A Proposal for Protecting Privacy During the Information Age*

This note argues that current law does little to protect individual and business privacy from the significant threats posed by computer technology. While conventional criminal statutes can be used against certain misues of computer resources, most do not address the difficulties of safeguarding computerized data. Those statutes aimed at computer crime either are incomplete or do not target Alaskan computer resources. This note proposes an Alaskan statute carefully drafted to avoid the loopholes in most existing statutes. The statute contains both criminal provisions, graded to the severity of the misconduct, and civil provisions, containing a unique standard of care for system operators.

> A wonderful fact to reflect upon, that every human creature is constituted to be that profound secret and mystery to every other. A solemn consideration, when I enter a great city by night, that every one of those darkly clustered houses encloses its own secret; that every room in every one of them encloses its own secret; that every beating heart in the hundreds of thousands of breasts there is, in some of its imaginings, a secret to the heart nearest it![1] - Dickens

I. INTRODUCTION

According to a 1990 Harris survey, seventy-nine percent of Americans are "concerned about threats to their personal privacy."[2] Nearly seventy-five percent believe "they have 'lost all control over how personal information about them is circulated and

---

* The author wishes to thank Professor James E. Coleman for the encouragement and criticism that made this note possible.

1. Charles Dickens, A Tale of Two Cities 21 (Signet Classic ed., New American Library 1980) (1859).

2. Craig M. Cornish & Donald B. Louria, *Employment Drug Testing, Preventative Searches, and the Future of Privacy*, 33 WM. & MARY L. REV. 95, 114 (1991).

used by companies.'"[3] The pervasiveness of computers and computerized data collection undoubtedly forms the basis for at least part of these fears. Many tasks in modern society, from the making of hotel reservations and the collection of income taxes to the design of products, have been made more efficient and more profitable by the application of computer technology.[4] Computerized efficiency does not come without a price, however, and that price is a loss of privacy.[5]

Computers pose a unique threat to individual privacy because they render vast amounts of personal data instantly accessible to strangers. Once information enters a computer databank, the person who provided it, and often those who collect, store and use it, lose control of the information.[6] The information then becomes prey to viruses,[7] hackers[8] and even legitimate businessmen.[9]

---

3. *Id.* (quoting *Privacy: Survey Finds Public Concern Rising Over Protection of Personal Privacy*, DAILY REP. FOR EXECUTIVES, June 12, 1990, at A8).

4. *See* David C. Tunick, *Computer Law: An Overview*, 13 LOY. L.A. L. REV. 315 (1980).

5. For example, many businesses keep computer databases on clients that include such information as age, income and spending patterns. The information is often sold, without the customer's knowledge, to direct mail advertisers. *Id.* at 335. While such activities may appear innocuous, the concentration of personal information means businesses can decide whether to do business with individuals based on attitudes, tastes, interests, politics, etc., thus facilitating a sort of computerized discrimination. Jonathan P. Graham, Note, *Privacy, Computers, and the Commercial Dissemination of Personal Information*, 65 TEX. L. REV. 1395, 1404 (1987).

6. Graham, *supra* note 5, at 1399. "Databanking," the storage of files in a computer, is the computer technology most often identified with threats to privacy. "Datashadow," or the trail an individual leaves behind through a series of computer-recorded transactions, is a related danger. Because it is more expensive to delete information than to leave it in the database, outdated personal information may remain on file for years. *Id.* at 1400. For example, a recent study concluded that only 12% of criminal history records transmitted from a North Carolina database to other law enforcement agencies were correct. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 719 (1987).

7. "Virus" is a generic term for hidden computer instructions which are potentially harmful, sometimes altering data files or copying them into other databanks. Viruses replicate many times during a single execution of a legitimate program. They are passed on quickly through modems, disks and networks. In 1988, 60,000 computers were infected and 6200 halted by a virus unleashed on an academic network by a graduate student. Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 6-7 (1990). Although the virus did not damage any computer data, the event exposed the vulnerability of networks and computers to outside tampering. *Id.*

Although privacy invasion often comes in small doses, its effects can be substantial. For example, since most computer matching programs[10] use social security numbers to make matches between data files,[11] an industrious business could collect customers' social security numbers, comb the numerous national matching programs and compile detailed profiles of each customer.[12] Thus, through the application of computers, the incremental erosion of privacy quickly can turn into a wholesale loss.[13]

Alaska is not immune from the threats to privacy posed by computers. For example, in 1977 a major oil company intentionally intercepted the computerized transmission and processing of a competitor's data on bids for drilling rights in Alaska. The oil company then used the intercepted information to underbid the

---

8. "Hackers," outsiders who have experience in bypassing computer security systems, may break into computer systems to steal information or merely to challenge themselves.

9. More dangerous than the computer hacker is the unscrupulous legitimate user who already possesses knowledge about the operation of the computer system. Cheryl S. Massingale & A. Faye Borthick, *Risk Allocation for Computer System Security Breaches: Potential Liability for Providers of Computer Services*, 12 W. NEW ENG. L. REV. 167, 171-72 (1990). The American Bar Association estimates that over 77% of computer crimes are committed by insiders. A.B.A. Task Force on Computer Crime, *Report on Computer Crime*, 1984 A.B.A. SEC. OF CRIM. JUSTICE 19.

10. "Computer matching" involves matching information from massive numbers of computerized personal files to conduct investigations. John Shattuck, *In the Shadow of 1984: National Identification Systems, Computer-Matching, & Privacy in the United States*, 35 HASTINGS L.J. 991, 1001 (1984).

11. Simitis, *supra* note 6, at 715.

12. *See* Graham, *supra* note 5, at 1396.

13. *See* Cornish & Louria, *supra* note 2, at 115. Networks are another computer technology that threatens privacy. Networks link computer terminals, making a service performed by a computer at one place available to a computer user at another place. Branscomb, *supra* note 7, at 1 n.1. Common network functions include inter-departmental electronic mail ("E-mail") and funds-transfer networks such as those connecting automatic teller machines. Networks threaten privacy because they often are not secure and because they are a powerful investigatory tool when coupled with databanks.

Networks often are paired with databanks for computer matching investigations. For example, when a government agency does a criminal investigation of an individual, computer networks are used to collect information on the individual's activities and prior convictions. The agency searches databases by entering, for example, the individual's social security number in the network. When a match is made, the individual's file is sent through the network from its database. Eventually, the agency can create a complete portrait of the individual based on files in several databases. Thus, a network may carry significant amounts of sensitive information.

competitor.[14] In order to discourage such behavior, Alaska needs a comprehensive statute protecting computer privacy.

