COMPUTER JURISPRUDENCE

LEGAL RESPONSES TO THE INFORMATION REVOLUTION

MICHAEL D. ROSTOKER • ROBERT H. RINES

Franklin Pierce Law Center
Academy of Applied Science

OCEANA PUBLICATIONS, INC.
New York • London • Rome

The search warrant used in *Ward v. Superior Court* is a good example of the technical specificity that should appear in computer crime search warrants. The *Ward* warrant specified the "computer memory bank or other data storage devices, magnetically imprinted with Information Systems Design (ISD) remote plotting computer programs."[77] In addition to the difficulty in determining what to request in the search warrant, there is the uncertainty of the form of the requested items to be seized. This is a problem for the drafter as well as the executor of the warrant. A requested computer program may be found in the form of punch cards, printout sheets, or still in intangible form within the computer.[78] Certain state[79] and federal jurisdictions[80] allow police officers to use civilian assistance in conducting warranted searches. The experts are considered special police agents, so their actions are protected by the laws of agency.[81] Until police become more adept at conducting such searches, the practice of having computer experts accompany police on these search and seizure forays appeas to be worthwhile.

VI. EVIDENTIARY PROBLEMS

The presence of computers has created additional complexities and definitional problems within the accepted rules of evidentiary procedure. Such difficulties are inherent whether the prosecution is for a computer crime or a more traditional offense. The basis for seeking admission of computer evidence in litigation is under the business records exceptions to the hearsay rule. Like any other conforming document, computer-generated evidence which meets the specifications of the appropriate statute or common law rule will qualify as a 'business record.'

Until computer-generated documents are generally accepted, photocopy statutes can be used as a basis for admision of computer evidence. Photocopy statutes allow admission of reproductions made in the regular course of business, thereby allowing the reproductions to be considered equal to the originals. However, authorities consider computer outprint microfilm to be the production of originals and not copies of information.[82] There is usually the requirement that the reproductions be made on a durable medium. There are also federal[83] and state[84] photocopy statutes. Most of the state statutes are modeled after the Federal Uniform Photographic Copies of Business and Public Records as Evidence Act,[85] which has been adopted by 39 states.[86]

There are a number of specific business records rules which allow for the admission of computer evidence. These rules are basically similar, and courts of various jurisdictions have frequently cited cases concerned with admissibility, from jurisdictions following differing evidentiary rules. These rules are:

1) the Federal Rules of Evidence, Rule 803[87], especially subsectioned (6) [88], (7) [89], and (8);[90]

2) the former Federal Business Records Act,[91] which was repealed and replaced in 1975 by the present Federal Rule of Evidence 803(6);

3) the Uniform Business Records as Evidence Act (UBREA). 92 As of 1977 26 states had adopted his rule; 93

4) common law rules in effect in Mississippi and Illinois;[94] and

5) specific state statutes governing the admissibility of computer evidence, as in Massachusetts,[95] New Jersey,[96] North Carolina,[97] and Arkansas.[98]

Some of these rules are sufficiently similar in construction, as the Federal Rules of Evidence and the Former Federal Business Records Act, that some courts have readily applied the interpretations of the old statute to cases founded on the newer rule.[99] In general all these rules require that the offering of evidence be made in good faith in the regular course of business, prior to the current judicial proceeding, and that it was in the regular course of the business to make such a record at the time of the transaction, or within a reasonable time thereafter. There usually is also a requirement that a witness present information indicating the accuracy and reliability of the computer system that generated the evidence. In some statutes the courts have the discretion to also require that the original data be made available.[100]

Under The Best Evidence Rule, when the terms of a writing are the basis of a question in litigation, the original writing must be produced unless it is unavailable for some reason other than the fault of the producer.[101] This rule does not apply to the question of the existence of a writing. The focus of the best evidence rule is just that - securing the best available evidence. The rule is not aimed at excluding evidence. Once a satisfactory explanation is given for the absence of an original writing, secondary evidence is admissible.

