Who Is Watching Your Keystrokes? An Analysis of M.G.L. ch. 214 § 1B, Right to Privacy and Its Effectiveness Against Computer Surveillance

I. INTRODUCTION

As a Massachusetts citizen, you have a statutory right to privacy.[1] The statute declares, "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy" and gives the Massachusetts Superior Court jurisdiction to hear the cases.[2] In the past thirty years, Massachusetts' courts have held, despite broad language of the statute, that many intrusions do not violate this statute. These intrusions include specific employer actions,[3] telemarketing,[4] newspaper articles,[5] and newspaper pictures.[6] This note applies Massachusetts' case law to hypothetical computer-based invasion of privacy cases to predict how the court would rule when confronted by this emerging problem.

This note begins with a brief discussion of the Samuel D. Warren and Louis D. Brandeis Law Review article that shaped the common law right to privacy.[7] The note then describes the Restatement of Torts' privacy categories.[8] Next, the note analyzes Massachusetts' privacy cases to determine what actually constitutes a reasonable and substantial or serious violation of privacy.[9] After

1. MASS. GEN. LAWS ch. 214, § 1B (2000) [hereinafter *Privacy Statute*].

2. *Id.* Ryan v. Normandin, 2001 Mass. App. Div. 148 (2001) (upholding dismissal of claim in District Court).

3. *See e.g.*, Cort v. Bristol-Myers Co., 431 N.E.2d 908 (Mass. 1982) (asking employees personal questions does not violate privacy statue); O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146 (Mass. 1990) (requiring employee's urinalysis after prior notice does not violate Privacy Statute); Williams v. Brigham & Women's Hospital, No. 00-1546A, 2002 Mass. Super. LEXIS 52 at *1 (Jan. 8, 2002) (interfering with employee's privacy was reasonable under the circumstances).

4. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 567 N.E.2d 912 (Mass. 1991) (calling a citizen multiple times in this specific business context does not violate the Privacy Statute).

5. Peckham v. Boston Herald, Inc., 719 N.E.2d 888 (Mass. 1991) (finding newspaper article newsworthy and therefore not actionable as violation of Privacy Statute).

6. Cefalu v. Globe Newspaper Co., 391 N.E.2d 935 (Mass. 1979) (ruling published newspaper picture of citizen in the welfare line did not violate his privacy).

7. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (detailing the evolving law to conclude that privacy needs to be protected).

8. RESTATEMENT (SECOND) OF TORTS § 652B-E (1977).

9. *See* discussion *infra* Part III(B-D) (discussing what constitutes a serious, substantial or unreasonable

this analysis, there is a brief overview of current computer technology[10] and a description of how someone uses a computer to invade the privacy of another. After analysis of a New Jersey common law violation of privacy case,[11] this note uses theoretical fact patterns to demonstrate how a Massachusetts state court might rule when confronted with a computer generated invasion of privacy claim.

II. HISTORY

A law review article written by Samuel D. Warren and Louis D. Brandeis recognized and shaped the common law right to privacy over a century ago.[12] In the first paragraph, they charged that all aspects of a changing society, encompassing the political, social and economic, required the identification of new rights and then used the common law to develop this new right to privacy.[13] The authors understood that with the development of society and civilization, there comes a need to protect the thoughts of man from intrusive, advancing technology.[14] Even in 1890, people knew how important privacy was and therefore recognized that privacy needed additional protection.[15] The "right to be let alone" was born.[16] The evolution of the right to privacy continues to this day.

The Restatement of Torts codified this right of autonomy. The Restatement contains four categories of invasion of privacy: (1) intrusion upon seclusion, (2) appropriation of identity, (3) disclosure of private facts, and (4) publicity that places another in a false light.[17] The right of privacy protects against an "unreasonable intrusion upon the seclusion of another."[18] The unreasonable intrusion alone is enough for a violation of a privacy right, yet it is not actionable until it becomes highly offensive.[19] The intrusion must be substantial and reach the level where a reasonable man would "strongly

---

intrusion of privacy).

10. *See* discussion *infra* Part IV (discussing computer technology and how it violates a user's privacy).

11. White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001); *see also* discussion of *White* case, *infra* Part IV (C).

12. *See* Warren & Brandeis, *supra* note 7, (detailing evolving law to conclude that privacy needs protection).

13. *Id.* at 193.

14. *Id.* at 195 (discussing how appropriation in newspapers and gossip have become rampant).

15. *Id.* at 196.

16. *Id.* at 195 (quoting Judge Cooley who used the phrase in COOLEY ON TORTS, 2d ed., p. 29).

17. RESTATEMENT (SECOND) OF TORTS § 652B-E (1977).

18. RESTATEMENT (SECOND) OF TORTS § 652B (1977). For example, a news photographer enters a patient's hospital room to take a photo of the patient because he has a unusual disease. RESTATEMENT (SECOND) OF TORTS § 652B, illus. 1 (1977). The patient already denied permission to the photographer. *Id.* The photographer violates the patient's privacy by taking the photograph. *Id.*

19. RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1997). While having your photograph taken in a public place may be invasive, the act does not reach the level of highly offensive needed to be actionable. RESTATEMENT (SECOND) OF TORTS § 652B, illus. 6 (1977).

object."[20] Intrusion covers violations, such as opening another's mail or searching another's wallet, as well as those violations using mechanical means, such as tapping a phone to eavesdrop on private conversations.[21]

The second category of privacy invasion is the act of taking another's name or likeness to use for the taker's own benefit.[22] An invasion of privacy occurs when a person or corporation uses the name or likeness of another without permission.[23] A person has exclusive control over how his likeness or name is used.[24] Most of the case samples consist of using the likeness commercially to sell or advertise a product.[25] The person stealing the name or likeness must benefit from using the appropriated name or likeness.[26] Merely using a similar sounding name or likeness does not meet the benefit requirement.[27] The value of the name is the underlying principle of this privacy violation.[28]

The third category covers a person's private life and aims to prevent unreasonable publicity about that private life.[29] The published information must be highly offensive to the person without being a legitimate concern of the public.[30] The First Amendment protects dissemination of information that the public has a right to know.[31]

The last category of the Restatement protects against publicity that unreasonably places a person in a false light to the public.[32] The information must be highly offensive and the defendant must have published the information with reckless disregard as to the falsity of the information or with actual knowledge.[33] The facts must be false and published, yet the statements

---

20. RESTATEMENT (SECOND) OF TORTS § 652B cmt. d (1997). As cited in footnote eighteen, a reasonable person would strongly object to having his picture taken while in a hospital room after denying the photographer permission. RESTATEMENT (SECOND) OF TORTS § 652B, illus. 1 (1977).

21. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1997). *See* DiGirolamo v. D.P. Anderson & Assoc., Inc., No. 97-3623, 1999 Mass. Super. LEXIS 190 (May 1999); *see infra* text accompanying notes 128-33 (discussing Massachusetts court tackling this situation).

22. RESTATEMENT (SECOND) OF TORTS § 652C (1977).

23. *Id.* A corporation, without permission, uses the name of an actor in an advertisement, declaring that the actor likes and uses the product. RESTATEMENT (SECOND) OF TORTS § 652C, illus. 1 (1977). The corporation violated the actor's privacy. *Id. See also* Wendt v. Host Int'l, 125 F.3d 806 (overturning summary judgment as plaintiffs raised genuine issues of material fact regarding defendant's use of their likenesses).

