form of larceny. As with the automobile, the criminal use of computer technology has increased the vulnerability of the community, and to the extent that the definition of crimes and the enactment of prohibitions is directed to the protection of the community, computer technology is a legitimate area of penal concern.

For the prosecutor, crime done by a computer is still crime. The difficulty in addressing this form of conduct comes not from the illegitimate and already prohibited ends, but from the complexity of the means. Computer technology has not only increased the potential effect of criminal applications, but has bred schools of red herrings to divert and dismay the trier of fact.

The argument that special recognition is not needed for computer crimes overlooks the basic need for laws to proscribe conduct, as well as to enable the redress of wrongs. The impact of a new technology is seldom consistent; the horse enabled the Cheyenne to become arguably the greatest light cavalry this side of Mongolia, while it provided the Piaute culture with a prime source of food.

The argument that computer-related crimes need no special recognition to enable their prosecution not only ignores the constitutional necessity of proscription, but logically could be applied to most laws. For example, attempted commercial burglary could be regarded as a usurpation of store floor space, and treated as a theft of the property interest in occupancy. Under such a statute, the vic-

* B.A. 1959, University of California; L.L.B. 1962, University of California School of Law (Boalt Hall). Mr. Ingraham is a member of the Bars of the State of California and United States Supreme Court, and is currently senior deputy district attorney (planning) Alameda County, California. He is past-Chairman, Computer Abuse subsection, Section on Law and Technology, American Bar Association and consultant to the Office of Technology Assessment, United States Congress.

tim would necessarily be compelled to calculate the value of the property invaded and the duration of the invasion. The prosecution would be for the theft of those values, and not for the intrusion as a crime complete in itself. It is precisely that absurdity —the requirement that the victim prepare evidence of an injury other than that with which he is really concerned—which the so-called computer crime bills have recognized and sought to redress.

I. The Problem of Charging a Computer Crime

The problem that computerization poses for prosecutors is also unchanged—drafting an accusatory pleading which identifies a statutory prohibition with the conduct in question. The pleading must not only fairly apprise the accused of the specific wrong committed, but must also achieve for the victim the vindication of those rights which society has undertaken to protect. This problem is exemplified in the case of *United States v. Jones*,[1] which turned on whether the creation of a false account number, and the attribution to that account of $133,681.77 worth of legitimate accounts receivable, constituted fraud or forgery. Because the check thereafter generated by the computer was drawn on a foreign bank, the United States attorney could prosecute only if the conduct were considered fraud, rather than forgery, since forgery of securities issued by a foreign bank is expressly excluded from the applicable statute.[2]

The United States district court for Maryland dismissed the prosecution on the basis that the critical document in the process was the accounts payable distribution slip on which the suspect had substituted the deceptive payee's account number. The slip was the input document for the keypunch operator, and attested to the verification of the account payable item by the invoice audit clerk. The

1. 414 F. Supp. 964, 6 CLSR 197 (D. Md. 1976), *rev'd*, 553 F.2d 351, 6 CLSR 209 (4th Cir. 1977).

2. * * *

> Whoever receives, conceals, stores, barters, sells, or disposes of any falsely made, forged, altered or counterfeited securities . . . moving as, or which are a part of, or which constitute interstate or foreign commerce, knowing the same to have been so falsely made, forged, altered or counterfeited;
>
> * * *
>
> Shall be fined not more than $10,000 or imprisoned not more than ten years, or both.
>
> This section shall not apply to any falsely made, forged, altered, counterfeited, or spurious representation . . . of an obligation, bond, certificate, security, treasury note, bill, promise to pay, or bank note, issued by any foreign government or by a bank or corporation of any foreign country.

18 U.S.C. § 2315 (1979).

alteration which worked the wrong was done by the supervisor of the accounts payable department.

The dismissal was based upon the court's analysis of the wrongful act. In rejecting the government's theory that it was not a forgery, and therefore could be prosecuted, the district court distinguished the case at bar from the conclusion of Clark and Marshall in their treatise,[3] that there can be no forgery if another person's signature is obtained on the instrument by false representation of the instrument's contents, purpose or accuracy. There was no other person, only a subservient staff and a compliant computer. It was a one-party transaction.[4]

Reversing the district court, the appellate court reasoned that:

> We think, however, that the acts of [defendant] did not constitute the *making* of a *false writing*, but rather amounted to the creation of a writing which was genuine in execution but false as to the statements of fact contained in such writing.[5]

The crime did not lie in the instrument, but in the defendant having implicitly deceived the computer and those who feed it into believing that there was a bona fide obligation to a person to whom none, in fact, existed. Therefore, it was found to be fraud, not forgery.[6]

Fascinating as this exegesis may be to the legal profession, it does little to alleviate the increasing public dismay over the efficiency and effectiveness of the criminal justice system. Throughout the appellate process in *Jones*, there was no denial that property had been wrongfully obtained, and personal careers had been severely jeopardized.

