CRIMINAL INVASION OF PRIVACY: A SURVEY OF COMPUTER CRIMES

Jordan M. Blanke*

ABSTRACT: Computers, databases, and the Internet have made personal information readily available. All states have enacted criminal laws to protect against abuses of accessing or using such data. This article traces the history of privacy as it pertains to personal information and explores the criminal laws against invasion of privacy.

CITATION: Jordan M. Blanke, Criminal Invasion of Privacy: A Survey of Computer Crimes, 41 Jurimetrics J. 443–463 (2001).

With the click of a mouse, a sophisticated computer user can gather vast amounts of information about almost any topic. For years computers have provided effective means for collecting and storing data. The combination of more powerful computers, the World Wide Web, and large databases has dramatically changed the quantity and quality of data that may be readily available to even a novice user. Some of these data include personal and private information. As is always the case when technology produces dramatic changes, the law must change to keep pace with these advances. When new abuses arise, new remedies and sanctions inevitably follow.

This pattern is emerging with respect to online data protection and online privacy. Part I of this Article discusses the creation and development of the right to privacy and the tort of invasion of privacy. Part II examines computer crime legislation and statutes that criminalize invasion of privacy.

---

*Jordan M. Blanke is Professor of Computer Information Systems and Law, Stetson School of Business and Economics, Mercer University, Atlanta, Georgia.

I. THE RIGHT TO PRIVACY

A. Common Law

The recognition of a broad right to privacy begins with the famous 1890 article by Samuel Warren and Louis Brandeis espousing the creation of the tort of invasion of privacy.[1] Warren and Brandeis discussed cases decided on such grounds as defamation, loss of property rights, breach of implied contract, and breach of confidence. They reasoned that these decisions really spoke of, and should have been decided upon, a right to privacy. Borrowing a phrase from a commentator of the day, they argued that it was time for the law to recognize the right "to be let alone."[2]

During the next fifteen years or so, several cases addressed the idea of a civil remedy for invasion of privacy. All involved an appropriation of name or likeness, usually for advertising or promotional purposes. The first cases to consider the Warren-Brandeis theory rejected it.[3] In 1905, however, the Supreme Court of Georgia fervently embraced the notion of a right to privacy in *Pavesich v. New England Life Insurance Co.*[4] The court ruled in favor of a man whose picture had been used to sell life insurance without his permission. The court invoked natural law and constitutional protection against unreasonable searches and seizures to hold that the state and federal constitutions guaranteed the right to privacy.[5]

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). The impetus for the article came from Warren, a successful Boston businessman, a member of the social elite, and a former law school classmate of Brandeis. Warren was upset with what he felt was excessive and obtrusive newspaper coverage of his daughter's wedding. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383–84 (1960).

2. THOMAS MCINTYRE COOLEY, A TREATISE ON THE LAW OF TORTS 29 (2d ed. 1888), *quoted in* Warren & Brandeis, *supra* note 1, at 195; Prosser, *supra* note 1, at 389.

3. In 1899, the Supreme Court of Michigan rejected the privacy claim of a well-known deceased politician whose name was used to sell a cigar. In *Atkinson v. John E. Doherty & Co.*, 80 N.W. 285 (Mich. 1899), the court insisted that only those rights based on sound and recognized principles of property were cognizable. In 1902, the New York Court of Appeals rejected a claim by a woman whose picture was used to advertise flour. Roberson v. Rochester Folding Box Co., 64 N.E. 442 (N.Y. 1902). In a 4-3 decision, the majority declared that a right to privacy did not exist and that there was no remedy against such behavior. *See id.* at 448. The court stated that there was no precedent for protecting against an invasion of privacy and feared the vast amount of litigation that might ensue if it granted such protection. *Id.* at 443. In response to a public outcry, New York enacted legislation making it a misdemeanor and a tort to use a name or picture for commercial purposes without written consent of the individual. *See* Prosser, *supra* note 1, at 385.

4. 50 S.E. 68 (Ga. 1905).

5. The court quoted approvingly the dissenting opinion in *Roberson*, which argued that the common law provides an "absolute right to be let alone." *Id.* at 78 (*quoting* COOLEY, *supra* note 2, at 29). Modern opinions in Georgia proudly recite the fact that the right to privacy "was birthed by this court." Cox Broad. Corp. v. Cohn, 200 S.E.2d 127, 130 (Ga. 1973), *rev'd on other grounds*, 420 U.S. 469 (1975). The Supreme Court of Georgia observed recently "the 'right to be let alone' guaranteed by the Georgia Constitution is far more extensive than the right of privacy protected by the U.S. Constitution." Powell v. Georgia, 510 S.E.2d 18, 22 (Ga. 1998). For a discussion of state constitutions that specifically provide for the right of privacy, see *infra* notes 23–44 and accompanying text.

Over the next several decades, state after state considered the tort of invasion of privacy. In another influential law review article in 1960, Professor William Prosser[6] outlined four forms of invasion of privacy: (1) intrusion upon plaintiff's seclusion or solitude, or into his private affairs; (2) public disclosure of embarrassing private facts about the plaintiff; (3) publicity that places the plaintiff in a false light in the public eye; and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[7] Prosser stated that an overwhelming majority of the states had recognized, in some form or another, the right to privacy.[8] Today all but two states, North Dakota and Wyoming, have adopted some form of the tort of invasion of privacy.[9] Most have adopted all four prongs of the definition.[10]

B. Federal Constitution

The United States Constitution does not specifically refer to a right to privacy, but it does protect various interests subsumed within the notion of privacy. In 1928, in *Olmstead v. United States*,[11] the Supreme Court held that the Constitution did not prevent federal officials from wiretapping telephone conversations without probable cause or a warrant as long as they did not trespass on private property in doing so. Five justices saw no illegal search or seizure under the Fourth Amendment and no compelled self-incrimination under the Fifth Amendment. In a strong dissent, Justice Brandeis continued his quest for recognition of a right to privacy:

> The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment. And the use, as evidence in a criminal proceeding, of facts ascertained by such intrusion must be deemed a violation of the Fifth.[12]

---

6. Prosser, *supra* note 1.

7. *Id.* at 389; *see also* RESTATEMENT (SECOND) OF TORTS § 652 (1977).

8. Prosser listed 26 states that had recognized the right, and 11 others that probably would have, had partially, or had legislatively, recognized it. *Id.* at 386–88. He cited only four states that still rejected it. *Id.* at 388.