24. RESTATEMENT (SECOND) OF TORTS § 652C cmt. a (1977).

25. RESTATEMENT (SECOND) OF TORTS § 652C cmt. b (1977). *See also* Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905) (cited by the Restatement as the seminal case for common law appropriation).

26. RESTATEMENT (SECOND) OF TORTS § 652C cmt. c (1977).

27. *Id.*

28. *Id.*

29. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

30. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a (1977). For example, a town resident has an affair with his best friend's wife. RESTATEMENT (SECOND) OF TORTS § 652D illus. 6 (1977). A magazine publishes pictures of the two of them in a hotel room together. *Id.* The magazine had invaded both party's privacy as this information is highly offensive. *Id.* In addition, it is not of a legitimate concern to the public as the parties are regular citizens, not public figures. *Id.*

31. RESTATEMENT (SECOND) OF TORTS § 652D special note (1977).

32. RESTATEMENT (SECOND) OF TORTS § 652E (1977).

33. *Id.*

do not have to be defamatory.[34] Once again, Constitutional restrictions apply.[35]

III. MASSACHUSETTS RIGHT TO PRIVACY STATUTE

Twenty-five states have statutes or provisions within their state constitutions protecting the right to privacy.[36] In 1967, a special commission issued a report detailing privacy issues in Massachusetts.[37] Through 1969, the Massachusetts courts declined to recognize a state action for invasion of privacy.[38] In 1973, the legislature codified the right to privacy in a broad statute: "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy."[39] The Massachusetts Legislature intended this statute to cover the same categories originally articulated by Dean Prosser.[40] The legislature made the statute broader than the Restatement, however, by using one sentence to incorporate three different tort categories.[41] This broad statute allows the court to continue interpreting the right expansively.[42]

The language of the privacy statute enables the courts to keep current with technology.[43] By implementing a broad statute, the legislature does not need to

---

34. RESTATEMENT (SECOND) OF TORTS § 652E cmt. b (1977).

35. RESTATEMENT (SECOND) OF TORTS § 652E cmt. d (1977). The First Amendment protects free speech under certain conditions, regardless of whether it invades one's privacy. *Id.* The *Sullivan* rule raises the standard of proof to "actual malice" when the plaintiff is a public official. New York Times v. Sullivan 376 U.S. 254 (1964). Actual malice is knowledge of the falsity of the statement or reckless disregard for the truth or falsity of the statement. *Id.*

36. ROBERT ELLIS SMITH, COMPILATION OF STATE & FEDERAL PRIVACY LAWS, 50-51 (1997) (listing states with a protected right to privacy by statute or state constitution). This number includes states with a right to publicity. *Id.* For example, Texas has a statute proclaiming "[t]he right of publicity for celebrities extends beyond death." *Id.* at 51.

37. COMMONWEALTH OF MA, INTERIM REPORT OF THE SPECIAL COMMISSION ON ELECTRONIC EAVESDROPPING, Mass. Senate 1967-1469 (October 26, 1967). The report concluded the judiciary should define the contours of a right to privacy rather than the legislature creating a bill that would be all-inclusive. *Id.* at 3.

38. Alexander J. Cella, *The Right of Privacy in Massachusetts – Generally*, 39 MASS. PRAC. § 1252, fn. 3 (West, 1986).

39. MASS. GEN. LAWS ch. 214, § 1B (2000). The Privacy Statute gives the Superior Court jurisdiction over disputes and allows them to enforce such rights and award damages. *Id.* Massachusetts also has a law protecting against appropriation. MASS. GEN. LAWS ch. 214, § 3A (2000); William L. Pardee, Note, *The Massachusetts Right of Privacy Statute: Decoy or Ugly Duckling?*, 9 SUFFOLK U. L. REV. 1248 (1975) (asserting that the Legislature ended the controversy regarding whether Massachusetts has a recognized right to privacy).

40. Pardee at 1252 (quoting West edition of the statute but disagreeing since the text of the statute does not support that contention). Dean Prosser was the main draftsman for the restatement. *Id.*

41. *Id.* Pardee goes on to suggest that new lines of interpretation could be developed and followed. *Id.* He also claims restrictions to the three categories make the law less useful. *Id.* The statute only covers three categories because Massachusetts has a separate law protecting against appropriation. MASS. GEN. LAWS ch. 214, § 3A (2000).

42. Survey, 1973 ANNUAL SURVEY OF MASSACHUSETTS §11.14 (1974). *But see* Pardee, *supra* note 39, at 1249 (stating only eight cases had been litigated on the privacy question).

43. Pardee, *supra* note 39, at 1250 (claiming a need for statute to be broad and flexible enough for changing times).

update or change the law simply because technology improved.[44] During the past thirty years, the Massachusetts courts have interpreted this broad statute as granting the court permission to decide on a case-by-case basis while taking societal values into consideration."[45] Litigation follows whenever someone uses new technology to discover private facts about another because the court interprets the statute on a case-by-case basis.

When legislators passed the Privacy Statute in 1973, technology was a threat to privacy, but not to the extent that it is today.[46] Even then, one could see that data processing would ultimately become very cheap and easy to use for legitimate or illegitimate purposes.[47] In the past, one could argue that the government and certain businesses must have access to personal information.[48] Today, however, that contention is not as clear.[49]

A. Massachusetts Legislative Intent

The legislature wrote the statute as if there are three causes of action within the statute: an unreasonable interference, a substantial interference, or a serious interference.[50] Yet, the word "or" does not mean there are three separate causes of action.[51] A serious or substantial violation, which is reasonable, is not actionable under the Privacy Statute.[52] The perfect example of a violation of privacy that is not actionable is a legal search and seizure.[53] While almost everyone would consider a search and seizure a serious or substantial violation

---

44. *Id.* at 1250.

45. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 567 N.E.2d 912, 915 (Mass. 1991).

46. Pardee, *supra* note 39, at 1249-50 (stating technology threat exists from public and private bureaucracies without mentioning a threat from private or public businesses); *see generally* ARTHUR R. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS (1971) (discussing existing technology threats and how they affect the future).

47. Pardee, *supra* note 39, at 1274. Jim Morse, *The Frightening Invasion of Our Privacy*, THE BOSTON HERALD, March 17, 1975 at A5 (editorializing about the different types of erosions of an individual's privacy).

48. Pardee, *supra* note 39, at 1274. Pardee viewed government and business-collected information as privileged and therefore permissible. *Id.*

49. Even after the attacks on September 11, 2001 there are protests against increased access to the privacy of individuals. *See* Reuters News Service, *Ashcroft, Ellison win U.S. Big Brother Privacy Awards*, *at* http://digitalmass.boston.com/news/2002/04/19/privacy.html (discussing winners of the "Big Brother" awards given by the advocy group, Privacy International). Privacy International is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations. Their web site is http://www.privacyinternational.org

50. MASS. GEN. LAWS ch. 214, § 1B (2000).

51. *E.g.*, Pardee, *supra* note 39, at 1267; *Schlesinger*, 567 N.E.2d at 914 (finding the assertion "an interference which falls under any one of the standards would constitute a violation" not correct); O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146, 1151 (Mass. 1990) (mentioning legislature did not intent to protect against reasonable interferences). *But see* Donna E. Artz, *Privacy Law in Massachusetts: Territorial, Informational and Decisional Rights*, 70 MASS. L. REV. 173, 175 (1986) (stating "reasonable can be understood to subsume the concepts of substantial and serious").