Though it is in just such fine distinctions that our liberties are rooted, the prospect of dismissal of a criminal case because of a discrepancy between statutory concepts and computer systems concerns those to whom the public looks for the protection of victims' rights, and argues compellingly for the sort of protection which the California legislature recently afforded property residing in computers.[7]

Nor is the overlooked loophole a creation of the computer era. As Oliver Wendell Holmes said over eighty years ago:

> We think it desirable to prevent one man's property being misappropriated by another, and so we make larceny a crime. The evil is

---

3. W. CLARK & W. MARSHALL, A TREATISE ON THE LAW OF CRIMES § 12.34 (1967).

4. 414 F. Supp. at 969, 6 CLSR at 205.

5. 553 F.2d 351, 355, 6 CLSR 209, 214 (4th Cir. 1977); emphasis in original.

6. Id. at 356, 6 CLSR at 216.

7. CAL. PENAL CODE § 502 (West Supp. 1979). The text of this statute is reprinted in the Appendix in the next issue of the Journal.

> the same whether the misappropriation is made by a man into whose hands the owner has put the property, or by one who wrongfully takes it away. But primitive law in its weakness did not get much beyond an effort to prevent violence, and very naturally made a wrongful taking, a trespass, part of its definition of the crime. In modern times the judges enlarged the definition a little by holding that, if the wrongdoer gets possession by a trick or device, the crime is committed. This really was giving up the requirement of a trespass, and it would have been more logical, as well as truer to the present object of the law, to abandon the requirement altogether. That, however, would have seemed too bold, and was left to statute. Statutes were passed making embezzlement a crime. But the force of tradition caused the crime of embezzlement to be regarded as so far distinct from larceny that to this day, in some jurisdictions at least, a slip corner is left open for thieves to contend, if indicted for larceny, that they should have been indicted for embezzlement, and if indicted for embezzlement, that they should have been indicted for larceny, and to escape on that ground.[8]

To which Mr. Justice Holmes would surely have added, if in superior prose, ". . . and if the thief uses a computer, to lose his pursuers in a maze of circuitry."

The computer not only facilitates crime by permitting a malefactor to exploit the speed and the naivite of his employers, but it also permits theft without deprivation. *Ward v. Superior Court*[9] concerned the use of a shared terminal and a third party's account number to cause a computer as one location to send a copy of a particular program to a competitor at a remote location. As the end of the six-second transaction, the program in question resided in both locations and, but for a fortuitous but unintended punched card dump[10] of the program, the theft might only have been detected after the victim had lost the competitive edge that the program had given it.

Ward's unauthorized duplication was assessed by the accusatory pleading as having violated two criminal prohibitions: grand theft[11] in the amount of the market value of the program, and theft

---

8. O. Holmes, *The Path of the Law, reprinted in* THE MIND AND FAITH OF JUSTICE HOLMES 84 (M. Lerner ed. 1954).

9. 3 CLSR 206 (Cal. Super. Ct. 1972).

10. A "punched card dump" is the result of transferring the contents of storage or of a part of storage onto paper cards. *See* AMERICAN NAT'L DICTIONARY FOR INFORMATION PROCESSING, *reprinted in* 1 R. BIGELOW, COMPUTER L. SERV. § 1-3 art. 1, at 53.

11. Grand theft is theft committed in any of the following cases:
> 1. When the money, labor, or real or personal property taken is of a value exceeding two hundred dollars ($200); * * *.

CAL. PENAL CODE § 487(1) (1965).

of a trade secret, a statutory offense in California.[12] The prosecutor chose not to pursue a "theft of time" theory, since the six seconds which the electronic transfer took from the business of the main computer was deemed too short to represent a significant loss in duration—though not in effect.[13] In *Ward*, the prosecutor had the advantage of a distinct product of definable commercial value. Even so, it was necessary to express the wrong in terms of asportation to meet the definition of theft,[14] and even then the court ruled in dicta that the asported program had to be tangible—reduced to visual form—for the law to protect it.