9. *See* Michael S. Raum, Comment, *Torts—Invasion of Privacy: North Dakota Declines to Recognize a Cause of Action for Invasion of Privacy*, 75 N.D. L. REV. 155, 162–64 nn.73–84 (1999).

10. *Id.*

11. 277 U.S. 439 (1928).

12. *Id.* at 478–79 (Brandeis, J. dissenting).

Almost four decades later, the Supreme Court recognized a constitutional right to privacy in *Griswold v. Connecticut*.[13] The Court struck down a Connecticut law banning the use of contraceptives, holding that the law violated the constitutional right to marital privacy. It found that the Constitution protects "zones of privacy" emanating from the "penumbras" of the First, Third, Fourth, Fifth, and Ninth Amendments.[14]

On the heels of *Griswold*, the Supreme Court overruled *Olmstead*. In *Katz v. United States*,[15] the Court found that an electronic listening device attached to a telephone booth violated the Fourth Amendment. In a concurring opinion,[16] Justice Harlan proposed the "reasonable" expectation of privacy rule that would later be adopted by the Court.[17]

In 1977, the Supreme Court considered the privacy of personal information in *Whalen v. Roe*.[18] A group of patients and physicians challenged a New York statute that required the reporting of all prescriptions of certain categories of drugs to state police. The information, including the names of the patient, the physician, and the pharmacy, were stored in a computerized database.[19] The Court discerned at least two "privacy" interests: the interest in avoiding disclosure of personal matters, and the interest in independence in making certain kinds of important decisions.[20] The Court held that the statute violated neither interest. It described various security measures required by the statute, but noted the potential for abuse:

> A final word about issues we have not decided. We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.[21]

13. 381 U.S. 479 (1965).
14. *Id.* at 484.
15. 389 U.S. 347 (1967).
16. *Id.* at 360 (Harlan, J., concurring).
17. Terry v. Ohio, 392 U.S. 1 (1968).
18. 429 U.S. 589 (1977).
19. *Id.* at 593.
20. *Id.* at 599.
21. *Id.* at 605–06.

The Supreme Court has not decided any cases on the basis of this possible right of informational privacy, and the lower courts are divided on whether the Constitution protects against government disclosure of personal information.[22]

C. State Constitutions

While the constitutions of at least ten states include the word "privacy,"[23] only a few provide protection outside the area of criminal search and seizure.[24] By far, the greatest privacy protection is afforded by the constitution of California,[25] which provides that privacy is an inalienable right.[26] Cases have held that this right is broader than the federal constitutional right;[27] creates a right of action against private as well as government entities;[28] applies to minors as well as adults;[29] prevents government and business interests from collecting and stockpiling unnecessary personal information, from improperly using information collected for one purpose for another, from disclosing information to a third party, and from not checking on the accuracy of the information;[30] and encompasses both "informational privacy" (precluding the dissemination and misuse of sensitive and confidential information) and "autonomy privacy" (protecting the making of intimate personal decisions and conducting personal activities without observation, intrusion, or interference).[31]

The Alaska constitution also provides that: "the right of the people to privacy is recognized and shall not be infringed."[32] This right is broader than that

---

22. For a discussion of these cases, see FRED H. CATE, PRIVACY IN THE INFORMATION AGE 60–62 (1997).

23. ALASKA CONST. art. I, § 22; ARIZ. CONST. art. 2, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, §§ 6 & 7; ILL. CONST. art. 1, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

24. Provisions in the Arizona, Illinois, Louisiana, South Carolina and Washington constitutions pertain generally to invasions of privacy with respect to criminal searches and seizures. *Id.*

25. *See* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW 132–35 (1996).

26. CAL. CONST. art. I, § 1.

27. People v. Wiener, 35 Cal. Rptr. 2d 321 (Ct. App. 1994); Am. Acad. of Pediatrics v. Van de Kamp, 263 Cal. Rptr. 46 (Ct. App. 1989).

28. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994); Kraslawsky v. Upper Deck Co., 65 Cal. Rptr. 2d 297 (Ct. App. 1997); Cutter v. Brownbridge, 228 Cal. Rptr. 545 (Ct. App. 1986).

29. Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797 (Cal. 1997); Am. Acad. of Pediatrics v. Van de Kamp, 263 Cal. Rptr. 46 (Ct. App. 1989).

30. Cent. Valley Chapter Seventh Step Found., Inc. v. Younger, 262 Cal. Rptr. 496 (Ct. App. 1989); Pitman v. City of Oakland, 243 Cal. Rptr. (Ct. App. 1988); Betchart v. Dep't of Fish & Game, 205 Cal. Rptr. 135 (Ct. App. 1984); Stackler v. Dep't of Motor Vehicles, 164 Cal. Rptr. 203 (Ct. App. 1980); Mullaney v. Woods, 158 Cal. Rptr. 902 (Ct. App. 1979).

31. Am. Acad. of Pediatrics v. Lungren, 940 P.2d 797 (Cal. 1997); Loder v City of Glendale, 927 P.2d 1200 (Cal. 1997); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994); Nahrstedt v. Lakeside Vill. Cond. Ass'n, 878 P.2d 1275 (Cal. 1994).

32. ALASKA CONST. art. 1, § 22.

guaranteed by the federal constitution[33] with its "emanations"[34] and "penumbras."[35]

Hawaii's constitution provides for a right to privacy.[36] The Hawaii Supreme Court has stated that its constitution "affords much greater privacy rights than the federal right to privacy"[37] and that:

> The right-to-privacy provision of article I, section 6 relates to privacy in the informational and personal autonomy sense, encompassing the common law right to privacy or tort privacy, and the ability of a person to control the privacy of information about himself, such as unauthorized public disclosure of embarrassing or personal facts about himself. ... It concerns the possible abuses in the use of highly personal and intimate information in the hands of government or private parties.[38]

The Montana constitution provides that the "right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."[39] The Montana Supreme Court has stated that the guarantee applies to state action in conducting a search or seizure, to "autonomy privacy," and to confidential "informational privacy."[40] Thus, the court refused to issue an investigative subpoena for medical records absent a sufficient showing of probable cause that an offense had been committed.[41]

Florida's constitution provides that "every natural person has the right to be let alone and free from governmental intrusion into the person's private life."[42] The Florida Supreme Court discussed the history of this provision:

> The citizens of Florida opted for more protection from governmental intrusion when they approved article I, section 23, of the Florida Constitution. This amendment is an independent, freestanding constitutional provision which declares the fundamental right to privacy. Article I, section 23, was intentionally phrased in strong terms. The drafters of the amendment rejected the use of the words "unreasonable" or "unwarranted" before the phrase "governmental intrusion" in order to make the privacy right as strong as possible. Since the people of this state exercised their prerogative and enacted an amendment to the

---

33. *See* Messerli v. State, 626 P.2d 81 (Alaska 1980); State v. Daniel, 589 P.2d 408 (Alaska 1979); Woods & Rohde, Inc. v. State Dep't of Labor, 565 P.2d 138 (Alaska 1977).

