UIC John Marshall Journal of Information Technology & Privacy Law

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

Article 26

1980

Case Digest, 2 Computer L.J. 777 (1980)

Drew Pomerance

CASE DIGEST

By DREW POMERANCE *

The materials in this section are intended to provide a concise overview of the United States case law relating to computer crime.[1] Each case is summarized in a separate digest entry. Each entry contains the following information:

- case name
- case citation
- subsequent history (if any)
- summary of salient facts
- legal analysis and holding of the court

The digest entries are organized alphabetically.

CR1 Hancock v. Decker, 379 F.2d 552, 1 CLSR 858 (5th Cir. 1967)

This was an appeal from the denial of a petition for habeas corpus. The defendant contended that he was unlawfully convicted of theft, in that the corporeal personal property that he was accused of taking did not have a value in excess of $50.00 as required by Texas law.[2] In affirming the denial, the court found that there "was ample evidence that [the defendant] committed the offense for which he was indicted."[3]

CR2 Hancock v. State, 402 S.W.2d 906, 1 CLSR 562 (Crim. App. 1966).

The indictment alleged theft of fifty-nine documents, which consisted of computer programs. The defendants were an employee of Texas Instruments and an employee of an insurance company. The defendants took the listings of these programs and attempted to sell

* B.A. Political Science, University of California at Berkeley. Mr. Pomerance is currently a third-year student at Hastings College of the Law, San Francisco, California.

[1] Only cases focusing on the crimes themselves are covered. Not included are computer crime cases where the question before the court was merely one concerning the admissibility of evidence or other collateral issue.

[2] 379 F.2d at 552, 1 CLSR at 858.

[3] *Id.* at 553, 1 CLSR at 859.

them to Texaco. Texaco contacted Texas Instruments, and the defendants were arrested.

The issue presented to the court was whether the computer programs constituted corporeal personal property as that term is used in the Texas theft statute. The statute defines "property" to include, *inter alia*, "all writings of every description, provided such property possesses any ascertainable value."[4] The testimony indicated that the programs had a reasonable market value of approximately $2.5 million. The court found that the programs were property within the meaning of the statute.[5]

The defendants also challenged their conviction on the ground that there was no evidence showing the market value of the computer programs. The court quoted a large portion of the testimony of a vice-president of Texas Instruments, and the manager of the computer center at Texas Instruments,[6] and found that this evidence was sufficient to authorize a finding that the computer programs had a market value "in excess of $50.00 each."[7]

CR3 United States v. Curtis, 537 F.2d 1091, 6 CLSR 1402 (10th Cir. 1976).

The defendant was convicted of mail fraud.[8] Defendant's scheme was a purported computerized dating service. In fact, the matching was accomplished manually by untrained clerical workers or by the defendant himself. The court held that there was substantial evidence in the record to establish the elements of the offense as charged, and upheld the conviction.

CR4 United States v. Jones, 414 F. Supp. 964, 6 CLSR 197, *rev'd*, 553 F.2d 351, 6 CLSR 209 (4th Cir. 1977).

Defendant Jones was charged with transportation of stolen, converted, or fraudulently obtained securities and with receiving, selling or disposing of those securities knowing them to have been stolen, converted or taken by fraud.[9] The securities at issue were five checks, made payable to the order of "A.L.E. Jones," and drawn on a Canadian bank against the account of a Canadian firm. The government alleged that the defendant transported the checks from Canada to Maryland and deposited the checks in a Maryland bank

[4] 402 S.W. 2d at 908, 1 CLSR at 865.

[5] *Id.*

[6] *Id.* at 909-11, 1 CLSR at 567-69.

[7] *Id.* at 911, 1 CLSR at 569.

[8] 18 U.S.C. § 1341 (1976).

[9] *Id.* §§ 2314, 2315.

account. The dispute revolved around the question of whether or not the securities, *i.e.*, the checks, were genuine, or instead were forgeries of checks of a foreign corporation to which federal law does not apply.[10]

The difficulty that the trial court had with the issue arose because the checks were printed by computer, complete with authorized facsimile signatures, and were printed as a direct result of tampering with the data stored in the computer and with the payment data input to the computer. The question facing the judge was whether these checks could be characterized as "falsely made, forged, altered, counterfeited or spurious."