> Implicit in the definition of "article" contained in Section 499c(a) is that it must be something *tangible*, even though the trade secret which the article represents may itself be *intangible*. Based upon the record here, the defendant Ward did not carry any tangible thing representing ISD's Plot/Trans Program from the ISD computer to the UCC computer unless the impulses which defendant allegedly caused to be transmitted over the telephone wire could be said to be tangible. *It is the opinion of the Court that such impulses are not tangible and hence do not constitute an "article"* within the definition contained in Section 499c(a)(1) as inclusive of "object, material, device or substance or copy thereof, including any writing, record, recording, drawing, sample, specimen, prototype, model, photograph, microorganism, blueprint or map." All of the foregoing things are tangible and under the principle of ejusdem generis, telephonic impulses would not constitute an article representing a trade secret.[15]

Whatever may be said of this analysis as an indication of judicial perception, particularly since on the facts of the case it was wholly gratuitous, it would clearly frustrate the rightful owner's reasonable and understandable expectation to be told that he had suffered no wrong that the court would hear until the form of unlawful possession became one which could be folded into a glider. For the very practical purpose provided by the program, reduction to print on paper would be wholly irrelevant.

Nor can all illegal uses of computers necessarily fit comfortably into theft analogies. A recent, unreported problem which confronted

---

12. *Id.* § 499c.

13. The author was prosecutor in the case.

14. The completed crime of larceny—as distinguished from an attempt—requires *asportation* or carrying away, in addition to the taking. * * * The requirement of asportation is not satisfied unless it is shown that "the goods were severed from the possession or custody of the owner, and in the possession of the thief, though it be but for a moment."

1 B. WITKIN, CALIFORNIA CRIMES, *Crimes Against Property* § 378 (1963); citations omitted; emphasis in original.

15. 3 CLSR at 208; emphasis in original.

the Alameda County juvenile court concerned the unauthorized use of a remote-entry word processing computer at a local educational institution. Armed with gleanings from waste baskets and some paraphernalia from a neighborhood electronics store, the perpetrator was able to get past the entry codes and play freely with the defenseless data base, endangering the integrity of the work stored therein by legitimate users, and going so far as to deride the initial efforts to frustrate his transgressions. The embattled and embarrassed administrators turned to the local prosecutors, only to be required to put their injury in terms of loss of computer time, which the court could recognize as being within the ambit of the available remedies. Electronic trespass, though the breach of privacy and property was great, had to be wrapped in concepts which long predated the computer age.

To the extent that the law prohibits theft, it is difficult to see the social benefit of compelling the prosecutor to characterize the forbidden activities in a less than accurate guise in order to pass the law's threshold. Burglary and rape, for example, need not be prorated in a rental mode to obtain the law's protection, because the interest that each law protects is recognized as deserving protection far beyond its market value. Information, regarded by government, industry, and academia as a significant item of value, deserves no less protection. The necessity of taking the additional effort to calculate the amount of time misappropriated places a cost on this protection not borne by victims of other transgressions.

Even minimal experience with computer systems renders one wary of crashes or unscheduled down times. The aspect of wrongful intrusion into a processing queue, which is most difficult to fit into traditional charging language, is therefore the one that most justifies statutory proscription. The intrusion engenders a ripple effect, which can disrupt or even destroy property. The property, though in the form of impulses invisible to the keenest microscope and beyond the grasp of the nervous system, nonetheless can represent and affect personal endeavor and individual rights.

It is axoimatic in computerization studies that system analysis strips away the carapace and identifies the real purpose and nature of the entity under examination. It is, therefore, not surprising to see computers having the same effect on legal concepts, where interests like property and privacy, long reified into tangibles, are now seen in their naked necessity. The placement of such interests in the different jeopardy of a computerized environment was not done with the informed consent of those affected, but as an operational necessity.

The fact of greater and unfamiliar vulnerability of legal inter-

ests, with which the public is more accustomed to dealing in a physical fashion, should not be taken as a Luddite jeremiad against an apparently inevitable cultural development, nor as a flaw in the computer itself. The same recognition of the need for laws to respect rights in other previously intangible matter applies to issues of privacy, controls on undetected surveillance, and inheritability of commercial interest in personalities. For want of a less bromidic term, the legal agenda is moving "back to the basics," in which the physical entities with which lawyers have become familiar are being recognized as the vessels, and not themselves the valuable contents to be protected.