34. Falcon v. Alaska Pub. Offices Comm'n, 570 P.2d 469 (Alaska 1977).

35. State v. Glass, 583 P.2d 872 (Alaska 1978).

36. HAW. CONST. art. I, § 6. Section 7 deals with searches and seizures.

37. State v. Kam, 748 P.2d 372, 377 (Haw. 1988).

38. State v. Lester, 649 P.2d 346, 353 (Haw. 1982).

39. MONT. CONST. art. II, § 10. This provision applies only to state action. *See* State v. Long, 700 P.2d 153 (Mont. 1985).

40. State v. Nelson, 941 P.2d 441, 448 (Mont. 1999); *see also* Hulse v. State, 961 P.2d 75 (Mont. 1998); Gryczan v. State, 942 P.2d 112 (Mont. 1997); State v. Dolan, 940 P.2d 436 (Mont. 1997).

41. *Nelson*, 941 P.2d at 450; *cf.* United States v. Miller, 425 U.S. 435 (1976) (holding that the Fourth Amendment offers no protection against a subpoena to a bank for a customer's financial records).

42. FLA. CONST. art. I, § 23.

> Florida Constitution which expressly and succinctly provides for a strong right of privacy not found in the United States Constitution, it can only be concluded that the right is much broader in scope than that of the Federal Constitution.[43]

Florida has applied its right of privacy in grandparent visitation cases, addressing the "right of decisional autonomy" or "childrearing autonomy," and holding that, absent a showing that denial of visitation would harm the child, the parents' right to privacy would be adversely affected by a visitation order.[44]

II. COMPUTER CRIME LEGISLATION

In 1978, Arizona[45] and Florida[46] passed the first "computer crime" bills. Since then, every state has enacted criminal legislation addressing computers.[47] Most states have modified existing definitions to close loopholes and have created new crimes, such as computer trespass, computer tampering, misuse of computer system information, and computer invasion of privacy.[48] The crime of computer invasion of privacy may be generally described as the use of a computer to view information without authority. For example, a person may use a computer

---

43. Winfield v. Div. of Pari-Mutuel Wagering, 477 So. 2d 544, 548 (Fla. 1985).

44. Von Eiff v. Azicri, 720 So. 2d 510 (Fla. 1998); Beagle v. Beagle, 678 So. 2d 1271 (Fla. 1996); S.G v. C.S.G., 726 So. 2d 806 (Fla. Ct. App. 1999).

45. ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (2000).

46. FLA. STAT. ch. 815.01–815.07 (1999).

47. ALA. CODE §§ 13A-8-100 to 13A-8-103 (2000); ALASKA STAT. §§ 11.46.200(a)(3), 11.46.484(a)(5), 11.46.740, 11.46.985, 11.46.990 (2000); ARIZ. REV. STAT. ANN. §§ 13-2301(E), 13-2316 (2000); ARK. CODE ANN. §§ 5-41-101 to 5-41-108 (1999); CAL. PENAL CODE § 502 (2000); COLO. REV. STAT. §§ 18-5.5-101 to 18-5.5-102 (1999); CONN. GEN. STAT. §§ 53a-250 to 53a-261 (1999); DEL. CODE ANN. tit. 11, §§ 931-939 (1999); FLA. STAT. ch. 815.01 to 815.07 (1999); GA. CODE ANN. §§ 16-9-90 to 16-9-94 (1999); HAW. REV. STAT. §§ 708-890 to 708-893 (1999); IDAHO CODE §§ 18-2201 to 18-2202, 26-1220 (1999); 720 ILL. COMP. STAT. 5/16D-1 to 5/16D-7 (2000); IND. CODE §§ 35-43-1-4, 35-43-2-3 (2000); IOWA CODE §§ 716A.1 to 716A.16 (1999); KAN. STAT. ANN. § 21-3755 (1999); KY. REV. STAT. ANN. §§ 434.840 to 434.860 (1998); LA. REV. STAT. ANN. §§ 14:73.1 to 14:73.5 (2000); ME. REV. STAT. ANN. tit. 17-A, §§ 431 to 433 (1999); MD. ANN. CODE art. 27, § 146 (1999); MASS. GEN. LAWS ANN. ch. 266, §§ 30, 33A, 120F (2000); MICH. COMP. LAWS ANN. §§ 752.791 to 752.797 (1999); MINN. STAT. §§ 609.87 TO 609.894 (1999); MISS. CODE ANN. §§ 97-45-1 TO 97-45-13 (2000); MO. ANN. STAT. §§ 569.093 to 569.099 (1999); MONT. CODE ANN. §§ 45-2-101, 45-6-310 TO 45-6-311 (1999); NEB. REV. STAT. §§ 28-1343 TO 28-1348 (2000); NEV. REV. STAT. §§ 205.473 TO 205.513 (2000); N.H. REV. STAT. ANN. §§ 638:16 TO 638:19 (1999); N.J. REV. STAT. §§ 2C:20-23 TO 2C:20-34 (2000); N.M. STAT. ANN. §§ 30-45-1 TO 30-45-7 (2000); N.Y. PENAL LAW §§ 156.00 TO 156.50 (1999); N.C. GEN. STAT. §§ 14-453 TO 14-457 (1999); N.D. CENT. CODE §§ 12.1-06.1-01, 12.1-06.1-08 (2000); OHIO REV. CODE ANN. §§ 2913.01, 2913.03(C), 2913.04 (Anderson 2000); OKLA. STAT. tit. 21, §§ 1951-1958 (1999); OR. REV. STAT. § 164.377 (1997); 18 PA. CONS. STAT. § 3933 (1999); R.I. GEN. LAWS §§ 11-52-1 TO 11-52-8 (2000); S.C. CODE ANN. §§ 16-16-10 to 16-16-40 (1999); S.D. CODIFIED LAWS §§ 43-43B-1 to 43-43B-8 (2000); TENN. CODE ANN. §§ 39-14-601 to 39-14-603 (1999); TEX. PENAL CODE ANN. §§ 33.01 to 33.04 (2000); UTAH CODE ANN. §§ 76-6-701 to 76-6-705 (1999); VT. STAT. ANN. tit. 13, §§ 4101 to 4107 (2000); VA. CODE ANN. §§ 18.2-152.2 to 18.2-152.14 (2000); WASH. REV. CODE §§ 9.26A.100, 9A.52.010, 9A.52.110 to 9A.52.130 (2000); W. VA. CODE §§ 61-3C-1 to 61-3C-21 (2000); WIS. STAT. § 943.70 (1999); WYO. STAT. ANN. §§ 6-3-501 to 6-3-505 (2000).