The judge held that "the mere fact that a computer was used to print these checks should not be permitted to confuse the matter."[11] The judge found that the computer merely acted as an extension of the defendant's accomplice and that the checks therefore fit within the definition of forgery.[12] Since the court found that the crime was forgery, the acts did not come within the proscription of federal law and the indictments were dismissed.

On appeal, the court held that instead of forgery, the crime was fraud or false pretenses. In making that ruling, the court made the following distinction:

> We think, however, that the acts of [defendant's accomplice] 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 facts contained in such writing. The distinction is critical to the sufficiency of the indictment.[13]

The court found that the Canadian firm's accounting department was defrauded into believing that the company owed a *bona fide* obligation to defendant Jones, and, accordingly, issued a "*genuine instrument containing a false statemept of fact as to the true creditor*."[14] Since the check did not fall within the forgery exclusion of the statutes, the court reversed the district court and reinstated the indictment.[15]

[10] Section 2314 provides in pertinent part:

> This section shall not apply to any falsely made, forged, altered, counterfeited or spurious representation of an obligation or other security . . . issued by any foreign government or by a bank or corporation of any foreign country.

Id. § 2314.

[11] 414 F. Supp. at 969, 6 CLSR at 205.

[12] *Id.* at 969, 6 CLSR at 205-06.

[13] 553 F.2d at 355, 6 CLSR at 214 (emphasis in original).

[14] *Id.* at 355, 6 CLSR at 215 (emphasis in original).

[15] *Id.* at 356, 6 CLSR at 217.

CR5 United States v. Lambert, 446 F. Supp. 890 (D. Conn. 1978).

The defendants were charged with selling information obtained from the Drug Enforcement Administration pertaining to the identity of possible informants and the status of drug traffic investigations. Defendant was indicted under 18 U.S.C. § 641.[16] On defendant's motion to dismiss, the court held that: (1) the statute is not restricted to the theft of tangible property, but the phrase " 'thing of value,' in conjunction with the explicit reference to 'any record,' covers the context of such a record"[17]; (2) the statute is not unconstitutionally vague and "an individual planning the unauthorized sale of information held in a government data bank had sufficient notice that such conduct would be covered by § 641"[18]; and (3) the statute is not facially invalid for overbreadth, since a narrow interpretation is possible which avoids deterring constitutionally protected speech.[19]

CR6 United States v. Sampson, 6 CLSR 879 (N.D. Cal. 1978).

Sampson, a former employee of the Institute for Advanced Computation, Inc. ("IAC"), a NASA contractor, and Miller, an employee of IAC, obtained unauthorized use of a United States government computer without the intent to reimburse the government for such use. Sampson used one of his home telephones to gain access to the computer, using the code name "Captain Libra." A NASA investigator discovered from computer printouts that a person using the name "Captain Libra" had used the computer. The investigator then confronted Sampson and Miller with the printouts, whereupon both admitted that these printouts reflected portions of their unauthorized use of the computer. Based upon Sampson's statement that he used the computer for an average of six hours per week for thirty-two weeks, a value of $1,924.00 was calculated for the commercial cost of Sampson's computer utilization.

Both Sampson and Miller were indicted for violations of 18

[16] Whoever embezzles, steals, purloins, or knowingly converts to his use or the use of another, or without authority, sells, conveys or disposes of any record, voucher, money, or thing of value of the United States or of any department or agency thereof, or any property made or being made under contract for the United States or any department or agency thereof; of

Whoever receives, conceals, or retains the same with intent to convert it to his use or gain, knowing it to have been embezzled, stolen, purloined, or converted . . . .

18 U.S.C. § 641 (1976).

[17] 446 F. Supp. at 895.

[18] *Id.* at 896.

[19] *Id.* at 896-900.

U.S.C. § 641.[20] Defendants moved to dismiss the indictment on the ground that it failed to state a criminal offense, arguing that computer time and computer storage capacity were not "property" within the meaning of the statute.