The difficulty of stringent statutes is well exemplified in *Regina v. McLaughlin*.[16] This case involved yet another instance of unauthorized, remote access use of a computer facility. Again, the motive owed less to Mammon or Moriarty than to the example of Sir Edmund Hillary, *i.e.*, it was there. It was apparently an intellectual challenge to break through and frustrate the security of the computer system.

The attorney general of Edmonton, Ontario, presented with proof that the challenge had been met and overcome, and that security had been breached, proceeded under section 287 of the Canadian Criminal Code,[17] and characterized the matter in the indictment as theft of telecommunication services. It should be noted that the intrusion did not crash the system, *i.e.*, make the system unavailable for legitimate users for any extended period of time.

The fundamental issue was whether or not the university's computer system was a telecommunication facility within the proscription of section 287. In finding that it was, Mr. Justice J. M. Hope reasoned in part:

> I turn now to the description given me of this facility. Throughout the trial it was referred to repeatedly as the computer as indeed it is called in modern day terminology. Dr. Allen in the course of his evidence referred to the facility as consisting of main frame, central processing unit, terminals, memory, printers all essential to the system.
>
> * * *
>
> Dr. Bent referred to the "central processing unit" as one part,

16. Unpublished oral judgment of the Hon. Mr. Justice J. M. Hope, Supreme Ct. of Alberta, Trial Div., Jud. Dist. of Edmonton, 32376-C (Dec. 14, 1978), *aff'd*, 7 CLSR 406 (Alb. Ct. App. 1979).

17. Section 287(1)(b) makes it an offense to "fraudulently, maliciously, or without colour of right," use "any telecommunication facility" or to obtain any "telecommunication service." *Id.* at 407.

and that there was some two dozen major units connected by electrical cable and that the computer was also connected to telecommunication facilities, and that there was at the time in question over 300 terminals for the unit, that some of the terminals were in the General Service Building wired directly to this Amdahl computer, and there were electromagnetic connections. He said that outside there was connection by telephone, that is, telephone cable and coaxial cables, there was a dial up connection by phone through the facilities of Edmonton Telephones, Alberta Government Telephones, and the Trans Canada Telephones System. Through these phone facilities the computer can be accessed by single telephone means. He described the terminals as being a "Deck Writer" (sic) types, and expanded by comparing them to typewriters. These Deck Writers record the dialogue between the operator and the computer on the computer sheets, which we have heard designated as "hard copy." He described C.R.T., cathode ray tube terminal, as printing on a screen on the terminal itself. He described a "buffer" as being part of the facility and used as the computer memory in one sense.

In the course of the evidence it was shown that a failure of electrical power from Edmonton Power shut down the facility. At one point he indicated the means of transmission from the terminal to the central processing unit was by electromagnetic signal, and that the terminal and its connections to the central processing system were all part of the facility.

It was interesting to me to note in my research that I could find no definition of the word "computer" in such well-known legal books as "Black's Law Dictionary, Fourth Edition," or in "Words & Phrases Legally Defined, Second Edition," or in "Words & Phrases Legal Maxims Canada, Second Edition."

I examined Webster's Third New International Dictionary and found among the definitions for a "computer" as being:

> an automatic electronic machine for performing simple and complex calculations. Any of several devices for making rapid calculations in navigation or gunnery.

From this it is apparent that in ordinary language as distinct from perhaps legal definitions, certainly it is recognized that the elements of being "automatic" and "electronic" and "several devices" are included when we speak of computers.

I don't consider it would be useful for me to refer to any other evidence in respect to this aspect. I say that from the evidence that I have mentioned, and the whole of the evidence of the case, I am satisfied beyond a reasonable doubt that the computer in all its components is a telecommunications facility within the meaning of the very wide definition that I have previously mentioned.[18]

---

18. *See* note 16 *infra.*

While perhaps technically correct, it does seem clear that a wrong was committed, and that a clearer proscription would, at the least, enhance the administration of justice. The price of uncertainty in criminal law is not paid by the prosecutor, but by the victim and the community whose interests are thereby excluded from consideration of the courts. Unfortunately, and perhaps unfairly, the gap between the ravished right and the succoring statutes is often difficult to bridge and, particularly in computer-related crimes, the charging process is critical.