Regulating computer use, however, involves a delicate compromise. Placing electronic "locks" on data makes computer use more cumbersome and impedes efficient information management. Further, information plays an important role in a modern, democratic society. One commentator identifies information as "the currency of the 'marketplace of ideas,' the prerequisite for political self-determination."[15] If society is overzealous in restricting the free flow of information, the so-called "right to be let alone" turns into an impediment to democratic decision-making.

Privacy is also important to a modern, democratic society, however. Just as "the marketplace of ideas" contributes to democracy, privacy contributes to autonomy, and ensures that individuals need not have every choice exposed by the popular will.[16] Finally, if information is the currency of the "marketplace of ideas," privacy provides value to that currency by making the individual the titleholder of a form of personal property.[17] Only by giving the individual the power to grant *or* refuse access to personal information can he profit from what logically belongs to him.

Alaska law presently does not strike the delicate balance between privacy and the free flow of information; rather, it leaves private information subject to exploitation by third parties.[18] This note proposes a statute aimed at addressing the issue of privacy in the information age. Part II considers privacy protection under current Alaska law. Part III analyzes computer privacy statutes enacted by both the federal government and other Ninth Circuit states. Finally, part IV offers a new computer privacy statute to

---

14. Thomas Whiteside, *Annals of Crime: Dead Souls in the Computer*, NEW YORKER, Aug. 22, 1977, at 57-58.

15. Seth F. Kreimer, *Sunlight, Secrets & Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 6 (1991).

16. Graham, *supra* note 5, at 1406.

17. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 963, 977 (1964).

18. Additionally, the law is insufficient in its protection of more conventional property interests, and any Alaskan computer legislation should protect against the threats computers pose to property as well as privacy. For example, the clever bank employee can slowly divert funds from a number of accounts into his own account with little fear of detection. Loss estimates for insider crime range up to five billion dollars per year. Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1900 (1991).

deal with the current deficiencies in Alaska law and to promote the tradition of strong individualism in Alaska.[19]

II. PRIVACY PROTECTION UNDER ALASKA LAW

Alaska's laws offer little protection for electronically stored data, and few cases have addressed the special privacy implications of widespread computer use. The Alaska Supreme Court, however, has recognized the right to privacy from both state and private intrusions in other contexts.[20] Thus, a general public policy supporting privacy in Alaska can be inferred. It is this policy which provides the theoretical foundation for an Alaskan computer privacy statute.

A. Criminal Penalties

1. *General Criminal Statutes.* The Alaska criminal statutes do not cover most misuses of computer resources. For example, Alaska's general theft statute defines "theft" as obtaining the property of another "with intent to deprive another of [it] or to appropriate [it] to oneself or a third person."[21] As the legislature has defined "property" to include "data or information stored in a computer program, system, or network,"[22] the statute would seem to apply to computer resources and information. The Alaska Supreme Court has ruled that "theft" requires interference with one's possession of property, however.[23] Unlike with other types of property, when information is misappropriated the "owner" retains possession of the information because, in essence, only a copy of the information has been stolen.[24]

---

19. *See* Ravin v. State, 537 P.2d 494, 504 (Alaska 1975) ("[S]tate has traditionally been the home of people who prize their individuality and who have chosen to settle or continue living here in order to achieve a measure of control over their own lifestyles which is now virtually unattainable in many of our sister states.").

20. *See* ALASKA CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); Siggelkow v. State, 731 P.2d 57, 62 (Alaska 1987) ("The right to be free from harassment and constant intrusion into one's daily affairs is enjoyed by all persons." (citing WILLIAM L. PROSSER, THE LAW OF TORTS § 117, at 807-09 (4th ed. 1971))).

21. ALASKA STAT. § 11.46.100(1) (1989).

22. *Id.* § 11.81.900(b)(46) (Supp. 1993).

23. *See* Howard v. State, 583 P.2d 827 (Alaska 1978)(intent to deprive owner of property necessary element of crime); Pulakis v. State, 476 P.2d 474 (Alaska 1970) (possession is the gravamen of larceny offense).

24. *See* Branscomb, *supra* note 7, at 32; Brenda Nelson, Note, *Straining the Capacity of the Common Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299 (1991).

Another Alaska statute provides limited protection against computer misuse. The offense of "theft of services" includes unauthorized use of computer time, systems, networks and programs.[25] While this statute prohibits unauthorized access, it does not protect against additional improper activities. A hacker who misappropriates a corporation's mailing list for illegitimate purposes would be guilty only of no greater crime than an employee who allowed his child to write a term paper on an office terminal. The current statute simply does not reach all of the potentially dangerous results of unauthorized access and theft of services. The misuse that current legislation *does* cover may be of the type more appropriately handled by internal corporate security.

2. *Alaska Computer Statutes.* The Alaska legislature has defined two criminal offenses specifically prohibiting the misuse of computers. The misdemeanor of criminal mischief in the third degree occurs when an unauthorized person "knowingly accesses a computer, computer system, computer program, computer network, or part of a computer system or network."[26] The statute is a good first step, for it recognizes computer abuse as behavior worth prohibiting but does not overestimate the threat posed by computer "spying" that makes no use of stored information.

The second offense, criminal use of a computer, occurs when an unauthorized person knowingly accesses a computer system and "(1) obtains information concerning a person; or (2) introduces false information . . . with the intent to damage or enhance the data record of a person."[27] Criminal use of a computer is a class C felony.[28] The criminal use statute is more interesting for what it does not cover, however, than for what it does. The statute addresses only unauthorized users; authorized users, such as employees of a database owner, could obtain data on an individual, organization or company and then put it to unauthorized uses.

The criminal use statute also may prohibit only the removal of personal data from a computer system, not its copying or misuse. In offenses against property, Alaska defines "obtain" as "to bring about a transfer or a purported transfer of a legal interest in the property . . . or to exert control over property of another."[29] As long as personal information remains stored in its original form in

---

25. ALASKA STAT. § 11.46.200(a)(3) (1989).

26. ALASKA STAT. § 11.46.484(a)(5) (1989). "'[A]ccess' means to instruct, communicate with, store data in, retrieve data from, or otherwise obtain the ability to use the resources of a computer . . . ." *Id.* § 11.46.990(1).

27. *Id.* § 11.46.740.