52. Pardee, *supra* note 39, at 1267.

53. *Id.; see also Schlesinger*, 567 N.E.2d at 914 (using search and seizure as an example of when a search is serious or substantial but reasonable).

of privacy, it is a reasonable and protected intrusion.[54] The courts have not resolved the issue of whether an attempted violation of privacy is a violation of the Privacy Statute.[55] A complaint must allege a serious or substantial and unreasonable violation, or at least something that the court could interpret as a violation of privacy.[56]

In *Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc.*,[57] the plaintiff sued telemarketers based upon cold call telephone solicitations he received at his business.[58] The plaintiff alleged that the telemarketing calls intruded upon his seclusion and therefore invaded his privacy.[59] The Supreme Judicial Court rejected the argument that there were three separate causes of action created by the language of the privacy statute.[60] The Court confirmed there are times when a serious or substantial violation of privacy occurs, yet because it is reasonable, it is not actionable.[61]

B. Substantial or Serious Interference

For an actionable violation of privacy to occur, the conduct must constitute an unreasonable and substantial or serious interference.[62] The trier of fact determines whether behavior reaches the level necessary for an actionable invasion of privacy.[63] If the intrusion does not reach the level of substantial or serious, no cause of action exists. As a result, the Massachusetts courts have ruled that the first step is to determine whether the intrusion reaches the serious or substantial level.[64] The court will look at the circumstances surrounding the intrusion, determine if there was a reasonable expectation of privacy or prior knowledge of the invasion and rule whether the invasion reaches the substantial or serious level.[65]

---

54. Pardee, *supra* note 39, at 1267.

55. *E.g.*, Bally vs. Northeastern Univ., 532 N.E.2d 49, fn 5 (Mass. 1989) (declining to decide whether the statute reaches an attempted invasion of privacy); French v. United Parcel Service, Inc., 2 F. Supp. 2d 128, 132 (D. Mass. 1998) (finding complaint fails to allege UPS attained private information); Cort v. Bristol-Myers Co., 431 N.E.2d 908, 914 (Mass. 1982) (suggesting there was no invasion of privacy because questionnaire not completed) (Abrams, J., concurring).

56. Transamerica Ins. Co. v. KMS Patriots, L.P., 752 N.E.2d 777, 783 (Mass. 2001) (finding there was nothing which could be interpreted as privacy violation).

57. 567 N.E.2d 912 (Mass. 1991).

58. *Id.* at 913. The plaintiff-lawyer received three to five business oriented phone calls throughout the year. *Id.* The calls did not disrupt his way of doing business. *Id.* He sued claiming that the telephone calls were a violation of his solitude and he wanted to be left alone. *Id. at* 914.

59. *Schlesinger*, 567 N.E.2d at 914.

60. *Id.* (using a search and seizure as an example of a reasonable violation of privacy).

61. *Id.*

62. MASS. GEN. LAWS ch. 214, § 1B (2000).

63. Ellis v. Safety Insurance Co., 672 N.E.2d 979 (Mass. 1996).

64. Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149 (Aug. 28, 1997).

65. *E.g.*, Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 567 N.E.2d 912 (Mass. 1991); O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146 (Mass. 1990); *Skelley*, No. 95-2512, 1997 Mass. Super. LEXIS 149 at *21.

In addition to holding there are only two causes of action within the Privacy Statute,[66] the Schlesinger court found the telemarketing calls to be neither substantial nor serious as an intrusion.[67] The Court looked at several factors to make that determination: the frequency of calls, the length of the average call, the intent behind the calls, and whether the calls disrupted the lawyer's activities.[68] The Court concluded that the solicitations which occurred three to five times per year, were short, were business related, and did not disrupt the plaintiff's business.[69] Thus, they did not reach the serious or substantial level required.[70] While the Court explained why this particular holding applies only to the business context, it is easy to see how the court might find differently in a non-business case.[71]

In a business context, the Supreme Judicial Court ruled that a police cadet's required urinalysis did not satisfy the statute's serious or substantial standard.[72] First, the Court dismissed the plaintiff's three separate causes of action argument.[73] Under the circumstances, the Court determined the intrusion was not serious or substantial and therefore did not violate the plaintiff's right to privacy under the Privacy Statute.[74] In a similar Superior Court decision, the court upheld the defendant's interference because the employer's legitimate business interest outweighed the reasonableness of requiring the employee to disclose private facts.[75]

In a non-business setting, the Superior Court found a serious or substantial

---

66. *Schlesinger*, 567 N.E.2d at 914 (describing Court's conclusion of only two causes of action, not three within the Privacy Statute).

67. *Id. at 915.*

68. *Id.*

69. *Id.*

70. *Id.*

71. *Id.* (detailing explicitly why in a business setting, this is not a violation). If the calls were numerous, unreasonably long, and disrupted the plaintiff, the court could find that it reached the level of serious or substantial. Weld v. CVS, No. CIV. A. 98-0897F, 1999 WL 494114 *1 (Mass. Super. June 29, 1999) (confirming that in other circumstances, this could turn into a serious or substantial violation), *aff'd* , Weld v. Glaxo Wellcome Inc., 434 Mass. 81 (2001).

72. O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146 (Mass. 1990) (dismissing the violation of privacy claim). The cadet signed an agreement to submit to an unannounced urinalysis when ordered to do so. *Id.* at 1148. The academy later required the cadet to submit to a urinalysis. *Id.* After detecting cocaine in his urine, the academy dismissed the cadet. *Id.* The cadet sued alleging a violation of his right to privacy. *Id.* at 1147. *See also* Byrne & MacMillan v. MA Bay Transp. Auth., 196 F. Supp. 2d 77 (D. Mass 2002) (using the balancing test to determine whether a violation of privacy occurred).

73. *O'Connor*, 557 N.E.2d at 1148. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 567 N.E.2d 912, 914 (Mass. 1991).