The scope of the federal best evidence rule is equivalent to the same common law rule.[102] Computer art is specifically included in the definition section of the federal rule.[103] Generally, admissions allowed under one of the recent business records exceptions are exempt

from the Federal best evidence rule.[104] Also courts have allowed the admission of a computer printout (deemed a copy) made specifically for litigation because the stored information was constructed during the normal business routine, and the printout was just a manifestation of that information.[105]

One of the first appellate computer evidence cases was *Transport Idemnity Co. v. Seib.*[106] The issue was the admissibility of the computer printout. The suit involved payment on a contract for sales commissions. A computer printout indicating accounting payments was admitted into evidence over the objection that there was a lack of proper foundation for its admission. This was later the basis of appeal. The trial record indicatd that the defendant produced a witness who testified as to the computer procedures, their accuracy, and the general business procedure of putting accounting records into the computer. The court held that it was the intent of the UBREA statute to permit the admission of systematically entered records. Because a foundation indicating this had been shown, the decision was affirmed.

In a widely cited case, *United States v. De Georgia*, the court admitted a computer printout into evidence as corroborative proof that the car the defendant had been charged with stealing had in fact been stolen.[107] The printout indicated no evidence that the car had been properly rented. The only foundation laid for admission of this printout was testimony that it was the company's procedure to enter all of its business records immediately into the computer terminal. Therefore there was no tangible listing of this information other than the computer print-

out. Although this case is frequently noted for the holding that computer printouts are admissable evidence, the court in its opinion noted that it had not ruled on the adequacy of the foundation for the admission because at trial the defendant did not raise any objection to that issue.[108]

In Mississippi, a state that does not have any business record statute, a good example of common law interpretation of the admissibility of computer evidence occurred in the case of *King v. State ex rel. Murdock Acceptance Corp.*[109] The court here relied on *Transport Indemnity v. Seib*[110] in ruling that no particular form of record was required, so long as the best form of evidence was secured. The court indicated that the law must take notice of commercially sanctioned means of business. Additionally, the court required that the computer equipment be identified as to its accuracy and procedure, that the policy of entering information into the computer was a matter of business routine, and that the equipment used was considered standard in the business. The court did not require that witnesses be present to testify as to the time and place of information entry into the computer.

VII PREVENTION AND SECURITY

Breaching the security of computer data can take many forms. Unauthorized access to a program allows data to be destroyed, copied, or modified. Data transmission lines can be tapped. Of greater importance is the potential for the modification of the system's programmed security processes. In order to implement the laws enacted to prosecute computer crime, security measures must be devised to detect the law breaker.

Case law reflects that the detection of most of the perpetrators of computer crime is by accident and not by any deliberate security measure. In *United States v. Siedlitz*, the crime was accidentally detected by a programmer of the accessed system who noticed that an obsolete password was being used in the system.[111] The criminal action in *Ward v. Superior Court* was detected only because of the accidental dumping of computer punch cards simultaneously with the telephone intrusion into the system.[112]

Detection becomes easier when there is an immediate tangible effect of a breach. This ease parallels the impact that the tangible factor has in the prosecution of computer crime. Law enforcement information indicates that the probability of detection and prosecution of computer crime is 1 in 22,000.[113] Studies reflect that only approximately 15 percent of computer crime is reported.[114]

A recent survey of 283 large state and federal government agencies and private corporations indicated that the average annual individual loss from computer crime ranged from $2 million to more than $10 million.[115] This was a conservative estimate based on 'known and verifiable losses due to computer crime'.[116] The study indicated that the greater percentage of these losses were sustained when the computer was the object of the crime;[117] the greater percentage of the perpetrators of these crimes were people within the organization;[118] the most influential factor motivating these perpetrators was personal financial gain and the second most influential reason was the intellectual challenge of doing it;[119] respondents to the study indicated that they perceived more comprehensive self-protection by the private sector as the most effective means of detecting and preventing

computer crime;[120] and finally, that the most prevelant methods that the respondants used to accomplish this goal was limiting access to computer programs and logic, and limiting access to computer operations.[121]

The American Society for Industrial Security (ASIS) has promulgated a listing of specific recommendations for improved computer security. These guideline summaries include:

1) 'separation of knowledge' through division of responsibilities, job rotation, physical isolation, controlled access, logging of stop-pages and interruptions;

2) written programming instructions with threat monitoring and audit trails built in;

3) careful accounting of all input documents;

4) periodic changes in access codes and passwords; and

5) scramblers and cryptographic applications in data transmission. 122

Large computer companies, such as IBM, have also developed similar recommendations for commercial user security programs.[123]

Equipment security features cannot be the sole method of deterrence. The education of the public regarding the uses and abuses of computers, and the consequences of any actions with and against computers, must accompany any security plan in order for the plan to be successful. In our society today, computer skills are most rapidly being developed for school children. The computer is a very powerful tool. Power is accompanied by corresponding responsibility. Because of the inherent damages in the abuse of that power, society will be derelict in its duties if it teaches only how to use the computer

without also explaining the possible consequences.