48. *See* statutes cited, *supra* note 47.

system at work to find out personal information about a neighbor. Almost every state has at least one statute that may be used to prosecute such behavior.[49]

The names of the crimes vary greatly, from the general to the specific. For example, Georgia,[50] Virginia,[51] and West Virginia[52] each have an offense called "computer invasion of privacy," and Maine has one called "criminal invasion of computer privacy."[53] The mental states required by the various statutes include numerous combinations of terms like "knowingly," "willfully," "intentionally," "recklessly," "without authority," "without consent," "without effective consent," "without permission," and "without right."[54] A number of states also address the situation where someone has authority to access a computer system, but exceeds that authority.[55]

The statutes vary greatly as to the proscribed actions. Most prohibit "access" of a computer, although some specify behavior such as "discloses," "uses," "makes use of," "takes," "takes possession of," "obtains," "retains," and "receives."[56] The object of the proscribed action also varies, although most states prohibit "access" to a "computer," "computer system," or "data."[57]

The laws usually contain a detailed set of definitions. Terms like "computer," "computer system," "data," "property," and "access" are defined in a vast majority of the statutes.[58] Some states already have amended their definitions. For example, Georgia passed its first "Computer Systems Protection Act" in 1981.[59] Ten years later, it replaced the entire statute.[60] Under the old law, a computer was defined as "an internally programmed, general-purpose, digital device that automatically processes substantial data."[61] The definition was arguably too broad, too narrow, and too vague. It was too broad because it included watches, calculators, microwave ovens, and other "general purpose, digital devices."[62] It was too narrow because it excluded analog and other nondigital computers.[63] The new definition is more explicit:

---

49. *Id.* Table I of the Appendix lists the statutes.

50. GA. CODE ANN. § 16-9-93(c) (1999).

51. VA. CODE ANN. §§ 18.2-152.5 (2000).

52. W. VA. CODE § 61-3C-12 (2000).

53. ME. REV. STAT. ANN. tit. 17-A, § 432 (1999).

54. *See* Appendix, Table I.

55. *See id.* For cases that have addressed the issue of exceeding authority, *see infra* notes 99–103 and accompanying text.

56. *See* Appendix, Table I.

57. *See id.*

58. Table II of the Appendix lists the terms that are specifically defined by each state. Table II also includes a list of other relevant terms that are defined, such as "without authority," "private personal data," and "database."

59. GA. CODE ANN. §§ 16-9-90 to 16-9-95, 1989 Ga. Laws 1981 §§ 1-6, 1982 § 16, 1989 § 16 (repealed 1991).

60. GA. CODE ANN. §§ 16-9-90 to 16-9-94 (1999).

61. GA. CODE ANN. § 16-9-92(2) (enacted 1981, repealed 1991).

62. *Id.*

63. *Id.*

> "Computer" means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device or system performing computer operations with or on data and includes any data storage facility or communications facility directly related to or operating in conjunction with such device; but such term does not include an automated typewriter or typesetter, portable hand-held calculator, household appliance, or other similar device that is not used to communicate with or to manipulate any other computer.[64]

Georgia is one of just three states, along with Virginia and West Virginia, that has a crime called "computer invasion of privacy."[65] The three statutes generally penalize the intentional use of a computer or computer network to examine the "employment, salary, credit or any other financial or personal information relating to any other person" with knowledge that the examination is not authorized.[66] These statutes arguably include the accessing of any of the proscribed personal data on the World Wide Web or in specialized databases by anyone who knows he lacks the authority to look at it.

The only reported cases under these three statutes come from Virginia. In *Plasters v. Commonwealth,*[67] a part-time police department dispatcher was convicted of several counts of computer invasion of privacy for accessing the Virginia Criminal Information Network for personal purposes.[68]

Under Virginia law, an individual who is injured by a of violation of the criminal invasion of privacy statute can bring a civil action for damages.[69] In *S.R. v. INOVA Healthcare Services,*[70] a health care professional brought a civil action against two nurses and several hospitals and health providers, alleging that the nurses had used a computer system to access and examine her personal medical information. The plaintiff, who worked with the nurses at the defendant's hospital, had admitted herself to the psychiatric unit of a different hospital also owned by the defendant to ensure confidentiality.[71] The court, noting that this was a case of first impression, delineated the elements of the civil cause of action:

> (1) the use of a computer or computer network by the offender; (2) with the intent to examine another's records; (3) in an unauthorized context when the offender knew or should have known that he was

---

64. GA. CODE ANN. § 16-9-92(1) (1999).

65. GA. CODE ANN. §16-9-93(c) (1999); VA. CODE ANN. § 18.2-152.5 (2000); W. VA. CODE § 61-3C-12 (2000).

66. GA. CODE § 16-9-93(C) (1999); VA. CODE ANN. § 18.2-152.5 (2000); W. VA. CODE § 61-3C-12 (2000). Georgia also includes "medical" data in the list of restricted information.

67. 2000 Va. App. LEXIS 473, at *3 (June 27, 2000).

68. *Id.* at *6. Similar cases arising under an Ohio statute have yielded similar results. The courts have generally held that police use of the Law Enforcement Automated Data System computer system for other than legitimate criminal justice purposes is a violation of Ohio's unauthorized use of computer property statute. *See* Floyd v. Thomas, 2000 Ohio App. LEXIS 2760, at *14–15 (June 26, 2000); Scarso v. Vill. of Mayfield, 1999 Ohio App. LEXIS 5459, at *13 (Nov. 18, 1999); State v. Giannini, 1998 Ohio App. LEXIS 6023, at *1(Dec. 11, 1998); State v. Violi, 1995 Ohio App. LEXIS 5882, at *16 (Dec. 29, 1995); Barker v. Kattelman, 634 N.E.2d 241, 248 (Ohio Ct. App. 1993).

69. VA. CODE ANN. § 18.2-152.12 (2000).

70. 1999 Va. Cir. LEXIS 287, at *2 (June 1, 1999).