74. *Id.* at 1151. The circumstances looked at included the consent order that the cadet had signed. *Id.*

75. Williams v. Brigham & Women's Hospital, No. 00-1546A, 2002 Mass. Super. LEXIS 52 *1, *22 - *23 (2002). The employer was investigating an employee for possible check fraud. *Id.* at *7. The employer asked about the employee's whereabouts on a particular day. *Id.* The employee revealed that she had an abortion on that day. *Id.* The employee was terminated but never charged with a crime. *Id.* at *10-*11. The employee sued under the Privacy Statute alleging a violation of her privacy because she was accused of a crime she did not commit, terminated from her position, and forced to reveal personal information about her abortion. *Williams*, 2002 Mass. Super LEXIS 52 at *22.

intrusion when parents sent a letter, including a teacher's personal information, to all the other parents of children enrolled at a school.[76] The letter contained information obtained from a Department of Social Services ("DSS") file and an official personnel file.[77] The court found that recipients of the letter could determine the identity of the teacher even though the letter did not specifically name him.[78] The writers seriously or substantially invaded the teacher's privacy because his identity could be determined.[79] In addition, releasing information from a confidential DSS report and personnel file, which by their nature contains personal information, reaches the serious or substantial level.[80] There is a high expectation of privacy in regards to a personnel file or DSS report.[81]

C. Unreasonable Interference

The next step of the test inquires whether the intrusion is unreasonable under the circumstances.[82] The courts use a balancing test to determine whether an intrusion is unreasonable.[83] The test balances the seriousness of the interference against the public's interest in that private information.[84] An unreasonable interference with privacy occurs when the interference goes beyond what is necessary under the circumstances.[85]

The courts recognize that not every intrusion is actionable, and accepts some intrusions as a part of life.[86] For example, a legitimate business interest can make an intrusion reasonable and therefore not actionable.[87] In this context, however, no recognized business interest privilege exists.[88] In this respect, the courts use a balancing test to determine whether there are legitimate business interests allowing a reasonable disclosure of personal information.[89] The Superior Court applied an expanded test into non-employment realms regarding whether there is a "legitimate countervailing interest" which makes disclosure

76. Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149, *1, *21 (Aug. 28, 1997).

77. *Id.* at *6.

78. *Id.* at *20-21.

79. *Id.*

80. *Id.* at *21.

81. *Skelley*, 1997 Mass. Super. LEXIS 149 at *21.

82. *Id.* at *21 (finding a serious or substantial violation occurred, then analyzed whether violation was unreasonable).

83. Pardee, *supra* note 39, at 1267.

84. *Id.*

85. *Id.*

86. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc, 567 N.E.2d 912, 915 (Mass. 1991).

87. Bratt v. Int'l Bus. Machs. Corp., 467 N.E.2d 126, 135 (Mass. 1984) (confirming the business legitimacy weighing test). The Massachusetts Court of Appeals asked the Supreme Judicial Court to certify answers to questions regarding the Privacy Statute. *Id.* at 128.

88. *Id.* at 135.

89. *Id.*

reasonable under the circumstances.[90]

In *Cort v. Bristol-Myers Corp.*,[91] the Supreme Judicial Court used the balancing test to determine whether a company could require employees to fill out a personnel questionnaire without violating their right to privacy.[92] The Court began by explaining that the higher the level of an employee, the more that employee is required to disclose and concluded that these employees, as medical supply salesmen, were in the middle of this spectrum.[93] The Court found the most personal section was appropriate, not intrusive, under the circumstances.[94]

D. High Expectation of Privacy

As mentioned previously, the courts consider whether a person has a "high expectation of privacy" when determining whether an invasion of privacy constitutes an unreasonable and serious or substantial intrusion.[95] By engaging in certain activities, one can lower the high expectation of privacy to a point that a violation is inactionable.[96] It is a factual question whether a person has given up his expectation of privacy.[97] Prior knowledge,[98] privileged disclosure,[99] public figure status,[100] or public facts[101] can lower this high expectation. The plaintiff's actions reduce this usually high expectation and the invasion is not actionable as it does overcome the substantial or serious threshold, nor is it an unreasonable intrusion.[102]

In both O'Connor[103] and Cort,[104] the Court considered the prior knowledge of

---

90. Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149 at *21 (Aug. 28, 1997) (citing *Bratt*, 467 N.E. 2d at 134-35). The court ultimately determined there was a material dispute on the issue of reasonableness to be determined at trial. *Id.* at *22.

91. 431 N.E.2d 908 (Mass. 1982).

92. *Id.* at 914. The company required their employees to fill out a questionnaire that covered subjects such as physical data, extra-curricular activities, medical questions, memberships and personal goals. *Id.* at 913. Several employees either refused to answer or gave flippant responses to the questions. *Id.* at 913, n.10 and n.11.

93. *Id.* at 913.

94. *Id.*

95. *Skelley*, No. 95-2512, 1997 Mass. Super. LEXIS 149 at *21.

96. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc, 567 N.E.2d 912, 915-16 (Mass. 1991). Peckham v. Boston Herald, Inc., 719 N.E.2d 888, 891 (Mass. 1991).

97. *Peckham*, 719 N.E.2d at 891.

98. O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146, 1151 (Mass. 1990) (finding cadet could not have a high expectation of privacy if he signed consent form). *Cort*, 431 N.E.2d at 913 (using fact that they had previously filled out questionnaire to find prior knowledge).

99. *See* Bratt v. Int'l Bus. Machs. Corp., 467 N.E.2d 126 (Mass. 1984).

100. *Peckham*, 719 N.E.2d at 893-94 (noting father known in the community leading to a newsworthiness dismissal).

101. *See* Chase v. First Parish Church, No. 98-1063, 2000 Mass. Super. LEXIS 36, *1 (Feb. 3, 2000).

102. Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149, *1 (Aug. 28, 1997).

103. O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146, 1151 (Mass. 1990).

104. Cort v. Bristol-Myers Co., 431 N.E.2d 908, 913 (Mass. 1982).

the invasion when dismissing the claim. In both cases, the individuals knew that future intrusions could occur.[105] One cannot plead invasion of privacy if he has, in any way, consented to the invasion.[106]

The Court also recognized disclosure of some personal information as privileged.[107] An employee was suing his employer based on, among other things, disclosure of medical information to other managers.[108] The Court found that disclosure of medical information, when it pertains to the employee's ability to perform his job, is privileged and thus inactionable.[109] In these types of situations, the Court uses the balancing test to determine the extent of the privacy and the privilege.[110]

Newsworthiness can be a factor in determining whether a published report is a violation of the right to privacy.[111] In such a case, the Massachusetts Appeals court used the reasoning of the Restatement and analyzed the question based upon what the community standards were.[112] The court identified several factors to find that the article was newsworthy and therefore not actionable.[113]

An intrusion is inactionable if the facts are already in the public domain, regardless if the person is a public figure.[114] A deaf woman sued several parties based upon two exchanges.[115] The first involved dissemination of information that was already in the public domain but as previously stated, there is no liability for disseminating public information.[116] Even though the information was very private to the woman, her deafness was known to the public.[117] In addition, she revealed the information herself to the class.[118] One who discloses private facts does not have a violation of privacy.[119]

---

105. *Id.* (finding that the employees completed a similar questionnaire when they were hired); *see also O'Connor*, 557 N.E.2d at 1151 (stating that the cadet signed an agreement stating future drug tests may occur).

106. *See Cort*, 431 N.E.2d 908; *see also O'Connor*, 557 N.E.2d 1146.

107. Bratt v. Int'l Bus. Machs. Corp., 467 N.E.2d 126, 135 (Mass. 1984).

108. *Id.* at 135 (using business interest weighing test to find employer had right to disclose personal information about employee).

109. *Id.* at 133 (explaining privilege exists and privilege can be lost by certain behavior).

110. *Id.* at 135 (balancing the business interest versus the intrusion of the employee's privacy).

111. Peckham v. Boston Herald, Inc., 719 N.E.2d 888 (Mass. 1991). A man sued a newspaper after it published details about a paternity suit against him and reported the mother may have to go on welfare to support herself because the father was not paying child support. *Id.* at 890–91 (describing article in full detail).

112. *Id.* at 893.