28. *Id.*

29. ALASKA STAT. § 11.46.990(11)(A) (1989).

the computer system, an unauthorized user may be able to access and use the data without violating the statute. The prohibition against criminal use of a computer appears to ban only limited activities and provides insufficient protection against privacy threats.[30]

B. Civil Remedies.

In *Darling v. Standard Alaska Production Co.*,[31] the Alaska Supreme Court followed the United States Supreme Court's ruling that trade secret laws protect privacy rights.[32] Thus, trade secret law may safeguard certain types of data stored on computers. For information to be considered a trade secret, the Alaska Uniform Trade Secrets Act requires that the information (1) derive independent economic value from not being generally known to the public and (2) be the subject of reasonable efforts to maintain secrecy.[33] Organizations easily could meet the second prong of the test by scrupulously protecting the information stored on computer from disclosure.[34]

The first prong of the test is the more difficult one to satisfy. In order to derive its value from secrecy, the information must not be "readily ascertainable by proper means by [] other persons who can obtain economic value from its disclosure or use."[35] Designs

---

30. One Alaska computer network which has received significant legislative attention is the criminal justice information system. There are specific limits on the use and right of access to the system, and regulations to ensure the security and privacy of the information stored on the system are authorized. *See* ALASKA STAT. § 12.62.010 (1989). The court of appeals recently held that prosecutors may use the network to run background checks on potential jurors, however. Tagala v. State, 812 P.2d 604 (Alaska Ct. App. 1991).

31. 818 P.2d 677 (Alaska 1991).

32. *Id.* at 681 (citing Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 487 (1974)).

33. ALASKA STAT. § 45.50.940(3) (Supp. 1993).

34. In *Darling*, the Alaska Supreme Court denied trade secret protection to a designer of a linked concrete block system. 818 P.2d at 683. In *State Department of Natural Resources v. Arctic Slope Regional Corp.*, however, the court held that data on oil well conditions was a trade secret. 834 P.2d 134, 138 (Alaska 1991). The distinction between the two rulings lies in the extent of the plaintiffs' efforts to protect the information. The plaintiff in *Darling* took no steps to ensure the secrecy of his invention as required by the Uniform Trade Secrets Act. Instead, he presented a seminar on his product before obtaining a patent, and later sought to recover under a theory of unjust enrichment. 818 P.2d at 678-79. The plaintiffs in *Arctic Slope*, on the other hand, sought an injunction to bar initial disclosure of their information. 834 P.2d at 136.

35. ALASKA STAT. § 45.50.940(3)(A) (Supp. 1993).

or formulas fit the secrecy requirement,[36] but personal information contained on customer databanks might not. While a person might be entitled to withhold his address, for example, a competitor easily could discover it from legitimate sources other than the database. Thus, the information would be "readily ascertainable" and not subject to trade secret protection. Furthermore, some personal information stored on databases might not be of any economic value, and that too would disqualify it from protection under trade secret law.

C. The Basis for a New Statute

Additional legislation is needed to protect against threats to individual privacy posed by computers in Alaska. As a basis for a new computer privacy statute, the legislature can look to both the Alaska Constitution and the common law for a general public policy favoring privacy in Alaska. For example, in Article I, section 22 of the Alaska Constitution, the State grants its citizens an express right to privacy.[37] Such privacy protection is broader than that offered by the federal Constitution.[38]

Nevertheless, the right of privacy granted by the Alaska Constitution only protects privacy interests against state action, and thus must by supplemented with a prohibition of private intrusions of privacy. The Alaska Supreme Court has recognized a common law right to privacy.[39] Furthermore, the court has derived a general public policy favoring privacy from the common law and the constitutional provision. In *Luedtke v. Nabors Alaska Drilling Inc.*,[40] the court used this policy to create a privacy right in the employment context. The court asserted that:

> [T]he citizens' right to be protected against unwarranted intrusions into their private lives has been recognized in the law of Alaska. The constitution protects against governmental intrusion . . . and the common law protects against intrusions by other private persons. As a result, there is sufficient evidence to support the conclusion that there exists a public policy protecting

---

36. Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1001-02 (1984).

37. The Alaska Constitution provides: "The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section." ALASKA CONST. art. I, §22.

38. State v. Glass, 583 P.2d 872, 878-79 (Alaska 1978).

39. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1133 (Alaska 1989) ("[T]here exists a common law right to privacy."). This right is based upon the Restatement (Second) of Torts § 652B, which provides that "[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of privacy, if the intrusion would be highly offensive to a reasonable person."

40. 768 P.2d 1123 (Alaska 1989).

> spheres of employment conduct into which employers may not intrude.[41]

This same public policy provides the theoretical foundation for a new computer privacy statute. By enacting such a law, the Alaska legislature would be acting pursuant to a tradition supporting individual privacy in the state.

III. THE FEDERAL AND NINTH CIRCUIT COMPUTER PRIVACY MODELS

Both the federal government and the states of the Ninth Circuit have been quite responsive to the computer threat to privacy. Their statutes may provide a model for an Alaskan statute. Not all of the statutes have been successful, however, and Alaska should be careful not to duplicate the mistakes. Most importantly, none of the statutes provides adequate protection against the threat of insider crime. Alaska has an opportunity to be among the vanguard of computer crime legislation by enacting a standard of care for system operators.

A. Federal Computer Privacy Statutes

The federal government protects computer privacy through four pieces of legislation: the wire fraud statute,[42] the Computer Fraud and Abuse Act,[43] the Electronic Communications Privacy Act[44] and the Computer Security Act.[45] The federal legislation covers only threats to national interests, however, and thus does not provide sufficiently comprehensive protection for Alaskan computer privacy concerns. While the Alaska legislature should be careful not to duplicate federal law needlessly, certain interests addressed by the federal legislation should be incorporated into an Alaskan computer privacy statute.

1. *The Federal Wire Fraud Statute.* The federal wire fraud statute addresses any person who uses wire communications to perpetrate a scheme to defraud.[46] Courts have construed the legislation to include computer offenses, so long as the fraud is perpetrated either over interstate lines or lines involved in foreign commerce.[47] Prosecutors have used the statute to convict persons

---

41. *Id.* at 1133.
42. 18 U.S.C. § 1343 (Supp. IV 1993).
43. *Id.* § 1030 (1988 & Supp. 1993).
44. *Id.* §§ 2510-2521 (1988).
45. 40 U.S.C. § 759 (1988 & Supp. IV 1993).
46. 18 U.S.C. § 1343 (Supp. IV 1993).
47. Jerome Y. Roaché, *Computer Crime Deterrence*, 13 AM. J. CRIM. L. 391, 393-94 (1986).

who deleted and added information to individuals' computerized credit files,[48] airline employees who kept the proceeds from falsified computerized ticket sales[49] and an ex-employee who retrieved information from his former employer's computer system.[50] Because of the simplicity of the statute, fraud easily could be found in cases of theft of computer time, valuable information or financial information. The legislation also is sufficiently flexible to reach situations involving destruction of computer resources.