71. *Id.* at *4.

> without authority to examine the records; and (4) the records so examined contain employment, financial, or personal information of the pleader.[72]

The court refused to dismiss the plaintiff's claim, holding that the kind of information contained in medical history files that the nurses accessed was "personal information" that fell squarely within the ambit of the statute.[73] The plaintiff had filed a ten-count motion for judgment alleging claims for, among others, breach of contract, negligent infliction of emotional distress, intentional infliction of emotional distress, invasion of privacy and computer invasion of privacy.[74] After a hearing, the trial court judge dismissed some of the claims and granted leave to file an amended motion.[75] Plaintiff filed a seven-count amended motion.[76] The court dismissed all the claims but the invasion of privacy and computer invasion of privacy counts. [77]

In Maine, "criminal invasion of computer privacy" requires that a person intentionally access a computer resource knowing that he is not authorized to do so.[78] "Computer resource" includes "computer information," which, in turn, includes confidential or proprietary information or facts.[79] There is also an "aggravated criminal invasion of computer privacy" statute that requires that a person intentionally and without authority make an unauthorized copy of computer software or computer information, damage a computer resource, or introduce a computer virus into a computer resource.[80] There are no reported cases under these sections.

Connecticut, Delaware, and New Hampshire have very general "unauthorized access to a computer system" statutes, prohibiting the access of a computer system without authorization, knowing that he is not authorized.[81] In Connecticut and New Hampshire, it is an affirmative defense that a person reasonably believed that he had authority, would have been able to get authority without payment of any consideration, or could not have known that his access was unauthorized.[82] In addition, each of these states criminalizes the "misuse of computer system information" when a person (1) as a result of accessing a computer, intentionally makes an unauthorized use, disclosure, or copy of data; (2) intentionally or recklessly and without authorization takes or intercepts data; (3) knowingly receives or retains data obtained in violation of subsection (1) or

---

72. *Id.* at *23.
73. *Id.* at *28.
74. *Id.* at *2.
75. *Id.*
76. *Id.* at *3.
77. *Id.* at *27.
78. ME. REV. STAT. ANN.17-A § 432 (1999).
79. ME. REV. STAT. ANN. 17-A § 431.
80. ME. REV. STAT. ANN.17-A § 433.
81. CONN. GEN. STAT. §§ 53a-250 to 53a-261 (1999); DEL. CODE ANN. tit. 11, §§ 931-939 (1999); N.H. REV. STAT. ANN. §§ 638:16 to 638:19 (1999).
82. CONN. GEN. STAT. § 53a-251(b)(2) (1999); N.H. REV. STAT. ANN. §§ 638:17(I) (1999).

(2); or (4) uses or discloses any data he knows or believes were obtained in violation of subsection (1) or (2).[83]

Connecticut and Delaware define "private personal data" as "data concerning a natural person which a reasonable person would want to keep private and which is protectable under law."[84] Both states use the definition to categorize the severity of the crime. Connecticut deems the value of private personal data to be $1500,[85] making its misuse a class D felony,[86] while Delaware values it at $500,[87] making its misuse a class A misdemeanor.[88] Many other statutes adjust the degree of crime to the factual circumstances, for example, based upon how much monetary damage is involved.[89]

In *Wesley College v. Pitts,*[90] the United States District Court for the District of Delaware entertained a civil case with federal claims and claims under a Delaware law that authorizes a civil action for violations of its computer crime statutes.[91] The court stated that Delaware's misuse of computer system information section requires "actual belief of wrongdoing or the cognizance of the 'high probability' of wrongdoing"[92] and that access "contemplates something more technologically advanced than an untoward glance at the computer screen of a careless user."[93] The case involved an acrimonious situation on a college campus with allegations of job descriptions worded so as to exclude present employees, denials of tenure and promotion, and intercepted emails, casual or otherwise. The court questioned whether the statutory term "data"[94] includes things like "gossip about an interoffice email delivered by one loose tongue to another."[95] Thus, the court granted summary judgment for the defendants on the state claims.

Missouri has two relevant statutes. "Tampering with computer users" prohibits a person from knowingly and without authorization, or without reasonable grounds to believe he has such authorization, (1) disclosing or taking data, (2) accessing a computer or computer system and *intentionally examining information about another person,* or (3) receiving, retaining, using, or disclosing any data he knows or believes was obtained in violation of this subsection.[96]

---

83. CONN. GEN. STAT. § 53a-251(e) (1999); DEL. CODE ANN. tit. 11 § 935 (1999); N.H. REV. STAT. ANN. § 638:17(IV) (1999). Note that Delaware substitutes the word "interrupts" for "intercepts."

84. CONN. GEN. STAT. § 53a-250(10) (1999); DEL. CODE ANN. tit. 11, § 931(10) (1999).

85. CONN. GEN. STAT. § 53a-259(c) (1999).

86. CONN. GEN. STAT. § 53a-254 (1999).

87. DEL. CODE ANN. tit. 11, § 939(i) (1999).

88. DEL. CODE ANN. tit. 11, § 939(e) (1999).

89. *See, e.g.*, ARK. CODE ANN. § 5-41-104 (1999); TEX. PENAL CODE ANN. § 33.02 (2000).

90. 974 F. Supp. 375 (D. Del. 1977), *aff'd*, 172 F.3d 861 (3d Cir. 1998).

91. DEL. CODE ANN. tit. 11, §§ 932, 935, 939 (1999).

92. *Wesley Coll.*, 974 F. Supp. at 392.

93. *Id.*

94. *Id.*

95. *Id.*

96. MO. ANN. STAT. § 569.095 (1999) (emphasis added).

In contrast, Kentucky specifically exempts from its statute the mere obtaining of information.[97] Even making false or fraudulent representations to access a computer, computer system, or data is not a violation if the sole purpose of the access was to obtain information and not to commit any other act proscribed by the section, such as fraudulent schemes or altering, damaging, or destroying data.[98]

In New York a person is guilty of "computer trespass" if he knowingly uses a computer without authorization to knowingly gain access to "computer material."[99] "Computer material" includes medical records, records maintained by the state that can be used to identify the individual and that are otherwise prohibited from law from being disclosed, and computer data that are not intended to be available to anyone other those "rightfully in possession thereof."[100] Two New York cases have addressed this statute. In *People v. O'Grady,*[101] an employee of the state Department of Taxation and Finance was convicted of computer trespass.[102] An investigation determined that she had used her log-in and employee identification to enter the department's computer system without authorization to access the tax records of family members of a woman with whom she had a dispute.[103] The court held that there was ample evidence to support the conviction.[104] In *People v. Katakam,*[105] however, a criminal indictment for computer trespass was dismissed because there was no proof that the computer access was unauthorized. A former employee had always enjoyed wide access to the former employer's computers, and it was not clear that the defendant had been forbidden access to a particular file.[106]