113. *Id.* at 894. The identified factors were the following: the father's role in the community, whether the subject matter was of a general public interest, and the central conflict of the situation being a public event, a judicial proceeding. *Id.* at 893-94.

114. Chase v. First Parish Church, No. 98-1063, 2000 Mass. Super. LEXIS 36 (Feb. 3, 2000).

115. *Id.* at *9. The first suit was based on two Sunday school teachers pressuring her to reveal information about her deafness and a childhood misdiagnosis. *Id.* at *3.

116. *Id.* at *9. *See* Jones v. Taibbi, 512 N.E.2d 260 (Mass. 1987) (finding arrest part of a public record and therefore not actionable as invasion of privacy). Once again, the court points to the Restatement for a discussion of public facts. *Id.* at 269-70.

117. *Chase*, 2000 Mass. Super. LEXIS at *9.

118. *Id.* at *12.

119. *Id.* at *13 (referencing *Cort*, 431 N.E.2d at 914 (Abrams, J., concurring)).

In the second instance, the same woman sued based on additional self-revelations, as well as the public display of a minister mocking her.[120] Once again, the Superior Court found this was already public information.[121] Several people saw the original incident that she confessed to and thus the public scene was not an intrusion.[122] There is no high expectation of privacy if others already have knowledge of the situation.[123] Similarly, the minister mocked her in a public location with other people able to freely observe the public exchange.[124]

As discussed above, activities that occur in a public place cannot constitute an intrusion.[125] When a newspaper publishes a photograph of persons lined up to collect unemployment benefits, no cause of action exists for violating the right to privacy for one of those in line.[126] The court references the Restatement as the reason behind why a picture taken on a public street is different from one taken in a private place.[127]

In an invasion of privacy case against a private investigator, the court broke down the alleged intrusion into four separate categories.[128] The Superior Court dissected what the difference is between public and private and examined technological advances by comparing an intrusion using the naked eye with an intrusion using enhanced vision techniques.[129] A violation may occur where there is a reasonable expectation of privacy.[130] There is a reasonable expectation of privacy inside, where one would need enhanced vision to be able to see.[131] The court found that even though enhanced vision is becoming more commonplace, it is still not reasonable to expect someone is watching you while you are inside your home.[132] The court logically applied the difference in

120. Chase v. First Parish Church, No. 98-1063, 2000 Mass. Super. LEXIS 36, *8 (Feb. 3, 2000). The plaintiff herself revealed to a class that when she was younger another child had to help her recite her lines during a school play. *Id.* In the second instance, a minister mocked her in front of others for wearing an enhanced hearing device. *Id.*

121. *Id.* at *10.

122. *Id.* The play in which she needed help from another student was a public activity. *Id.*

123. *Chase*, 2000 Mass. Super. LEXIS 36 at *10.

124. *Id.* at *11.

125. *See* Cefalu v. Globe Newspaper Co., 391 N.E.2d 935. *See also* DiGirolamo v. D.P. Anderson & Assoc., Inc., No. 97-3623, 1999 Mass. Super. LEXIS 190 at *1 (May 1999).

126. *Cefalu*, 391 N.E.2d at 939. Having a picture taken of you in public is not a violation. *Id.*

127. *Id.*

128. *DiGirolamo*, 1999 Mass. Super LEXIS 190, at *5. The categories are the following:
1) to look through someone's window into her apartment with the naked eye; 2) to look at someone with the naked eye when she walks out onto a balcony; 3) to photograph, videotape, or look at someone with some degree of enhanced vision, such as a telescopic lens, when she walks out onto a balcony; [and] 4) to photograph, videotape, or look at someone with enhanced vision while she remains inside her home.
Id. at *5-6.

129. *Id.* at *7-10 (stating society's expectation of privacy does not diminish with advancing technology).

130. *Id.* at *15-16. There is no reasonable expectation of privacy while outside on a balcony. *Id.*

131. DiGirolamo v. D.P. Anderson & Assoc., Inc., No. 97-3623, 1999 Mass. Super. LEXIS 190 at *10 (May 1999).

132. *Id.*

standards between enhanced and normal vision because the court needed to define a bright line rule to notify investigators about what practices are legal.[133]

A court uses the multiple factors discussed above to determine if a violation of privacy occurred.[134] The Federal District Court of Massachusetts used numerous factors, that several persons were present and the incident was not highly personal or intimate in nature, to determine it was public even though the incident occurred at a private residence.[135] The court then went on to use the balancing test to find the employer had a legitimate business reason for wanting information about the incident.[136] Accordingly, seeking that information was not a violation of the employee's privacy.[137]

IV. COMPUTER TECHNOLOGY

In the past, a computer user only had to worry about hackers invading a computer or employers watching what s/he did on the computer.[138] Now, suspicious spouses and lovers are filling the adultery discussion chat rooms with conversations about which spyware is best to catch an on-line cheating spouse.[139] From downloading a hard drive to see what the user saved to the computer to actually installing software that records all of a user's keystrokes, the technology to spy on each other is easily available and is a detriment to the right to privacy.[140]

A. E-Blaster

If a jealous husband has access to his wife's computer, just once, he can install software that would record every keystroke she had typed and every web site she had visited and have that information sent to him via e-mail every thirty minutes.[141] For less than one hundred dollars, installing this software provides

133. *Id.* at *7. *See* Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 567 N.E.2d 912, 915 (Mass. 1991) (reasoning courts need to file decisions which are practical and capable of reasonable enforcement).

134. French v. United Parcel Serv., Inc., 2 F. Supp. 2d 128 (D. Mass. 1998). There was an alcohol related incident at the home of an employee, which involved other employees, resulting in an injured employee going to the hospital. *Id.* at 130. The vigorous investigation and subsequent suspension because of the incident caused the employee to become depressed. *Id.* The employee charged that the company violated his privacy by requiring disclosure of the facts of the incident, which he considered private. *Id.* at 131.

135. *Id.*

136. *French*, 2 F. Supp. 2d at 131.

137. *Id.* The employer's business interests outweighed the employee's privacy interest because of involvement of the supervisor, the alcohol abuse, and all the participants were employees. *Id.*

138. Bill Wallace & Jamie Fenton, Cable News Network (CNN), *Analysis: Your PC could be watching you*, *at* http://www.cnn.com/2000/TECH/computing/11/15/desktop.tracker.Idg/index.html (analyzing different types of spyware on the market).

139. Libby Copeland, *Cyber-Snooping into A Cheating Heart*, THE WASHINGTON POST, Aug. 8, 2000 at C01, http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A52154-2000Aug7 (discussing marriage break-up after suspicious husband installed spyware and "caught" wife cheating).

140. See discussion, *infra* Part IV(A) and accompanying notes 141-80, (discussing finding a computer using cheating spouse or companion).