The simplicity of the wiretap statute also results in limitations, however. The statute focuses on fraud instead of privacy, and thus fails to criminalize "snooping." The lack of focus on privacy concerns also means the statute does not make vital distinctions between actions such as the theft of a valuable corporate mailing list and an employee's use of the company computer to do personal work. It also fails to address improper dissemination of computerized information by insiders. Moreover, the statute only covers communications on wires used in interstate commerce.[51] Thus, the federal wire fraud statute provides a good beginning for state legislation protecting computer privacy interests, but does not cover many of the activities that should be included in an Alaskan statute.

2. *The Computer Fraud and Abuse Act.* The Computer Fraud and Abuse Act of 1984 ("CFAA"),[52] part of the Crime Control Act, was the first federal statute to address computer crime.[53] Because it applies only to computer crime affecting a federal interest, most threats to computer privacy are not affected by the CFAA.[54] Still, the CFAA provides some guidance for a

---

48. United States v. Alston, 609 F.2d 531 (D.C. Cir. 1979).

49. United States v. Giovengo, 637 F.2d 941 (3d Cir. 1980).

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

51. Data storage or other computer functions that do not involve electronic transmissions affecting interstate or foreign commerce are not within Congress' powers. *See* U.S. CONST. art. I, § 8, cl. 3.

52. 18 U.S.C. § 1030 (1986).

53. Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 455 (1990); Roaché, *supra* note 47, at 397.

54. 18 U.S.C. § 1030. In light of several policy considerations, Congress decided to limit the scope of federal computer crime legislation. Griffith, *supra* note 53, at 484. Congress wanted state and local legislators to handle most offenses of that nature. *Id.* Congress also found that most computer crime was committed by insiders and not the well-publicized teenage hacker. *Id.* at 486. But, in the 1986 amendment to the CFAA, Congress precluded liability in purely insider cases. (The Senate Judiciary Committee defined "purely insider cases" as those involving unauthorized access to intra-department, as opposed to in-

proposed Alaskan computer privacy statute.

First, the CFAA differentiates between types of undesirable activity and the penalties appropriate for each. For example, the CFAA distinguishes between simple trespass[55] and trespass with the intent to defraud.[56] One who accesses a computer without authorization but with no intent to use stored information should not be punished as severely as one who does with an intent to defraud.[57]

Second, Congress made clear that information did not have to be removed from a databank in order for a crime to occur. The legislative history of the CFAA explains that "obtaining" financial information does not require gaining physical possession of it, as theft statutes do, but includes mere observation (i.e., "snooping.") as well.[58] Thus, the statute avoids the difficulties that would be encountered by an Alaska prosecutor attempting to apply Alaska's theft statute to a perpetrator who copied, but did not remove, information from a computerized database.

Third, the CFAA takes into account the unique nature of computer technology, as Congress carefully crafted the statutory language to ensure that only malicious computer operators would be prosecuted. The 1986 amendments changed the *mens rea* from "knowingly" to "intentionally" for computer fraud that results in obtaining financial information. "Knowledge" is often an inappropriate *mens rea* standard for crimes involving computers because it requires that a result be practically certain, but does not require the desire to achieve that result.[59] A computer operator might stumble inadvertently upon financial data by accidentally entering a data retrieval command. Once the appropriate command is entered erroneously, the retrieval of data is a virtual certainty despite the operator's lack of desire to retrieve the data. Thus, a

---

ter-department, resources. S. REP. NO. 432, 99th Cong., 2d Sess. (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2485. This alleviated concerns that the statute could be used against whistleblowers. *Id.*) In passing the 1986 amendment, Congress reaffirmed its initial skepticism about the need for a broad federal law: "The [Senate Judiciary] Committee . . . prefers . . . to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature." S. REP. NO. 432, at 2482; *see also* 18 U.S.C. § 1030(e)(2) (1988) (defining a "federal interest computer").

55. 18 U.S.C. § 1030(a)(3) (1988).

56. *Id.* § 1030(a)(4) (1988).

57. S. REP. NO. 432 at 2487.

58. *Id.* at 2484.

59. *Id.*

careless but innocent computer operator could be penalized under a "knowledge" standard.

The CFAA is not without its weaknesses, however. For example, it provides no civil remedies,[60] and protects only a narrow range of computers and information. An Alaskan statute should include a civil remedies provision for a broad range of offenses while incorporating the strengths of the federal statute.

3. *The Electronic Communications Privacy Act.* As the name suggests, the Electronic Communications Privacy Act ("ECPA")[61] safeguards the privacy of communications made by electronic means. The ECPA protects electronically transmitted data in a manner similar to the federal wire fraud statute.[62] Many computer operations involving transmission of data, such as networking and electronic mail, are especially sensitive to privacy threats. Under the ECPA, computer hackers may neither intentionally intercept electronic communications[63] nor access stored communications.[64] The ECPA also provides some protection for databases, since they can be characterized as communications in storage at remote locations.[65]

The ECPA is not without its limitations, however. Many crucial terms such as "computer" and "access" are left undefined.[66] Additionally, like the CFAA, the ECPA does not contain a civil remedies provision. Finally, the ECPA is concerned only with eavesdropping on electronic communications.[67] Destructive activities such as releasing viruses or unauthorized use of computer resources are not prohibited by this act. An Alaskan statute should close the gaps in the ECPA to provide better privacy protection as well as improved safeguarding of computer resources.

---

60. *Cf.* Darryl C. Wilson, *Viewing Computer Crime: Where Does the Systems Error Really Exist?*, 11 COMPUTER/L.J. 265, 276 (1991) ("The most troubling aspect [of Illinois' computer statute] is the complete removal of the civil remedies section.").

61. 18 U.S.C. §§ 2510-2521 (1988).

62. Robert W. Kastenmeier et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 727.

63. 18 U.S.C. § 2511(1) (1988).

64. *Id.* § 2701.

65. Kastenmeier et al., *supra* note 62, at 728.

66. *See* 18 U.S.C. § 2510 (1988) (defining terms used in the ECPA).