As mentioned earlier, a number of states specifically address the issue of a person exceeding his or her given authority.[107] In *Briggs v. State,*[108] the Court of Appeals of Maryland reversed a conviction of a former employee who contended

---

97. KY. REV. STAT. ANN. § 434.845 (2) (1998). This statute states that "accessing, attempting to access . . . even though a fraud, false or fraudulent pretenses, representations or promises may have been involved . . . shall not constitute a violation of this section if the sole purpose of the access was to obtain information and not to commit any other act proscribed by this section." *Id.*

98. KY. REV. STAT. ANN. § 434.845 (1998).

99. N.Y. PENAL LAW § 156.10 (1999).

100. N.Y. PENAL LAW § 156.00(5).

101. 695 N.Y.S.2d 140 (N.Y. App. Div. 1999)

102. *Id.* at 142.

103. *Id.*

104. *Id.*

105. 660 N.Y.S.2d 334 (N.Y. Sup. Ct. 1997).

106. *Id.* at 337.

107. ARIZ. REV. STAT. § 13-2316 (2000); 720 ILL. COMP. STAT. 5/16D-3 (2000); KAN. STAT. ANN. § 21-3755(b)(1)(C) (1999); MD. ANN. CODE art. 27, § 146(c)(1) (1999); MICH. COMP. LAWS § 752.795 (1999); NEB. REV. STAT. §§ 28-1344 to 28-1347 (2000); N.M. STAT. ANN. § 30-45-5 (2000); N.D. CENT. CODE § 12.1-06.1-08 (2000); OKLA. STAT. tit. 21, § 1953(A)(3) (1999). For states that address exceeding authority in specific definitions of "authorization," "without authorization" or "without authority," see GA. CODE ANN. § 16-9-2(11) (1999); HAW. REV. STAT. § 708-890 (1999); ME. REV. STAT. ANN. tit. 17-A, § 431(11) (1999); N.Y. PENAL LAW § 156.00(6) (1999); N.C. GEN. STAT. § 14-453(1A) (1999); R.I. GEN. LAWS § 11-52-1(15)(e) (2000); UTAH CODE ANN. § 76-6-702(2) (1999); VA. CODE ANN. § 18.2-152.2 (2000).

108. 704 A.2d 904 (Md. 1998).

that his access was not without authority, but rather merely exceeded his given authority. At the time, the Maryland statute prohibited access that was intentional, willful, and without authority.[109] It did not address the issue of exceeding one's authority. After *Briggs*, the legislature added the phrase "or exceed the person's authorized access."[110]

In a similar case in Florida, where the applicable statute speaks only of "without authorization," the Court of Appeals reversed the denial of a defendant's motion to dismiss criminal charges. The court held in *Gallagher v. State*[111] that criminal sanctions were not the appropriate remedy for a public employee who exceeded his authority.[112]

Besides New York, two other states specifically protect public information. In West Virginia, any person who knowingly, willfully, and without authorization accesses a computer and obtains information filed by any person with the state that is required to be kept confidential is guilty of a misdemeanor.[113] In Nebraska, any person who intentionally accesses a computer without authorization or knowingly and intentionally exceeds authorization, and obtains information filed by the public with the state that is by statute required to be kept confidential is guilty of a misdemeanor.[114]

In Minnesota, a person who intentionally and without authority attempts to or does penetrate a "computer security system" is guilty of unauthorized computer access.[115] A "computer security system" is a software program or computer device that is intended to protect the confidentiality and secrecy of data and information.[116]

In South Carolina, willfully, knowingly, and without authorization or for an unauthorized purpose engaging in "computer hacking" is a crime.[117] "Computer hacking" means accessing a computer for the purpose of establishing contact, but without the intent to defraud or commit any other crime.[118] If there were such intent, it would be a more serious offense.[119]

As discussed above, most other states have similar statutes that generally prohibit the intentional accessing of computers or data. In Massachusetts a court upheld the constitutionally of its "unauthorized access to computer system" statute.[120] The defendant had illegally accessed a hospital computer system on at least 44 occasions, accessing at least 1,720 confidential patient files. The court rejected the defendant's contention that the statute was unconstitutionally vague

---

109. *Id.* at 907.
110. 27 MD. ANN. CODE § 146(c)(1) (1999).
111. 618 So. 2d 757 (Fla. Dist. Ct. App. 1993).
112. *Id.* at 758.
113. W. VA. CODE § 61-3C-11 (2000).
114. NEB. REV. STAT. § 28-1346 (2000).
115. MINN. STAT. § 609.891(1) (1999).
116. MINN. STAT. § 609.87(11).
117. S.C. CODE ANN. § 16-16-20(4) (1999).
118. S.C. CODE ANN. § 16-16-10(j).
119. S.C. CODE ANN. § 16-16-20(1).
120. Commonwealth v. Farley, 1996 WL 1186936, at *3 (Mass. Super. Oct. 18, 1996).

because it failed to define the word "access." The court noted that all fifty states have criminal statutes regarding accessing a computer system without authority and that the majority use the term "access."[121]

For the most part, the crime of invasion of privacy has focused on the first prong of the civil tort, intrusion. The vast majority of states prohibit the "accessing" of data or information. In states that also ban the "use" or "disclosure" of such data or information, the second and third prongs, public disclosure of embarrassing private facts and false light, may become relevant. The fourth prong, appropriation, is rarely involved.

III. REFLECTIONS

There is much public discussion and debate about privacy. Congress is examining over forty bills on the subject.[122] New questions arise as technology advances. For example, as most courts move towards electronic filing systems, often with online access, is it still appropriate to make the entire record public? These records often contain social security numbers, bank account information, and other sensitive personal information. Should such information be removed from the files that are placed online? Similarly, with computers, digital storage devices, and the Internet, records of criminal convictions can be distributed widely. Does the ease of access to these data alter the balance between society's interest in seeing the information and the individual's right to privacy?