141. Copeland, *supra* note 139, at C01. There are many companies that publish computer monitoring

an easy opportunity to ascertain her computer activity.[142] Spyware, also known as "adulteryware," has become a boon to the spying industry.[143]

Spector initially marketed E-Blaster to parents as a way to keep an eye on their children's on-line activities.[144] A short time later, it became apparent people were using it as a tool to catch cheating lovers.[145] Currently half of the software's sales are for monitoring spouses while only twenty percent of sales of the software are for monitoring children.[146]

E-Blaster has the capability of monitoring all of one's computer keystrokes, including passwords and deleted words, and can either store the information on the computer for later retrieval or send it to a remote site, such as another computer.[147] The purchaser installs the software and while it runs behind the scenes, a computer user uses the computer in her normal way, which may include an e-mail or chat session with a lover, unaware of the monitoring.[148] There are programs that work as a defense against these spying programs but continuing improvements to the spyware deem the defense programs almost useless.[149]

B. Internet Cookies

In addition to worrying about who is monitoring computer use, one must be aware of who is monitoring the sites he visits on the World Wide Web.[150] Cookies are unique data stored on a computer after one visits a website.[151] A common example of a cookie's function is when a user enters a password protected website and signs in with a name and password.[152] When he returns to that site, his password is already there and he can enter the site directly

---

software. *Id.* The site http://www.eblaster.com is home to the most well known cyber spying software.

142. Copeland, *supra* note 139, at C01; *see also* http://www.eblaster.com (advertising Spector software for $99.95); a www.google.com search, in April 2002, using "cheating spouse" brought up 2,610 websites, "cheating husband" found 4,380 and "cheating wife" brought up almost 33,000 sites!

143. Wallace & Fenton, *supra* note 138 (quoting E-Blaster spyware company spokesperson as saying approximately fifty percent of sales are for monitoring spouses). *See* http://www.spectorsoft.com/products/SpectorPro_Windows/customers.html for users personal stories.

144. Copeland, *supra* note 139, at C01.

145. *Id.* (detailing letter from wronged fiancée). Prudence, another software targeted towards parents watching their children, stopped promoting the software altogether when it became apparent that spouses were using the software to catching cheaters instead. *Id.*

146. Wallace & Fenton, *supra* note 138 (quoting Doug Fowler, Spectorsoft Chairman, saying they sell "about 10 times what it was a year ago – more than 7,000 sales overall").

147. Copeland, *supra* note 139, at C01.

148. *Id.*

149. Michael K. McChrystal, ET AL., *Carnivores, Cyber Spies & the Law*, 74 WIS. LAW. 14, 16 (Feb. 2001) (discussing technology as a threat to data privacy and security).

150. Anick Jesdanun, ABC News, *Privacy Predicament. Report: Net Users Take Few Privacy Precautions*, *at* http://www.abcnews.go.com/sections/tech/DailyNews/pewprivacystudy000821.html (quoting a poll finding eighty-six percent of online users are "very concerned" or "somewhat concerned" about privacy online). Of those answering the poll, only ten percent have their computers set up to reject cookies. *Id.*

151. Inna Fayenson, *'Cookies' Challenge Meaning of Privacy*, 226 N.Y. L.J., No. 93, s10 (Nov. 13, 2001).

152. *Id.*

without having to re-type the information.[153] Some cookies even track the searches he performs and relates that information back to the site.[154] This scenario raises the most concern among people trying to guard their privacy because the site keeps track of their clicking activity.[155]

Web users have tried suing companies that use cookie technology based upon federal and state claims.[156] Users have sued DoubleClick because of their web advertising practices.[157] DoubleClick, the Internet's largest advertising service, bought a huge database of off-line consumer information.[158] Then, the company altered its privacy statement deleting the language that personal information would not be matched with personal information gathered online.[159] Consumers alleged DoubleClick would combine its on-line database with its new offline consumer profiles to create a huge database matching users online activities with off-line personal information.[160] After the Federal Trade Commission instigated an investigation into whether the collection comprised an unfair or deceptive trade practice, DoubleClick backed down and declared it would not combine the information until attaining a privacy standard.[161] *In re DoubleClick Inc. Privacy Litigation*,[162] a class-action suit was unsuccessful when the court ruled against their federal claims and then dismissed their state claims of common law invasion of privacy because of lack of jurisdiction.[163]

One option to prevent sites from depositing cookies to your computer is to disable your computer's ability to accept them.[164] A battle between computer

153. *Id. See* http://www.yahoo.com or http://www.nytimes.com for examples of sites that use cookies allowing you to enter the site without having to continue signing your user name and password each time. A recent visit to my laptop's cookie folder revealed over 130 cookies. Some addresses were recognizable (default@nytimes) while others were not (default@S0014-01-2-16-217494-54117[2].txt). Still others were cookies from sites not visited (default@sexhound). In addition to being a nuisance, these cookies took up memory space on the hard drive (29.7KB).

154. These cookies are also known as third-party cookies or spyware. See www.lavasoft.com for a site explaining spyware and offering free downloadable software (Ad-Aware) that combats spyware by detecting and deleting it from your computer.

155. Fayenson, *supra* note 151.

156. Peter Brown, *Online Privacy in the U.S.: Legislation, Cases and Industry Standards*, 637 PRACTISING LAW INSTITUTE: PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES, 131, 149 (Feb. – Mar. 2001) (citing DoubleClick case, RealNetworks case and Avenue A/MatchLogic case as federal privacy related cases in the system). The courts have subsequently dismissed all three of these cases: In Re RealNetworks, Inc. Privacy Litigation, 2000 US Dist. LEXIS 1458 (Feb. 10, 2000) *dismissed* 154 F. Supp. 2d 497 (S.D.N.Y. 2001)); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (D.C. Cir. 2001).

157. In re DoubleClick Inc. Privacy Litigation, 154 F. Supp. 2d 497, 505 (S.D.N.Y. 2001).

158. *Id.* DoubleClick bought the valuable database company for more than one billion dollars. *Id.*

159. *Id.*

160. *Id.*

161. *DoubleClick Inc.*, 154 F. Supp. 2d. at 505. *See also* Donna Goodison, *Web Ad Service Ends Privacy Flak: DoubleClick Settlement Changes Policy*, THE BOSTON HERALD, Aug. 27, 2002, at 33 (announcing settlement agreement between DoubleClick and ten state attorneys general). DoubleClick paid $450,000 under the settlement agreement for costs and consumer education. *Id.*

162. 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

163. *Id.* at 526. Computer users brought the suit based upon Federal statute claims. *Id.*

164. Barry D. Bayer, *The Price of Privacy: No-Cost Web Security*, 223 THE LEGAL INTELLIGENCER 119

users and sites developed over whether sites should continue to use opt-out or should change to opt-in.[165] Currently if the user does not want a site to drop cookies, he needs to opt-out of the program since the site presumes he wants to participate.[166] Consumer groups want the sites to change their opt-out policy to the opt-in policy, thereby asking the user for permission before depositing cookies on the system.[167]

Senator Edwards (D-N.C.) introduced a bill to support the disclosure of spyware practices in 2001.[168] He believes spyware is a shocking example of the eroding right to privacy.[169] Disclosure in a "clear and conspicuous notice" is an important aspect of the bill.[170] The bill is still in committee at this time.[171]

C. Hard Drives

In addition to keeping an eye on a computer for spyware and cookies, the user needs to be aware that hard drives may also contain private information.[172] Someone can take advantage of private information on a hard drive simply because the user does not know the private material is there.[173] Even if the user thinks his information is password protected and someone accesses it without permission, he does not have an actionable claim.[174] The test requires the existence of a reasonable expectation of privacy.[175]

A husband filed a common law invasion of privacy action and wiretap violation against his estranged wife because she accessed e-mails he had stored on the home computer to use in a custody battle.[176] For the invasion of privacy

---

(explaining how to disable cookies through web browser). This is, however, not an easy solution. Disabling the cookies function prevents a user from accessing sites. The free e-mail site http://www.yahoo.com requires cookies to use their e-mail. The sports site http://www.espn.com has a "lite version" for users not accepting cookies. Changing the setting to "prompt" for cookies creates problems as well. Requests to deposit a cookie inundate a user when entering almost every website, as well as when navigating the site.