Deterrence of computer crime can best be achieved by educating the public about the problem, by developing finer equipment security, by enacting specific laws to give notice of proscribed behavior, and by enforcing those laws.

VIII CONCLUSION

Although individual courts and legislatures have been slow to adopt comprehensive computer crime statutes, the apparent legarthy is due to a deficit in the technical skill necessary to define what constitutes a computer rather than the belief that the existing statutes are sufficient. Primarily the uncertainties in treating software intrusions have provided the greatest concern.

Redefinition of property values to provide violation of rights for diminution of value rather than the traditional loss of possession has provided a basis for a new era of statutes aimed at computer violators. Trade secret protection also provides a measure of protection by providing criminal sanctions for the unauthorized use of another's effenescent, through valuable, computerized data. However, trade secret protection alone provides only a limited range software that can be considered. Current legislation has attempted to use new definitions of computers, property, theft and larceny to give notice of prescribed computer-related behavior; however, this new legislation is largely untried by the courts and lacks inter-jurisdictional consistency.

Evidentiary acceptance of computers has been more easily adopted. Under the Federal Rules of Evidence, and other evidentiary procedure acts, the courts have generally allowed the introduction of computer generated information with only the most common of formalities.

Legislation alone, however, will not protect computers in the modern world. Efficient self-help measures, such as the installation of security devices and educating users as to the possible consequences of unauthorized computer useage will provide the other two cornerstones in the construction of a computer-secure society.

71. *Id.*, at 2191-2192.

72. *Id.*, at 2191-2192.

73. *Id.*, at 2192.

74. 1984 U.S.C.C.A.N. 509, *supra* note 63, at 530.

75. U.S. Const. Amend. IV.

76. *Katz v. United States*, 389 U.S. 347 (1967).

77. J. Becker, *The Investigation of Computer Crime*, app. 5 (1980).

78. J. Becker, *The Trial of a Computer Crime*, 2 Computer L.J. 441, 444, (1980).

79. See, *People v. Boyd*, 123 Misc.2d 634, 474 N.Y.S.2d 661 (Sup. Ct., 1984); *State v. Klosterman*, 317 N.W.2d 796 (N.D.1982); *State v. McColgan*, 631 S.W.2d 151 (Tenn. Cr. App. 1981); *People v. Superior Court*, 25 Cal. 3d 67, 157 Cal. Rptr. 716, 598 P.2d 877 (1979); *Commonwealth v. Farrar*, 271 Pa. Super. 434, 413 A.2d 1094 (1979); *State v. Scigliano*, 120 Ariz. 6, 583 P.2d 893 (1978).

80. See, 18 U.S.C. §3105 (1969); *United States v. Wright*, 667 F.2d 793 (9th Cir. 1982); *United States v. Clouston*, 623 F.2d 485 (6th Cir. 1980).

81. See, *People v. Esposito*, 37 N.Y.2d 156, 371 N.Y.S. 2d 681, 332 N.E.2d 863 (1975); *People v. Luciani*, 120 Misc. 2d 826, 466 N.Y.S.2d 638 (1983).

82. Bender, Computer Law,, *supra* note 33, at 6-19.

83. 18 U.S.C. §1732 (1976).

84. As of 1980 the following states had enacted state photocopy laws: Alabama, Alaska, Arkansas, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Idaho, Iowa, Kansas, Kentucky, Maine, Mary-

land, Massachusetts, Michigan, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York, North Carolina, North Dakota, Oklahoma, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virgin Islands, Virginia, Washington, West Virginia, Wisconsin, Wyoming.

85. 14 U.L.A. Civ. Proc. and Rem. Laws 145 (Master ed. 1980).

86. *Supra* note 84.

87. Fed. R. Evid. 803.

88. Fed. R. Evid. 803(6) states:

> A memorandum report, record, or data compilation, in any form, of acts, events, conditions, opinions, diagnoses, made at or near the time by, or from information transmitted by, a person with knowledge, if kept in the course of a regularly conducted business activity, and if it was the regular practice of that business activity to make the memorandum, report, record, or data compilation, all as shown by the testtimony of the custodian or other qualified witness, unless the source of the information or the method or circumstances of preparation indicate lack of trustworthiness. The term 'business' as used in this paragraph includes business, institution, association, profession, occupation, and calling of every kind, whether or not conducted for profit.