67. The ECPA defines "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication . . . ." *Id.* § 2510(4) (Supp. 1993).

4. *The Computer Security Act.* Congress passed the Computer Security Act ("CSA")[68] to "improv[e] the security and privacy of sensitive information in Federal computer systems."[69] This statement of purpose illustrates both the breadth and the limitations of the statute, as it expresses broad concern with computer privacy but limits its reach to sensitive information stored on *federal* computers.[70] Further, the protection afforded to "sensitive information" only extends to data that could adversely affect the national interest or that is protected by the Privacy Act.[71] Most computer-stored information does not meet such specifications.

The federal government's concern with privacy is admirable and should be considered when developing an Alaskan computer privacy statute. Alaska, however, should extend protection much further than the CSA. State legislation should protect more types of computer systems and information, as well as provide a private cause of action.[72]

5. *Lessons from Federal Legislation.* The CFAA provides the most useful aspects for an Alaska criminal computer use statute to adopt. Its differentiation between types of culpable conduct and threatened interests is crucial to effective and fair legislation regarding improper computer activities. Congress carefully defined the *mens rea* and *actus reus* elements of the crime to fit the special difficulties posed by computer technology. The result is a statute that is a good first step toward combatting computer abuses.

Overall, the federal statutes are effective in limited areas, but they were not passed as a cohesive effort to fight computer crime. The result is a piecemeal treatment of the threat to computer resources and personal privacy. None of the statutes provides a standard of care for computer operators, thus leaving insiders the freedom to act negligently in the management of private informa-

---

68. 40 U.S.C. § 759 (1988 & Supp. IV 1993).

69. Computer Security Act of 1987, Pub. L. No. 100-235, § 2(a), 101 Stat. 1724 (1988).

70. State and local governments, private individuals and corporations own many more computers than does the federal government. *Compare* S. REP. NO. 432, 99th Cong., 2d Sess. 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2479 (reporting that by 1990, the Federal Government was expected to be using 250,000 to 500,000 computers) *with* FINAL REPORT: SMALL BUSINESS COMPUTER SECURITY EDUCATION AND ADVISORY COUNCIL, *published in* 7 COMPUTER L. REP. 525 (1988) (reporting that by 1987, 11 million small businesses used computers).

71. Computer Security Act of 1987, Pub. L. No. 100-235, § 20(d)(4), 101 Stat. 1727 (1988).

72. *See* Wilson, *supra* note 60, at 276.

tion stored in computers. Additionally, the statutes are limited to federal interests, leaving interests unique to Alaskan citizens unprotected. A cohesive and comprehensive statute would better serve the broad privacy interests recognized under Alaska law.[73]

B. Computer Privacy Statutes of Ninth Circuit States

Other states in the Ninth Circuit have passed laws dealing with the problem of computer crime. Comprehensive state statutes such as California's could serve as the model for Alaska's new legislation, while others should serve as examples of potential pitfalls.

1. *California.* Motivated by a desire to expand the protection afforded by previous computer tampering legislation,[74] the California legislature passed one of the most comprehensive computer crime laws in the nation.[75] Appropriately, the statute begins with the declaration that "protection of the integrity of all types and forms of lawfully created . . . computer systems . . . is vital to the protection of the privacy of individuals."[76] Prohibited activities under the California statute include introducing a virus,[77] trafficking in passwords,[78] using computer time without authorization[79] and making use of stored data without permission.[80] Such specificity ensures that no criminal will find refuge in loopholes contained in more generally drafted statutes. Attempting to deal with all computer crime through a general computer fraud statute, as some states have done,[81] is analogous to attempting to include armed robbery, burglary, pick-pocketing, and shoplifting in a single, general theft statute. Although the crimes have much in common, their differences require distinct treatment.

The California statute also contains a provision regarding forfeiture of computer equipment[82] as well as one prohibiting the

---

73. See part II.C. for a discussion of the Alaska public policy favoring broad privacy rights.

74. CAL. PENAL CODE § 502(a) (West 1988).

75. Camille Cardoni Marion, Note, *Computer Viruses and the Law*, 93 DICK. L. REV. 625, 632 (1989).

76. CAL. PENAL CODE § 502(a) (West 1988).

77. *Id.* § 502(c)(8) (West Supp. 1994). See *supra* note 7 for a detailed explanation of a "virus."

78. *Id.* § 502(c)(6) (West 1988).

79. *Id.* § 502(c)(3).

80. *Id.* § 502(c)(2).

81. *E.g.*, ARIZ. REV. STAT. ANN. § 13-2316(A) (1989) (defining "computer fraud" as "accessing, altering, damaging or destroying without authorization any computer, computer system, [or] computer network . . . .").

82. CAL. PENAL CODE § 502(g) (West Supp. 1994). *See also id.* § 502.01(a)(1)

use of computers after conviction.[83] Such provisions are essential to the statute's effectiveness because they serve as an obstacle to those who might attempt to repeat their criminal conduct. Also, such statutes match the punishment with the crime by depriving the criminal of the instrumentality of his offense, much like existing statutes prohibit convicted felons from owning a gun. Finally, the California statute contains a civil remedies provision[84] and covers situations where the perpetrator was in another jurisdiction when he accessed California computers.[85] While some of the provisions may be unnecessary or duplicative of federal efforts, the California statute is comprehensive in its protection of computer privacy and resources.

Still, there is room for improvement. Despite its emphasis on privacy, the California statute seems crafted to protect the interests of business, rather than those of the individual. For example, the statute pays too little attention to the threats that insiders pose to individual privacy. Employees whose access or use of computer systems exceeds the scope of their authority cannot be prosecuted unless their activities damage the system or they use more than $100 worth of computer services.[86] Such a threshold of protection might be adequate to protect commercial interests, which can easily be measured by a dollar value and are unlikely to be significant below the $100 mark; however, the standard fails to protect individuals against those who might invade and misuse personal data records without causing any damage to the system. Such an emphasis on businesses' privacy is repeated throughout the statute. The California statute lacks both a standard of care for system operators (to accompany the provision for civil remedies) and specific protection for whistleblowing. A standard of care would require system operators to forgo installing sub-standard security devices as a means of cutting costs.

2. *Other Ninth Circuit States.* Computer crime statutes of other Ninth Circuit states are not as comprehensive as California's. Most of these other states define two types of computer crime: schemes to defraud through use of a computer, which is usually a

---

(defines property subject to forfeiture); *id.* § 502.01(e) (property subject to forfeiture includes parental property of a minor convicted of computer crime).