The district court denied the motions, holding that the consumption of computer time and the use of computer storage capacity were inseparable from the physical identity of the computer itself. The court found the indictment legally sufficient, because the computer time and the use of its storage capacities were "things of value."

CR7 United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

Optimum Systems, Inc. ("OSI"), a computer service company, was under contract to install, maintain, and operate a computer facility at Rockville, Maryland, for use by the Federal Energy Administration ("FEA"). Under the contract, persons working for FEA in various parts of the country could use keyboards at communications terminals in their offices to send instructions over telephone circuits to the computers in Rockville; the computers' responses would be returned over telephone circuits and displayed on the sender's CRT (cathode-ray tube) terminal.

Seidlitz helped to prepare the software installed at the Rockville facility and was responsible for the security of the central computer system. After approximately six months as Deputy Project Director of OSI, Seidlitz resigned his job and returned to work at his own computer firm in Alexandria, Virginia.

Approximately six months later, a computer specialist employed by FEA, and temporarily assigned to the OSI facility, detected an unauthorized intruder who had gained access to the computer system. It was determined that the intruder had gained access by telephone from outside the OSI facility. The telephone company was then requested to trace the call. The telephone company manually traced[21] the call to Seidlitz' Alexandria office, but would not divulge the results of the trace except in response to a subpoena.

The following day, OSI activated a special feature of its computer system, known as the "Milten Spy Function," which automatically records any requests made of the computer by an intruder and any computer responses to such requests. The telephone company was again asked to trace the call when it was suspected that the un-

[20] *See* note 16 *supra*.

[21] A manual trace entails a physical tracing of the telephone circuitry backward through the various switching points, and does not involve listening in on the line or breaking into the conversation.

authorized person was using the computer. This trace lead once again to Seidlitz' Alexandria office, though OSI was not so informed.

OSI then advised the FBI of the intrusions and, at the FBI's suggestion, the telephone company conducted two additional manual traces when alerted by OSI. Both of these calls were terminated, however, before the traces had progressed beyond the telephone company's office in Lanham, Maryland, which served 10,000 subscribers. The telephone company then installed "originating accounting identification equipment" in the Lanham office.[22] Shortly thereafter, two calls were made to the OSI computer and were traced to Seidlitz' Lanham residence. The FBI then searched (with a warrant) Seidlitz' Alexandria office, seizing, *inter alia*, a copy of the user's guide to the OSI system and some forty rolls of computer paper on which OSI source code was printed. Seidlitz' Lanham residence was also searched (with a warrant), where the officers found a portable communications terminal which contained a teleprinter for receiving written messages from the computer, as well as a notebook containing access codes previously assigned to authorized users of the OSI computers.

The indictment against Seidlitz charged him with transmitting two telephone calls in interstate commerce as part of a scheme to defraud OSI of property consisting of information from the computer system.[23]

Seidlitz filed a motion to suppress the evidence seized from his office and residence, claiming that the searches had been invalidated by the use of illegal electronic surveillance to obtain the information contained in the affidavits supporting the warrants. The district court rejected this motion ruling, *inter alia*, that the information obtained by use of the "Milten Spy Function" was not covered under Section 605 of the Communications Act of 1934[24] and that neither Title III of the Omnibus Crime Control and Safe Streets Act of 1968[25] nor the fourth amendment[26] were violated, since the information was obtained with the consent of a party to the defendant's telephonic communciations. The court further ruled that neither Title III nor the fourth amendment were violated during the tracing of the telephone calls, since the number of the telephone from which

[22] This equipment automatically ascertains, without interrupting any communication, the telephone number of any of the 10,000 area telephones from which any subsequent calls to the OSI computers originated.

[23] This is the federal wire fraud statute. 18 U.S.C. § 1343 (1976).

[24] 47 U.S.C. § 605 (1976).

[25] 18 U.S.C. §§ 2510 et seq. (1976).

[26] U.S. CONST. amend. IV.

the calls were placed was determined by a process which did not entail the interception of the *contents* of the communciations.