The next few years will see many changes in the law that will completely redefine the nature of informational privacy. As people become more aware of the ramifications of disclosing personal information, they will demand greater privacy with respect to the collection and use of that data. Almost every state already has at least one statute under which a computer invasion of privacy can be prosecuted. Yet, even in states with statutes directly geared towards such activity, prosecutions have been few.[123] Perhaps this is not surprising, given the uncertainty about the scope of protection for personal information. As a clearer definition of what is protected emerges, these statutes will be used more. The basic nature of the crime is accessing information that one knows should not be accessed. Both the "outsider," who has no authority to access the information, and the "insider," who is entrusted with some authority, but who abuses or exceeds that authority, commit these crimes. As the law of informational privacy evolves, we will see more criminal prosecutions for invasion of privacy.

---

121. *Id.*

122. *See* ELECTRONIC PRIVACY INFORMATION CENTER, EPIC BILL TRACK, *available at* http://www.epic.org/privacy/bill_track.html (last visited July 28, 2001).

123. For example, in Georgia, which has a specific "computer invasion of privacy" statute, there were nine arrests made under this statute from 1996 to 2001, according to a representative of the Georgia Bureau of Investigation in a telephone conversation on September 6, 2001. Also, Fulton County Senior Assistant District Attorney in White Collar Crime, Cassandra Kirk, reported in a telephone conversation on September 6, 2001, that her office has had three indictments under this statute, with two defendants pleading guilty to other computer crime offenses, and has one other case awaiting indictment under this statute.

Appendix

Table I. State Computer Crime Statutes That May Address an Invasion of Privacy

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
Alabama	Offense against intellectual property	w, k & w/o a	access, examination	data	internal or external to a computer
	Offense against intellectual property	w, k & w/o a	discloses, uses or takes	data	
Alaska	Criminal use of a computer	w/o right, k	accesses	computer	and as a result of that access obtains information about that person
	Criminal mischief	k	accesses	computer	
Arizona	Computer fraud	i & w/o a or ea	accessing	computer, data	
Arkansas	Computer trespass	i & w/o a	accesses	computer, data	
California	Computer crime	k & w/o permission	accesses	computer	
	Computer crime	k accesses & w/o permission	takes, copies or makes use of	data	whether internal or external to a computer
Colorado	Computer crime	k & w/o a	uses	computer, data	
Connecticut	Unauthorized access to a computer system	knowing he is not authorized	accesses	computer system	Affirmative defenses include reasonable belief that he had or would have had authorization.
	Misuse of computer system information	as a result of access	intentionally makes an unauthorized display, use disclosure or copy	data	"Private personal data" means data concerning a natural person which a reasonable person would want to keep private and which is protectable under law. It is deemed to have a value of $1500 and is used in assessing the degree of the crime.
	Misuse of computer system information	i or recklessly & w/o a	takes or intercepts	data	
	Misuse of computer system information	i or recklessly & w/o a	knowingly receives or retains	data obtained in violation of this section	
	Misuse of computer system information	i or recklessly & w/o a	uses or discloses	data he knows or believes was obtained in violation of this section	
Delaware	Unauthorized access to a computer system	knowing he is not authorized	access	computer system	"Private personal data" means data concerning a natural person which a

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
	Misuse of computer system information	as a result of access	intentionally makes an unauthorized display, use disclosure or copy	data	reasonable person would want to keep private and which is protectable under law. It is deemed to have a value of $500 and is used in assessing the degree of the crime.
	Misuse of computer system information	i or recklessly & w/o a	takes or interrupts	data	
	Misuse of computer system information	i or recklessly & w/o a	knowingly receives or retains	data obtained in violation of this section	
	Misuse of computer system information	i or recklessly & w/o a	uses or discloses	data he knows or believes was obtained in violation of this section	
Florida	Offense against computer user	w, k & w/o a	accesses	computer	
Georgia	Computer invasion of privacy	knowledge that examination is w/o a	examination	employment, medical, salary, credit, or other financial or personal data	
Hawaii	Unauthorized computer use	i & w/o a	accesses	computer, data	
Idaho	Computer crime	k & w/o a	uses, accesses	computer, data	
Illinois	Computer tampering	k & w/o a or ea	accesses	data	
Indiana	Computer trespass	k or i	accesses	computer system	
Iowa	Unauthorized access	k & w/o a	accesses	computer	
Kansas	Computer trespass	i & w/o a	accessing	data, property	
	Computer crime	i & w/o a	accessing & copying, disclosing or taking possession of	computer, property	
	Computer crime	i ea	accessing & copying, disclosing or taking possession of	computer, property	
Kentucky	Unlawful access to a computer	k & w	access	data, computer	shall not constitute a violation if the sole purpose of the access was to obtain information
Louisiana	Offense against intellectual property	i & w/o consent	disclosure, use, copying, taking or accessing	intellectual property	

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
Maine	Criminal invasion of computer privacy	i & knowing that he is not authorized	accesses	computer resources	
Maryland	Unauthorized access to computers	i, w & w/o a or ea	access	computer, computer database	
Massachusetts	Unauthorized accessing of computer systems	w/o a & k	accesses	computer system	
Michigan	Fraudulent access to computer	i & w/o a or ea	access to acquire	property	
Minnesota	Unauthorized computer access	i & w/o a	penetrates	computer security system	"computer security system" is a software program or computer device intended to protect the confidentiality and secrecy of data and information
Mississippi	Offense against intellectual property	i & w/o consent	disclosure, use, copying, taking or accessing	intellectual property	
Missouri	Tampering with computer users	k & w/o a	access	computer	
	Tampering with computer data	k & w/o a	discloses or takes	data	
	Tampering with computer data	k & w/o a	accesses and intentionally examines	information about another person	
	Tampering with computer data	k & w/o a	receives, retains, uses or discloses	data he knows or believes was obtained in violation of this section	
Montana	Unlawful use of a computer	k or purposely, & w/o consent	obtains the use of	computer	"obtain the use of" includes retrieving data from or otherwise making the use of any resources of a computer
Nebraska	Access without authorization	i & w/o a, or k & i ea	accesses	computer, data	
	Depriving or obtaining property or services	i & w/o a, or k & i ea	obtains	property or services	
	Obtaining confidential public information	i & w/o a, or k & i ea	obtains	information filed by the public and required to be kept confidential	
Nevada	Unlawful use or access of a computer	k, w & w/o a	accesses	computer	