83. *Id.* § 1203.047 (employment connected with computer is forbidden while on probation for violation of § 502 or § 502.7); *id.* § 2702 (no access to prison computer if convicted of computer crime).

84. *Id.* § 502(e) (West 1989 & Supp. 1994).

85. *Id.* § 502(j) (West 1994).

86. *Id.* § 502(h)(2) (West 1989 & Supp. 1994).

felony,[87] and unauthorized use of computer resources, which is usually a misdemeanor.[88] Such statutes suffer from the limitations of general statutes discussed above.[89] For example, in Washington, a police officer who obtained pictures and biographies of female University of Washington students for his personal use avoided conviction under the state's computer trespass statute because it prohibited only unauthorized *access to*, not unauthorized *use of*, computerized information.[90] The defendant was authorized to use the state licensing bureau computers which stored the students' personal information because he was a police officer. Because the police officer's actions were neither an unauthorized use nor a scheme to defraud, he would have escaped punishment under most other states' computer privacy statutes as well.[91]

Nevada has made an attempt to provide greater protection to the interests threatened by computer technology. Nevada's computer crime statute contains a unique provision under which district attorneys can seek an injunction to prevent the occurrence of computer crimes without demonstrating proof of actual damage and without precluding prosecution.[92] Some scholars have argued that expedited methods of investigation and prevention are necessary because computer functions and computer crimes can occur in a split-second.[93]

Like California, however, Nevada neglects the threat of insider computer crime. The Nevada statute presumes an employee has the authority to access and use any computer system or stored data owned or operated by his employer.[94] Again, such lack of concern for the threat "authorized" users pose leaves the individual with insufficient privacy protection. Most individuals agree to provide personal information to companies and governments because the benefits gained through social security numbers, censuses, etc., are worth the price of diminished privacy. The cornerstone of that agreement, however, is the individual's assumption that the information will not be used for purposes other than those for

---

87. *E.g.*, IDAHO CODE § 18-2202(1) (1987); MONT. CODE ANN. § 45-6-311(1)-(c) (1989); OR. REV. STAT. § 164.377(2)(a) (1990).

88. *E.g.*, IDAHO CODE § 18-2202(3) (1987); MONT. CODE ANN. § 45-6-311(1)-(a) (1989); OR. REV. STAT. § 164.377(4) (1990).

89. *Supra* text accompanying note 81.

90. State v. Olson, 735 P.2d 1362, 1364 (Wash. Ct. App. 1987).

91. Alaska's current criminal use of a computer statute does not prohibit such activities either. *See supra* text accompanying notes 26-30.

92. NEV. REV. STAT. § 205.491 (1992).

93. Diana Wilkes, *The Wiretap Statute: A Haven for Hackers*, 31 JURIMETRICS J. 415, 418 (1991).

94. NEV. REV. STAT. § 205.485 (1992).

which it was collected.[95] Unscrupulous businesses might not adhere to such an implicit agreement, and courts faced with such conflicts often find that the individual's initial consent to the collection of personal information justifies its further use.[96] An Alaskan statute should remedy these abuses by limiting the use of personal information to those specifically condoned by the subject of such information.

3. *Lessons from Ninth Circuit States' Legislation.* State legislation is important in the area of computer abuse. It ensures that local, as well as federal, interests are addressed. An effective state statute should cover a variety of computer abuses and tailor its language to fit the unique characteristics of computer technology. The California statute provides the best model for a state criminal computer use statute. Its comprehensiveness and attention to the types of improper conduct bring a wide variety of computer abuses within its scope. The result is an excellent model for how computer abuses should be targeted in Alaska.

All of the state statutes, however, suffer from an insufficient emphasis on the privacy of the individual. Like the federal statutes, none of the state legislation provides a standard of care for computer operators. Moreover, none ensures that the use of personal information is limited to the specific purposes for which it was collected. The Alaskan statute should incorporate provisions protecting against insider crime in order to provide its citizens with the best protection of privacy rights available.

IV. THE PROPOSAL TO PROTECT COMPUTER PRIVACY IN ALASKA

A. The Need for New Legislation

American philosopher John Stuart Mill argued that punishment is justified only when it is designed to prevent harm to others.[97] Thus, the pertinent issue is whether society is so harmed by computer hackers, who often are talented teenage pranksters, that it should impose criminal liability upon them as though they were common thieves. This question must be answered in the affirmative. While stolen goods often are replaceable, stolen privacy is not. Unlike material goods, privacy is not insurable, and once personal information is made public, courts cannot order the

95. Bloustein, *supra* note 17, at 999.

96. Kreimer, *supra* note 15, at 110; *see* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 419 (1960).

97. Nelson, *supra* note 24, at 319.

publicizers to forget or retrieve the information they have acquired improperly.

Providing criminal sanctions for misuse of computerized information is a relatively new idea. According to one commentator: "Penal law has always protected property and, in some instances, has also recognized the need to protect secret information . . . . The integration of the two, however, and the protection of confidential information as a type of property is a relatively new idea in the criminal realm."[98] States have resisted the imposition of criminal law on computer misuse in part because they see such sanctions as too severe for the type of computer-related misconduct society seeks to control. In light of the deeply-rooted public policy in Alaska favoring individual privacy, however, criminal penalties for computer intruders are justified.

Over seventy-seven percent of computer users polled by the American Bar Association support adoption of state computer crime statutes.[99] Although it has been argued that only the common law can provide the necessary flexibility to deal with rapidly changing technology,[100] a carefully designed statute could provide the requisite flexibility, as well as extensive enforcement mechanisms.[101] This type of legislation could be further supplemented by a civil tort of unauthorized dissemination of computerized information. Such a comprehensive privacy protection scheme would provide misdemeanor sanctions when a felony would be unfairly harsh[102] and civil remedies when the victim should be compensated for financial losses.

B. The Proposed Legislation

1. *Definitions and Scope.* The statute proposed by this note begins with detailed definitions of important terms.[103] Such definitions are necessary because they ensure that all culpable conduct is covered,[104] allow gradations in punishment and clarify

---

98. Eli Lederman, *Criminal Liability for Breach of Confidential Commercial Information*, 38 EMORY L.J. 921, 929 (1989).

99. A.B.A. Task Force on Computer Crime, *supra* note 9, at 26.

100. Graham, *supra* note 5, at 1426.

101. Note, *supra* note 18, at 1915.

102. *Cf.* Marion, *supra* note 75, at 633 (in cases when interference with computer systems does no more than inconvenience legitimate users, criminal penalties may not be appropriate).