II. THE CHARGING PROCESS

Before the vandalized victim and the intrepid investigator are able to approach the court, it is necessary that the violation be characterized in terms of an offense or offenses recognized by the statutes. This process of writing up the wrong done is called "charging"—drafting the accusatory pleading or filing the complaint. Charging, the process through which the investigation of an offense and the accumulation of evidence to prove it becomes the accusatory pleading with which the defendant will be charged, is belatedly receiving recognition as the heart of the prosecution process. Experience has demonstrated that even a court willing to permit broad evidence may be restrained from allowing a significant gap between pleading and proof.[19] No investigation should be initiated without the clear guidelines afforded by the available statutes, and no case should be accepted for filing without explicit satisfaction of the statutes. The enormity of the loss and the prestige of the victim set in motion influences which can trigger the crippling raglan reflex,[20] under which the attitude of "Charge something now and amend it later" may swamp the circuits.

Computer-related crimes are relatively new, and few legislatures have extended to them the recognition already afforded gilts, barrows, jacks, jennies, suine carcasses, amalgam, broadsides, flumes or avocados.[21] Even automobiles are a relatively recent protected class. Justice precludes procrastination until yet another specification is brought within the eighth commandment, and the prosecutor faced with a computer-related crime is afforded the all-too-rare opportunity to exercise creativity.

---

19. *In re* Hess, 45 Cal. 2d 171, 288 P.2d 5 (1955).

20. The raglan reflex was first noted in Fitzroy Somerset, first Lord Raglan, whose decision to charge at Balaclava in 1854 demonstrated that sincerity and dedication alone cannot overcome reality. Reflexive charging has been militarily rare since the decline of the cavalry, but it is still often encountered in prosecution.

21. *See, e.g.*, CAL. PENAL CODE § 487(1) & (3) (1965).

The first step in charging a computer-related crime, is to ascertain precisely what was done. This does not require a knowledge of binary logic or a grasp of the distinction between software and hardware. Indeed, such expertise might actually prove a disadvantage, since the prosecutor might overlook the fact that such knowledge is not common, and should not be assumed to be held by either the judge or the jury. If so esteemed a leader of the legal profession as retired Associate Justice Arthur J. Goldberg can flaunt his ignorance of computer technology,[22] it should not be thought that the courts will soon be as familiar with computers as they have become with horseless carriages.

As more and more states accept the need for particular protections for computer-stored information, the problem now frequently encountered of converting trespass to theft will inevitably be reduced. The development of new legislation should include, at a minimum, a strong disclaimer that it is not intended to pre-empt other statutes which might, depending on a particular case, be more appropriate and more susceptible to proof. Striking a watchman with a disk pack should remain the battery that it is, and not be elevated to the status of a computer crime. There are enough red herrings in our courts already.

Most computer-related crimes are, at their core, the same crimes that have been prosecuted since the apple was plucked and Cain was banished. At the outset of every investigation, and surely no later than the drafting of the complaint, visions of dazzling one's peers with electronic competence and the prestige of flourishing a new statute should be weighed against the hard realities of the judge and prospective jury. Any juror with even a scintilla of familiarity with computer technology likely will be weeded out, leaving only persons whose sole connection of computers is fiscal, monthly, and frustrating.

Even lacking a specific computer-related crime statute, consideration should be given whether a theft charge, particularly *by* embezzlement or false pretenses, or *of* trade secrets or commercial assets, might not do as well. The theft of time requires accounting, and, even though time has a market value, there have been significant delays in developing admissible proof of its value. Where personal information is the pelf, the currently developing bodies of privacy protective legislation may yield a malleable statute. Finally, the generally liberal acceptance of evidence based upon a conspiracy theory might justify such a charge.

22. Beeler, *Ex-Justice Goldberg Sees Privacy Major Issue*, Computerworld, Apr. 9, 1979, at 20, col. 1.

III. CONCLUSION

Computer crime *does* exist, and computer-related crime even more so. Wrongs are suffered and losses incurred well beyond that foreseen by the wrongdoer. Doing something about it is a challenge which no prosecutor can avoid, though it calls him even unto the Halls of Legislation. The rights, property and liberty of those that prosecutors claim to protect are vulnerable from a new direction, and the drums are rolling.