89. Fed. R. Evid. 803(7) *Absence of Entry in Records Kept in Accordance with the Provisions of Paragraph* (6) states:

> Evidence that a matter is not included in the memoranda reports, records, or data compilations, in any form, kept in accordance with the pro-

visions of paragraph (6), to prove the nonoccurrence or nonexistence of the matter, if the matter was of a kind of which a memorandum, report, record, or data compilation was regularly made and preserved, unless the sources of information or other circumstances indicate lack of trustworthiness.

90. Fed. R. Evid. 803(8) states:

> Records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth (A) the activities of the office or agency, or (B) matters observed pursuant to duty imposed by law as to which matters there was a duty to report, excluding, however, in criminal cases matters observed by police officers and other law enforcement personnel, or (C) in civil actions and proceedings and against the Government in criminal cases, factual findings resulting from an investigation made pursuant to authority granted by law, unless the sources of information or other circumstances indicate lack of trustworthiness.

91. 28 U.S.C. 1732(a) (1968).

92. 9A Uniform L. Annot. 506 (1965).

93. As of 1977 the following states had adopted UBREA: Arizona, California, Connecticut, Delaware, Georgia, Hawaii, Idaho, Michigan, Minnesota, Missouri, Montana, Nevada, New Hampshire, New Jersey, New York, North Dakota, Ohio, Oregon, Pennsylvania, Rhode Island, South Dakota, Tennessee, Texas, Vermont, Virgin Islands, Washington, and Wyoming.

94. Bender, Computer Law, *supra* note 33, at 6-96, 6-98.

95. Mass. Gen. Laws Ann. ch. 233, 78 (1970).

96. N.J. Stat. Ann. 2A:84, Rules 62(5) and 63(13) (1982).

97. N.C. Gen. Stat. 55-37.1 (1981).

98. U.R.E. 28-1001, Rule 803(6).

99. Bender, Computer Law, *supra* note 33, at 6-46.

100. E.g. Massachusetts.

101. McCormick, *Handbook of the Law of Evidence 229* (2d ed. 1972).

102. Bender, Computer Law *supra* note 33, at 5-54.

103. Fed. R. Evid. 1001 *Definitions* states:

> (1) Writings and Recordings. 'Writings' and 'recordings' consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing, photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation....(3) Original. An 'original' of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original'....

104. See, *United States v. Kimmel*, 274 F.2d Cir. 1960); *United States v. Vandersee*,279 F.2d 176 (3d Cir. 1960); *United States v. Anderson*, 447 F.2d 833 (8th Cir. 1971); *United States v. Miller*, 500F.2d 751 (5th Cir. 1974), rev'd on other grounds, 421 U.S. 1010 (1975).

105. *Transport Indemnity Co. v. Seib*, 178 Neb. 253. 260, 132 N.W.2d 871 (1965);*Com. v. Hogan*, 7 Mass. App.236 387 N.E.2d 158, 168 (1979), aff'd., 8 Mass. App. 921, 396 N.E.2d 978 (1979), aff'd., 17 Mass. App. 186, 456 N.E.2d 1162 (1983).

106. 178 Neb. 253, 132 N.W.2d 871 (1965).

107. 420 F.2d 889 (9th Cir. 1969).

108. *Id.*, at 894.

109. 222 So.2d 393 (Miss. Sup. Ct. 1969).

110. 178 Neb. 253.

111. 589 F.2d 152. (4th Cir. 1978).

112. 3 C.S.L.R. 206.

113. Volgyes, *The Investigation, Prosecution, and Prevention of Computer Crime:* A State-of-the-Art Review, *2 Computer L.J. 385, 388.*

114. *Id.* at 388.

115. ABA Task Force, *supra* note 1, at 14-15.

116. *Id.* at 13.

117. *Id.* at 17.

118. *Id.* at 19.

119. *Id.* at 22.

120. *Id.* at 23.

121. *Id.* at 24.

122. Sokolik, *Computer Crime - The Need for Deterrent Legislation*, 2 Computer L.J. 353, 368-369 (1980).

123. *Id.* at 369-370.

Original research and preliminary writings by:

Carla Ottaviano, B.A. Smith College, J.D. Franklin Pierce Law Center, was a Senior Probation Officer for the State of Connecticut Office of Adult Probation, now in private practice.