Over defense objections, much of the challenged evidence was admitted at trial, and the telephone traces, as well as the operation of the "Milten Spy Function," were described to the jury. In the face of this evidence, Seidlitz conceded that he had retrieved the information from the computers, but claimed to have acted only out of concern for the security of the OSI system and stated that he intended to present the printouts to OSI officials to prove to them that their security was inadequate. Seidlitz also claimed that the software system that he retrieved—WYLBUR—was not a trade secret or other property interest of OSI sufficient to qualify as "property" within the meaning of the wire fraud statute.[27] Seidlitz was convicted of two counts of fraud by wire.

On appeal, Seidlitz renewed his "illegal surveillance" claims and further argued that the evidence before the jury was insufficient to establish either his fraudulent intent or that the WYLBUR system constituted "property." The court of appeals affirmed, holding that (1) the use of manual telephone tracers and the "Milten Spy Function" did not constitute an invalid electronic surveillance; and (2) there was sufficient evidence from which the jury could have found that the WYLBUR system was "property," and that Seidlitz possessed fraudulent intent in obtaining the WYLBUR system without authorization.

CR8 Ward v. Superior Court, 3 CLSR 206 (Cal. Super. Ct. 1972).

This is an unreported decision of a state trial court's ruling on the defendant's demurrer and motion to strike. Defendant Ward was an employee of University Computing Company ("UCC"), a computer service company. Ward was charged with theft of a trade secret belonging to ISD, another computer service company, in violation of California Penal Code sections 499C[28] and 487.[29]

The trade secret was a computer program titled "Plot/Trans," developed by ISD and valued at $5,000. This program gave ISD a competitive advantage over UCC and other competitors. Both the source code[30] and object code[31] of the program were stored in the

[27] 18 U.S.C. § 1343 (1976).

[28] *See* text accompanying note 33 *infra*.

[29] 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 (West).

[30] Source code (or source language) is the "original symbolic language in which a program is prepared for processing by a computer. It is translated into object lan-

memory of the ISD computer.

The evidence showed that on January 19, 1971, Ward dialed up the ISD computer, furnished a customer's site and billing numbers and secured a printout of the source code of the Plot/Trans program. Contemporaneously, the ISD computer punched out a card deck[32] of what had been accessed, on which the time of access was also punched. The theft was discovered when the card deck was delivered to Shell (the customer whose code numbers Ward used), and ISD learned that Shell had not accessed the program. An investigation of telephone records revealed that the call had come from UCC, and not Shell. A search warrant was obtained and the printout of the program was discovered in Defendant Ward's office at UCC.

California Penal Code § 499C(b) provides that:

> Every person is guilty of theft who, with intent to deprive or withhold from the owner thereof the control of a trade secret . . . does any of the following:
>
> 1. Steals, takes or carries away any article representing a trade secret.
>
> * * *
>
> 3. Having unlawfully obtained access to the article, without authority makes or causes to be made a copy of any article representing a trade secret.[33]

The court held that § 499C(a) requires that the "article" taken must be tangible, even though the trade secret which the article represents may itself be intangible. Based upon the record, the court found that the only thing that Ward "carried" from the ISD computer to the UCC computer were the electronic impulses transmitted over the telephone wires. The court held "that such impulses are not tangible and hence do not constitute an 'article' within the definition contained in Section 499C(a)(1) . . . ."[34]

The court did find, however, probable cause to believe that Ward had made a copy of the printout through the use of the UCC computer, and thereafter carried that copy from the UCC computer

guage by an assembler or compiler." C. SIPPL, DATA COMMUNICATIONS DICTIONARY 449 (1976).

[31] Object code is the "[o]utput from a compiler or assembler which is itself executable machine code or is suitable for processing to produce executable machine code." *Id.* at 330.

[32] A card deck is "[a] set, group or 'deck' of punched cards." *Id.* at 39.

[33] CAL. PENAL CODE § 499c(b) (West).

[34] 3 CLSR at 208.

to his office—an act forbidden by Section 499. Therefore, the court found probable cause to believe that the offenses were committed and that Ward had committed them, and overruled the motions.