165. Brock N. Meeks, MSNBC, *Congress targets privacy issues*, *at* http://www.msnbc.com/news/498459.asp. Opt-in requires the user to actively turn on the cookie. *Id.*

166. *Id.*

167. *Id.*

168. Spyware Control and Privacy Protection Act of 2001, S. 197, 107th Cong. § 2 (2001). The bill went to the Committee on Commerce, Science, and Transportation on Jan. 29, 2001 and no action has been taken since then. *Id.*

169. Brian Krebs, *Senator John Edwards Introduces 'Spyware Control Act'*, *at* http://grc.com/spywarelegislation.htm.

170. *Id.*

171. *Id.*

172. White v. White, 781 A.2d 85 (N.J. Super. Ct. Ch. Div. 2001) (dismissing husband's claim against estranged wife for intrusion when she downloaded hard drive of computer and found love letters).

173. *Id.* at 92.

174. *Id.*

175. *Id.* (reinforcing objective test for reasonable expectation of privacy).

176. *Id.* at 86-87. New Jersey does not have a statutorily protected right to privacy, but the courts have recognized the common law theory. *White*, 781 A.2d at 91. Although separated, the husband and wife continued to live in the same house. *Id.* at 87. The husband slept in the sunroom, where the family computer was stored; both the room and the computer were accessible to everyone in the household. *Id.* The wife became suspicious about her husband's activities after she allegedly found a letter from the husband's

count, the court focused on the location of the computer to find the intrusion was not highly offensive to the reasonable person.[177] The court found the husband did not have a subjective expectation of privacy because the entire family had access to the room and computer.[178] Furthermore, the wife's actions were not highly intrusive because she was looking for evidence that her husband was cheating.[179] The court concluded by analogizing rummaging through a computer's hard drive with rummaging through a file cabinet to rule that seizure of the e-mails was not an invasion of the husband's privacy.[180]

V. MASSACHUSETTS STATUTE ANALYSIS

In Massachusetts, there are no computer-based invasions of privacy cases.[181] A broad statute empowers the court to keep current with changing technology.[182] The Massachusetts courts have interpreted the broad privacy statute as granting permission to decide privacy claims on a case-by-case basis.[183] The courts balance relevant factors, consider societal values and determine a rule that is easily enforceable.[184]

A. Hard Drives

The Massachusetts courts may follow the New Jersey court's analysis if confronted with the issue of a spouse downloading material from any

girlfriend, so she hired a private investigator who, as part of the investigation, downloaded the computer's hard drive. *Id.* at 87. The husband disputes the allegation that the wife found the letter lying around, saying he hid it from plain view. *Id.* The hard drive housed e-mails, both sent and received and images the husband saved to his America Online file cabinet thinking they were password protected. *White*, 781 A.2d at 87. America Online's personal file cabinet actually saves to the hard drive. *Id.* at 87-88. Since it is the hard drive and not America Online, you do not need a password to access saved material. *Id.* at 88. The wife wanted to use these e-mails as evidence against her husband in the custody battle. *Id.* at 88. The court first discussed inter-spousal immunity, and then dismissed the violation of the N.J. Wiretap Act claim. *Id.* at 88-91.

177. *E.g.*, *White*, 781 A.2d at 91-92; Molly J. Liskow, *Wiretap Act, Husband's Privacy Not Violated by Wife's Retrieval of E-Mail on "Family Computer,"* 10 N.J. L. REV. 41, (Oct. 2001); Stephanie Levy, *Retrieving Spouse's E-Mail Did Not Violate State Wiretap Law*, TRIAL, Jan. 2002 (analyzing the wire tap aspect of the case).

178. *White*, 781 A.2d at 92 (citing husband's claim he knew not to leave letter from girlfriend in plain view). In addition, whether there is a reasonable expectation of privacy is objective, so the fact that the husband went to great lengths to protect his e-mails does not weigh into the discussion. *Id.*

179. *Id.* New Jersey's Appellate Division had already ruled in a previous case that the wife had a legitimate reason to look through the file cabinet for evidence of unfaithfulness. *Id.*

180. *Id.*

181. At the writing of this article, there are numerous cases that discuss the Privacy Statute in the context of a violation but there have not been any cases with the narrow focus of computer generated privacy violations.

182. Pardee, *supra* note 39, at 1250 (claiming statute has to be broad and flexible enough for changing times).

183. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc, 567 N.E.2d 912, 915 (Mass. 1991).

184. *Id.; see also* INTERIM REPORT OF THE SPECIAL COMMISSION ON ELECTRONIC EAVESDROPPING, *supra* note 37 (report confirms legislature, in 1967, wanted to let judiciary determine scope of privacy law).

accessible computer.[185] First, the Massachusetts legislature intended the statute to mirror the delineations of the Restatement,[186] much like New Jersey.[187] Second, the court may analyze the circumstances and manner of disclosure to determine if a violation has occurred.[188] Like the New Jersey court, a Massachusetts court may allow the downloading of information from the hard drive if a spouse were looking for information about an on-line affair because the circumstances dictate that the hard drive is where one would find that information.[189] Third, the court would use the subjective standard to determine if the spouse subjectively had a reasonable expectation of privacy when other members of the household have access to the computer.[190] Therefore, a future Massachusetts court could rely on those findings that the spouse did not have a reasonable expectation of privacy and find there is no intrusion.[191]

B. Installing Spyware

While downloading a hard drive and installing E-Blaster software may seem similar enough, there are enough differences to lead the Massachusetts courts to possibly find an invasion of privacy. The court would probably find that a software intrusion reaches the level of serious or substantial and unreasonable intrusion necessary.[192] If the computer invader does not have a right to access the computer to install the software, the court should find that the computer user has a high expectation of privacy.[193] If the court finds there is a legitimate business interest[194] or consent,[195] it could rule the claim is invalid.

The court will look at the factors surrounding the alleged invasion, including how the user gained access to the computer to install the software, to determine if it reaches the level of a serious or substantial intrusion.[196] The court will take into consideration the location of the computer when a person installed the spyware, whether other users had free access to the computer and whether the

185. This analysis does not take into account any rulings on inter-spousal immunity that may apply.

186. *Pardee*, *supra* note 39, at 1252 (citing comment section of Privacy Statute). Massachusetts has an appropriation statute. MASS. GEN. LAWS ch. 214 § 3A (2000).

187. *White*, 781 A.2d at 91. *See also Pardee*, *supra* note 39, at 1252 (discussing commentator's comment that statute is to be interpreted as it is interpreted by the Restatement). Pardee disagrees with that comment and argues that the statute should not be limited in that way. *Id.* at 1252–53.