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
	Unlawful acts regarding computers	k, w & w/o a	discloses, uses, takes, retains possession of, copies, obtains access to	data	
New Hampshire	Unauthorized access to a computer system	knowing he is not authorized	accesses	computer system	Affirmative defenses include reasonable belief that he had or would have had authorization.
	Misuse of computer system information	as a result of access	knowingly makes an unauthorized display, use disclosure or copy	data	Unlike Connecticut and Delaware, there is no definition of "private personal data".
	Misuse of computer system information	k or recklessly & w/o a	takes or intercepts	data	
	Misuse of computer system information	k or recklessly & w/o a	knowingly receives or retains	data obtained in violation of this section	
	Misuse of computer system information	k or recklessly & w/o a	uses or discloses	data he knows or believes was obtained in violation of this section	
New Jersey	Wrongful access to a computer system	purposefully & w/o a	accesses	computer system	where the accessing cannot be assessed a monetary value or loss
	Disclosure of data from wrongful access	purposefully & w/o a	access and discloses	data, database	where the accessing and disclosing cannot be assessed a monetary value or loss
	Wrongful access to a computer system	purposefully & w/o a	accesses	computer	where this action does not result in the altering, damaging or destruction of any property or services
New Mexico	Unauthorized computer use	k, w & w/o a or ea	acceses, uses, takes, obtains, copies	computer, computer property	
New York	Computer trespass	k uses & w/o a	knowingly gains access to	computer material	"computer material" includes medical records, records maintained by the state and prohibited by law from being disclosed, and data that is not intended to be available to anyone other than those rightfully in possession thereof
North Carolina	Accessing computers	w & w/o a	accesses	computer	
North Dakota	Computer crime	i & w/o a or ea	access, copying,	computer, data	

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
			disclosing, or taking possession of		
Ohio	Unauthorized use of computer property	k	access	computer	Affirmative defenses include reasonable belief that he had or would have had authorization.
Oklahoma	Prohibited act	w & w/o a	access	computer, property	
	Prohibited act	w & w/o a	access and copy, make use of, disclose, or take possession of	computer, property	
	Prohibited act	w ea	copy, disclose or take possession of	computer, property	
Oregon	Computer crime	k & w/o a	uses, accesses	computer, data	
Pennsylvania	Unlawful use of computer	i & w/o a	accesses	computer, computer database	
Rhode Island	Intentional access	i & w/o a	access	computer, data	
South Carolina	Computer crime	w, k & w/o a	engages in computer hacking	computer	"Computer hacking" means accessing a computer, but without intent to defraud or commit any other crime.
South Dakota	Unlawful use of computer	k & w/o consent	obtains the use of or accesses	computer system	Unlike Montana, there is no definition of "obtains the use of "
Tennessee	Computer offense	i & w/o a	accesses	computer	
	Computer offense	i & w/o a	accesses for the purpose of gaining access to computer material	data, computer	Unlike New York, there is no definition of "computer material"
Texas	Breach of computer security	k & w/o effective consent	accesses	computer	
Utah	Computer crime	w/o a	gains access to and discloses	computer property, computer, data	and thereby causes damages to another
	Computer crime	w/o a	gains access to and obtains	property, information without legal right	This crime is a felony if the information obtained is confidential; a misdemeanor if not.
	Computer crime	i, k & w/o a	gains access to	computer, computer property	
Vermont	Unauthorized access	k, i & w/o lawful a	accesses	computer, data	

	Name of crime	Mental state*	Action	Object of action	Miscellaneous
Virginia	Computer invasion of privacy	i & knows he is w/o a	examines	employment, salary, credit, or other financial or personal data	
Washington	Computer trespass	i & w/o a	gains access to	computer system, electronic database	
West Virginia	Computer invasion of privacy	k, w & w/o a & knowledge that he is w/o a	accesses and examines	employment, salary, credit, or other financial or personal data	
	Obtaining confidential public information	k, w & w/o a	accesses and obtains	information filed with the state that is required by law to be kept confidential	
	Unauthorized possession of computer information	k, w & w/o a	possesses	computer data with knowledge that it was obtained in violation of this section	
Wisconsin	Offenses against computer data and programs	w, k & w/o a	accesses	data	
Wyoming	Crimes against computer users	k & w/o a	accesses	computer	
	Crimes against intellectual property	k & w/o a	discloses or takes	data having a a value of greater than $750 and which is a trade secret or is confidential	

* Abbreviations:
a authorization or authority
ea exceeding authority
i intentionally
k knowingly
w willfully
w/o without

Table II. Terms Specifically Defined by State Statute

	Access	Computer	Computer System	Data	Property	Intellectual Property	Other terms defined
Alabama	√	√	√	√	√	√	
Alaska	√	√	√	√			obtain; property of another
Arizona	√	√	√		√		
Arkansas	√	√	√	√	√		
California	√		√	√			injury; victim expenditure
Colorado		√	√		√		authorization; to use
Connecticut	√	√	√	√	√		private personal data
Delaware	√	√	√	√	√		private personal data
Florida	√	√	√		√	√	
Georgia		√		√	√		use; victim expenditure; without authority
Hawaii	√	√	√	√	√		without authorization
Idaho	√	√	√		√		
Illinois	√	√		√	√		
Indiana	√		√	√			
Iowa	√	√	√	√	√		
Kansas	√	√	√		√		
Kentucky	√	√	√	√	√	√	
Louisiana	√	√	√		√	√	
Maine	√	√	√				computer information; computer resource; not authorized
Maryland	√	√	√				computer data base
Massachusetts					√		
Michigan	√	√	√		√		
Minnesota	√	√	√		√		authorization; computer security system
Mississippi	√	√	√		√	√	use
Missouri	√	√	√	√	√		
Montana		√	√		√		obtain the use of
Nebraska	√	√	√	√	√		
Nevada	√	√		√	√		
New Hampshire	√	√	√	√	√		
New Jersey	√	√	√	√			data base
New Mexico	√	√	√	√			computer property; database
New York		√					computer data; computer material; uses a computer or computer service; without authorization
North Carolina	√	√	√	√	√		authorization
North Dakota	√	√	√		√		
Ohio		√	√	√			gain access
Oklahoma	√	√	√	√	√		victim expenditure
Oregon	√	√	√	√	√		
Pennsylvania	√	√	√		√		data base
Rhode Island	√	√	√	√	√		computer data; uses; without authority
South Carolina	√	√	√	√	√		
South Dakota	√	√	√				
Tennessee	√	√	√	√	√	√	
Texas	√	√	√	√	√		effective consent
Utah	√	√	√				authorization; computer property; confidential
Vermont	√	√	√	√	√		
Virginia		√			√		computer data; uses; without authority
Washington	√	√		√			
West Virginia	√	√			√		authorization; computer data; computer resources
Wisconsin		√	√	√	√		
Wyoming	√	√	√		√	√	