103. See *infra* Appendix § A.

104. For example, since the federal wire fraud statue covers only transmissions made on interstate wires, it does not reach interceptions of computer resources or data via microwaves or other electronic devices. Diana Smith, Note, *Who is Calling Your Computer Next? Hacker!*, 8 CRIM. JUST. J. 89, 99 (1985). The

technical computer language that may be unclear to the layman. The statute also has a jurisdictional hook similar to that in the California statute.[105] This would allow Alaska to prosecute computer operators in other jurisdictions who commit crimes against computer resources in Alaska. Additionally, the proposed legislation has a provision for injunctions[106] similar to that found in Nevada's statute.[107] Such an early intervention technique provides greater protection against the danger the lightning speed of computerized crime poses to privacy rights.

2. *Criminal Provisions.* The proposed statute recognizes four types of computer crime: fraud, intrusion, criminal use and vandalism.[108] Computer fraud reaches activities that utilize computers to cause financial losses or gains, including such activities as illegally transferring money, altering credit records and deliberately destroying computer programs.[109] Intrusion occurs when a user intentionally gains access to and makes use of any information stored on computer systems without the system operator's permission, or makes use of personal information stored on computer systems without the subject's permission.[110] Such dual protection guards against threats to business and individual privacy. The statute protects individual privacy in another unique way: computer intrusion also occurs if a system operator knowingly fails to provide a reasonable level of security for systems storing personal information.[111] Such provisions can help to assure Alaskans that their privacy will be protected by organizations even after personal information has been surrendered to the organizations' computers.

Criminal use of a computer includes intentional, unauthorized use of computer time and unauthorized facilitation of access.[112] Vandalism covers disruption of computer services and the introduction of viruses.[113] Fraud and intrusion are felonies, while criminal

---

proposed Alaska statute has a catch-all clause in the definition of "access" that reaches unspecified means of "otherwise gain[ing] entry to the resources" of computers. See *infra* Appendix § A(1).

105. *See infra* Appendix § D.

106. *See infra* Appendix § E.

107. *See supra* text accompanying note 92.

108. See *infra* Appendix § B; *cf.* Tunick, *supra* note 4, at 326-28 (recognizing financial crime, information crime, theft of services and vandalism as common computer crimes).

109. See *infra* Appendix § B(a)(1).

110. *See infra* Appendix § B(b)(1).

111. *See infra* Appendix § B(b)(2).

112. See *infra* Appendix § B(c)(1).

113. See *infra* Appendix § B(d)(1).

use and vandalism are misdemeanors.[114] Thus, the proposed statute reserves higher penalties for those who actually make use of the information stored on computers. The proposed statute also contains a computer equipment forfeiture provision,[115] impeding those who have misused their computer skills from returning to their improper activities.

Unlike other existing statutes, the proposed legislation makes insiders as well as outsiders liable for computer crime. It focuses not on the authorization for access but instead on the authorization for activities engaged in after such access.[116] Thus, the statute covers wrongdoers regardless of whether their access is authorized. Further, the proposed law protects whistleblowers with an exception for unauthorized users who appropriate computer data in order to report corporate crimes to the authorities.[117]

The statute covers both misusers of information stored on computers and mere "snoopers." Computer fraud and intrusion focus on those who misuse information.[118] Accordingly, these crimes define improper conduct with terms such as "alter," "damage," "take," "copy" or "make use." The statute does not contain the deficiency, common to statutes modeled after theft statutes, of requiring the actor to obtain possession of the information before a crime can occur. Criminal use and vandalism require improper use, not improper change in locale, of computerized information and resources.[119] Thus, the *actus reus* of these crimes are activities such as facilitation of access and disruption of services. Finally, the *mens rea* of all of the crimes is intent. The statute does not use

---

114. *Compare infra* Appendix §§ B(a)(2) & (b)(3) *with* Appendix §§ B(c)(2) & (d)(2).

115. See *Infra* Appendix § B(e).

116. *See, e.g., infra* Appendix § B(a)(1)(A) ("without permission" modifies alters, not accesses); Appendix § B (b)(1)(A) ("without permission" modifies takes, not accesses); Appendix § B (c)(1)(A) ("without permission" modifies uses).

117. *See infra* Appendix § B(f). Publicly employed whistleblowers are protected from termination of employment by statute, ALASKA STAT. § 39.90.100 (Supp. 1993), and privately employed whistleblowers are protected by common law. *See* Knight v. American Guard & Alert, Inc., 714 P.2d 788, 792 (Alaska 1986). The current law does not provide any protection from criminal prosecution, however. In the recent Alyeska Pipeline Service Company scandal, employee Bob Scott leaked information on environmental violations to oil industry critic Charles Hamel, who then passed the information on to Congress. Kim Fararo, *Alyeska Hearing Ends; Ruling Six Months Away*, ANCHORAGE DAILY NEWS, June 5, 1992, at B1. Only the deficiencies in the current law prevent Scott's prosecution; there is no statutory exemption for unauthorized access to computers for the purpose of reporting wrongdoings.

118. *See infra* Appendix §§ B(a) & (b).

119. *See infra* Appendix §§ B(c) & (d).

the less appropriate mental state of knowledge, which, because of the unique nature of computers, would include operators who access restricted computer resources without any desire to do so or to cause harm.

3. *Civil Provisions.* In addition to providing a cause of action for the misconduct of system operators and individuals, the civil provision of the proposed statute imposes a duty of reasonable care on the system manager.[120] "Reasonable care" is defined as including standard industry security measures (such as purging old files and data), maintaining adequate security systems, and restricting uses of collected personal information.[121] The imposition of a standard of care on computer system managers is unique to the proposed legislation. The provision is designed specifically to impress upon the collectors and users of personal information the importance of guarding personal privacy. Such a standard of care makes the proposed Alaskan statute stricter than any existing statute.

In order for the Alaska legislature to combat computer abuses effectively, however, the civil statute must be accompanied by a criminal statute. Although tort law is useful when a hacker misappropriates computerized data of clear financial value, there usually is little measurable pecuniary loss on which to predicate damages in situations where personal information is misappropriated.[122] Furthermore, the typical hacker often is a student who has little money with which to pay a civil judgment; a civil remedy alone would not provide a sufficient deterrent to his dangerous conduct.[123] Only a comprehensive legislative initiative that includes penal sanctions would ensure protection for the property and the privacy of an individual in an information society.