188. Peckham v. Boston Herald, Inc., 719 N.E.2d 888, 891 (Mass. 1991.

189. White v. White, 781 A.2d 85, 92 (N.J. Super. Ct. Ch. Div. 2001).

190. *Id.* at 91-92 (finding computer in a public place as to other members accessing it).

191. DiGirolamo v. D.P. Anderson & Assoc., Inc., No. 97-3623, 1999 Mass. Super. LEXIS 190 at *11 (May 1999) (explaining no reasonable expectation of privacy when in plain view). *White*, 781 A.2d at 91-92 (stating computer was in a room accessible to all therefore no reasonable expectation of privacy existed).

192. Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149 at *21 (court will first find whether serious or substantial then whether it is unreasonable).

193. *DiGirolamo*, 1999 Mass. Super. LEXIS 190 at *1.

194. Bratt v. Int'l Bus. Machs. Corp., 467 N.E.2d 126, 135 (Mass. 1984).

195. O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146, 1151 (Mass. 1990). Consent will preclude an invasion of privacy claim. *Id.*

196. Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc, 567 N.E.2d 912, 915 (Mass. 1991).

user believed he was the only user.[197]

With an unauthorized download of the software, the computer user does not have knowledge that someone is monitoring his keystrokes and activities.[198] The installer receives all information secretly by e-mail, as frequently as every thirty minutes.[199] The software records every keystroke by the user, including those words or phrases deleted.[200] Furthermore, the software automatically captures the user's keystrokes without his/her knowledge.[201] The court could find a pattern of harassment that the court in Schlesinger did not.[202] It could also find that installing software without a user's consent reaches the level of serious or substantial that the O'Connor[203] court did not find.

The software captures every keystroke and reports it to the installer, even deleted ones; while the user thinks he deleted text, the installer knows the user typed it.[204] Based upon the arguments in their article, Warren and Brandeis may find the dissemination of thoughts the user deleted before publishing to anyone an intrusion upon the privacy of the user.[205] A user does not have the ability to deny access to his privacy when he does not know there is software that captures his deleted thoughts.[206]

A court could find an unreasonable intrusion by using the balancing test that weighs the seriousness of the offense against the importance of the public interest.[207] Living in the community does not authorize ex-spouses or shunned lovers to see everything a computer user types and deletes as if he could read his/her thoughts.[208] A Massachusetts court may look to see what other acceptable activities the spouse participated in before installing such intrusive software.[209]

---

197. White v. White, 781 A.2d 85, 92 (N.J. Super. Ct. Ch. Div. 2001) (listing factors to conclude plaintiff did not have a reasonable expectation of privacy).

198. Copeland, *supra* note 139, at C01.

199. *Id.*

200. *Id.*

201. *Id.*

202. *Black's Law Dictionary* defines harassment as "[w]ords, conduct, or action (usu. repeated or persistent) that, being directed at a specific person, annoys, alarms, or causes substantial emotional distress in that person and serves no legitimate purpose." BLACK'S LAW DICTIONARY 721, (7th ed. 1999). *See* Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc, 567 N.E.2d 912, 915 (Mass. 1991).

203. O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146, 1150 (Mass. 1990).

204. Copeland, *supra* note 139, at C01.

205. Warren & Brandeis, *supra* note 7, at 198 (stating common law allows everyone to control how his "thoughts, sentiments, and emotions shall be communicated to others"). Raymond S.R. Ku, *Think Twice Before You Type; The Government's Use of a Keystroke-Monitoring Device in a Criminal Investigation Raises Troubling Privacy Questions*, 163 N.J. L.J. 8 (Feb. 2001) (describing how keystroke monitoring devices monitor thought itself).

206. Pardee, *supra* note 39, at 1258 (arguing privacy is broader than four or five categories and must be defined as denying access).

207. Pardee, *supra* note 39, at 1267.

208. Warren & Brandeis, *supra* note 7, at 198 (asserting common law protects thoughts and how they are communicated to others).

209. DiGirolamo v. D.P. Anderson & Assoc., Inc., No. 97-3623, 1999 Mass. Super. LEXIS 190 at *11

C. Cookies

A Massachusetts court would probably find that depositing cookies on a computer user's hard drive is not a violation of the Privacy Statute.[210] The court would probably find the level of intrusion does not meet the substantial or serious level. A study showed that although fifty-six percent of computer users surveyed did not know what a cookie was, of those who did, only ten percent had their browsers set to reject cookies.[211] The court could view this as a form of consent and find a violation cannot occur if the user consents to it.[212]

Even if the court did find that the invasion reached the substantial or serious level, it would probably not find the invasion to be unreasonable.[213] The court may find this is one of those intrusions that one should expect as part of living in a civilized society.[214] In addition, there is a legitimate business interest in determining the habits of the user for advertising purposes.[215] Finally, a user can "opt-out" of nearly all the programs to disable cookies and prevent information from being transferred back to a company.[216]

VI. CONCLUSION

Regardless of how the legislature wrote the statute, it is now clear that there are only two causes of action under the Privacy Statute. A violation must be a substantial and unreasonable intrusion or a serious and unreasonable intrusion. The court's first step determines whether the violation reaches the serious or substantial level. Then the court looks to whether the violation is unreasonable. It must pass both steps in order to be actionable. Based upon relevant case law, it appears that getting past these two steps in a computer-based invasion of privacy will be very hard.

The courts have set themselves up to have to decide many privacy cases in order to find the bright line where violations occur. By reviewing the claims on a case-by-case basis, the courts have to decide numerous cases to shape the contours of this emerging law. In addition, there are many factors to consider when reviewing privacy cases: prior knowledge, newsworthiness of the

---

(May 1999) (delineating public versus private intrusions). *See also* White v. White, 781 A.2d 85, 92 (N.J. Super. Ct. Ch. Div. 2001) (declaring computer search is not "highly intrusive" because spouse looking for evidence of infidelity) and discussion of *White*, *supra* notes 174-80.

210. MASS. GEN. LAWS ch. 214, § 1B (2000) (stating "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy").

211. Jesdanun, *supra* note 150 (discussing how few users take privacy precautions on-line).

212. *See* O'Connor v. Police Commissioner of Boston, 557 N.E.2d 1146 (discussing how signing an agreement constitutes consent which nullifies a violation of privacy claim).

213. *See* Skelley v. Trustees of the Fessenden School, No. 95-2512, 1997 Mass. Super. LEXIS 149 at *21 (finding a serious or substantial violation occurred, then analyzed whether the violation was unreasonable).

214. Pardee, *supra* note 39, at 1267.

215. *See* Bratt v. Intn'l Bus. Mach. Corp, 467 N.E.2d 126, 135 (Mass. 1984) (using business legitimacy test).

216. *See* discussion *supra* notes 164-67 and accompanying text (describing battle over opt-in versus opt-out).

information, public or private disclosure and whether the information is already in the public realm.

The courts have a baseline statute that declares that a citizen shall have a right against substantial or serious and unreasonable intrusions of privacy. This broad statute allows for expansive judicial interpretation and these interpretations of serious or substantial and unreasonable intrusions will grow with the activities of society. Legislators have the ability to change the statute to reflect the attitudes of society and the citizens of the state, if the court interpretations do not. Massachusetts' legislators took the steps to outline what constitutes an invasion of privacy, rather than relying on judicial interpretation.

Janine H. McNulty