---

120. See *infra* Appendix § C(2). Such a provision addresses the difficulties arising with teenage hackers, who might not have the resources to compensate victims. *See* Massingale & Borthick, *supra* note 9, at 174.

121. See *infra* Appendix § A(8).

122. *Compare* Graham, *supra* note 5, at 1431-32 ("[C]ourts commonly allow the granting of general damages in dignitary tort cases . . . even though no physical or economic harm is shown.") *with* Massingale & Borthick, *supra* note 9, at 181 (courts deny damages for purely economic loss in negligence claims).

123. Marion, *supra* note 75, at 634. *See also* Roaché, *supra* note 47, at 392 ("One of the major purposes of penal legislation is to prevent crime. Penal legislation informs a potential violator that the act he is contemplating is illegal and punishable.").

V. CONCLUSION

Almost anything of value, from financial accounts to personal information, is reflected in some record on a computer. Leaving Alaska's computers unprotected is like leaving the bank vault unlocked. The state's current laws are not sufficient to protect against the unique threat computer technology presents to privacy concerns. The legislature should respond to this threat by passing a bill aimed specifically at the dangers of computer crime. Both the federal computer privacy statutes and the California computer crime statute provide good models for Alaskan legislation, but no statute provides the standard of care for system operators that is necessary to prevent insiders from misusing their ability to access broad computer resources and information. Alaska, in keeping with its tradition as reflected in other contexts, should meet the challenge of providing its citizens with the most stringent privacy protection practical.

Carol R. Williams

APPENDIX: PROPOSED LEGISLATION

Section A. Definitions.

In this chapter, unless the context requires otherwise,

(1) "access" means to instruct, communicate with, store data in, retrieve data from, or otherwise gain entry to the resources of a computer, computer system, computer network, or any part of a computer system or network;

(2) "computer" means an electronic device that performs logical, arithmetic, and memory functions by the manipulation of electronic, optical, or magnetic impulses, and includes all input, output, processing, storage, computer software, and communications facilities that are connected or related to a computer;

(3) "computer network" means an interconnection, including by microwave or other means of electronic or optical communication, of two or more computer systems, or between computers and remote terminals;

(4) "computer program" means an ordered set of instructions or statements, and related information that, when automatically executed in actual or modified form in a computer system, causes it to perform specified functions;

(5) "computer system" means a set of related computer equipment, devices and software;

(6) "computer services" includes, but is not limited to, computer time, data processing, or storage functions, or other uses of a computer, computer system, or computer network;

(7) "data" includes a representation of information, knowledge, facts, concepts, or instructions, that is being prepared or has been prepared in a formalized manner and is used or intended for use in a computer, computer system, or computer network. Data may be in storage media, stored in the memory of a computer or in transit or presented on a display device;

(8) "reasonable level of protection of privacy of personal information" means computer security measures generally in use in the relevant industry, and includes, but is not limited to, security devices such as passwords, deleting expired accounts, and using personal information only in the manner authorized by the subject of such information;

(9) "without permission" means without the permission of the owner or operator of any data, computer, computer system, or computer network, unless otherwise indicated;

(10) "computer contaminant" means any set of computer instructions that are designed to modify, damage, destroy, record or transmit information within a computer, computer system, or computer network, without the intent or permission of the owner

of the information. It includes, but is not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some fashion usurp the normal operation of the computer, computer system, or computer network.

Section B. Computer Crimes.

Subsection (a). Computer Fraud.

(1) A person commits computer fraud if he commits any of the following acts:

(A) intentionally accesses and without permission alters, damages, deletes or destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (i) devise or execute any scheme or artifice to defraud, deceive, or extort, or (ii) wrongfully control or obtain money, property or data; or

(B) intentionally accesses and without permission adds, alters, damages, deletes, or destroys any credit record of an individual or institution, or any computer software, or computer programs, which reside or exist internal or external to a computer, computer system, or computer network;

(2) Criminal computer fraud is a class C felony.

Subsection (b). Computer Intrusion.

(1) A person commits computer intrusion if he commits any of the following acts:

(A) intentionally accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network; or

(B) intentionally accesses and without the person's permission takes, copies, or makes use of any information concerning a person from a computer, computer system, computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;

(2) the owner or operator of a computer, computer system, or computer network commits computer intrusion if he knowingly fails to provide a reasonable level of protection of privacy of personal information;

(3) Criminal computer intrusion is a class C felony.

Subsection (c). Criminal Use of a Computer.

(1) A person commits criminal use of a computer if he commits any of the following acts:

(A) intentionally and without permission uses or causes to be used computer services; or

(B) intentionally and without permission provides or assists in providing a means of accessing a computer, computer system or computer network;

(2) Criminal use of a computer is class A misdemeanor.

Subsection (d). Computer Vandalism.

(1) A person commits criminal computer vandalism if he commits any of the following acts:

(A) intentionally and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network; or

(B) intentionally introduces any computer contaminant into any computer, computer system, or computer network;

(2) Criminal computer vandalism is a class A misdemeanor.

Subsection (e). Forfeiture.

Any computer, computer system, computer network, or any software or data, owned by the defendant, which is used during the commission of any offense described in this section shall be subject to forfeiture.

Subsection (f). Protection for Whistleblowers.

Subsections (b) and (c) do not apply to any person to the extent that he accesses his employer's computer system, computer network, computer program, or data for the purpose of reporting, exposing, or investigating illegal activities.

Section C. Civil Remedies.

In addition to any other civil remedy available,

(1) the owner or lessee of the computer, computer system, computer network, computer program, or data may bring a civil action against any person convicted under this section for compensatory damages, including any expenditure reasonably related and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged or deleted by the access;

(2) the provider or subject of personal information which resides or exists internal or external to a computer, computer system, or computer network may bring a civil action against any person convicted under this section, or against any computer, computer system, or computer network owner or operator who fails in his duty to provide a reasonable level of protection of the privacy of personal information.

Section D. Jurisdiction.

For purposes of bringing a civil or criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction.

Section E. Injunction.

If it appears that a person has engaged in or is about to engage in any conduct which violates section B of this statute, the attorney general or appropriate district attorney may file an injunction in any court of competent jurisdiction to prevent the continuation of that conduct. The injunction may be issued without proof of actual damage sustained by any person, and such issuance does not preclude the criminal prosecution and punishment of a violator.