NOTES

CURIOUSER AND CURIOUSER: ARE EMPLOYERS THE MODERN DAY ALICE IN WONDERLAND? CLOSING THE AMBIGUITY IN FEDERAL PRIVACY LAW AS EMPLOYERS CYBER-SNOOP BEYOND THE WORKPLACE

*Cicero H. Brabham, Jr.**

* Information Technology Editor, *Rutgers Law Review*. J.D. Candidate, May 2011, Rutgers School of Law—Newark; M.S./B.S. in Computer Science and W. Burghardt Turner Fellow, Stony Brook University 1994/1991. I dedicate this Note to my wife, Bernadette, for her love, guidance, and support—we did it, babe! In addition, to my children, Briana, Brandon, Bethany, and Bailey, thank you for making every day better than the last. Finally, I would like to thank the Editors and Staff of *Rutgers Law Review*, especially my research editor, Naomi Barrowclough, who pushed me to take the road less traveled when I authored this Note.

> "Recent inventions and business methods . . . have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that what is whispered in the closet shall be proclaimed from the house-tops."[1]

I. INTRODUCTION

Have you ever logged on to a password-protected Web site while at work? If the answer is yes, then you may recall being told by your employer that employees have no expectation of privacy while surfing the Web with their office computers.[2] What if you forgot to log-out and, unbeknownst to you, your employer decides to enter this open door to access your password-protected communications stored on this external Web site? Has your employer now invaded your privacy? The courts are unclear on this issue[3] and what protection, if any, federal law provides.[4]

Under the Federal Stored Communications Act ("Storage Act"), liability extends to any person who "intentionally accesses without authorization a facility through which an electronic communication service is provided; or . . . obtains . . . access to a wire or electronic communication while it is in electronic storage . . . ."[5] Although Congress did not provide a definition of the term "authorization,"[6] federal courts, in interpreting legislative intent, have likened it to

---

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

2. A typical employee handbook "explicitly addresses [Internet] access on company computers." *See, e.g.*, Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548, 552-53 (S.D.N.Y. 2008). For example, it might state that:

> [Internet] users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over *the system*. This includes the use of personal e-mail accounts *on Company equipment. The Company*, in its discretion *as owner of the* [Internet] *system*, reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through *the system*, for any reason, without the permission of any system user, and without notice.

Id.

3. *See* Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 399-401 (N.J. Super. Ct. App. Div. 2009) (analyzing recent case law surrounding the many legal "gray areas" created when employers retrieve personal communications that an employee sent or received through an external application via their company issued computer), *aff'd in part and modified in part*, 990 A.2d 650 (N.J. 2010).

4. *See* Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 129 (2005) (noting that "[c]ourts, legislators, and legal scholars alike have had a very hard time making sense of [the] federal statutes" that govern electronic wired and stored communications).

5. 18 U.S.C. § 2701(a) (2006).

6. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 n.8 (9th Cir. 2002).

the term "consent" found in the Federal Electronic Communications Privacy Act ("Wiretap Act").[7] However, by merely analogizing the two terms, the courts have only increased, rather than simplified, the complexities entangling these two federal laws.[8]

This Note analyzes whether the current, broad interpretation of "consent," which enables employers to monitor internal electronic communications under the Wiretap Act,[9] should equally apply to "authorization" in cases involving external electronic storage brought under the Storage Act. Moreover, it considers the ramifications of allowing employers unfettered access to electronically secured information in a manner that would otherwise be an invasion of privacy under common law.[10]

After a brief introduction of the current issues facing employees concerning the privacy of their personal electronic communications while at work, Part I of this Note reviews the federal law put in place to protect electronic means of communication from unauthorized intrusions. In addition, Part I provides a background of the implied consent doctrine. It considers whether a broad interpretation of

---

7. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *3 (D.N.J. July 25, 2008).

8. *See* discussion *infra* Part IV.

9. Under the consent exception to the Wiretap Act, most employers are exempt from liability for invasion of privacy. *See* Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (holding that it is settled law that the Act "affords safe harbor not only for persons who intercept calls with the explicit consent of a conversant but also for those who do so after receiving implied consent"). The exception states that:

> It shall not be unlawful . . . for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (2006). The authorization exception to the Storage Act provides that:

> [W]hoever . . . intentionally accesses without authorization a facility through which an electronic communication service is provided; or . . . alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided [herein]. . . . [except] with respect to conduct authorized . . . by a user of that service with respect to a communication of or intended for that user.

18 U.S.C. § 2701(a)-(c) (2006).

10. *See* Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 620-21 (3d Cir. 1992) (interpreting Pennsylvania's common law recognition of the tort of "'intrusion upon seclusion'" as meaning "'[o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person'" and applying it in the employment context for a urinalysis test (quoting RESTATEMENT (SECOND) OF TORTS § 652B (1977))).

consent is in line with congressional intent, and examines the extremes courts are willing to go to in order to implement the doctrine. Part II argues against a similar broad reading of the term "authorization" in the face of the existing struggle to define the term within the context of the Storage Act, and suggests specific changes that will transform the Storage Act into the legislation Congress intended. Finally, Part III advocates in favor of upholding the strong public policy of protecting personal privacy rights by proposing judicial restraint in interpreting the Storage Act during the current inconsistencies in applying federal law.

II. EVOLUTION OF THE IMPLIED CONSENT DOCTRINE

The Wiretap Act was initially adopted to govern third-party intercepts of telephone and electronic communications that occur without a warrant.[11] Under "prevailing statutory construction," courts interpret the Act to also extend to an employer's right to monitor employee electronic communications.[12] This is especially true if the employee unambiguously consents to monitoring,[13] and the basis for inquiry is tenuously related to the employment context.[14] Unambiguous consent has not been a necessary threshold before an employer is safe from liability.[15] In many Wiretap Act cases, the courts use circumstantial evidence of an employee's acquiescence to monitoring to find that the employee implicitly consents.[16]

In the seminal case of *Watkins v. L.M. Berry & Co.*, the Eleventh

---

11. Philip L. Gordon, *Job Insecurity?*, 79 DENV. U. L. REV. 513, 513-14 (2002) (discussing how judicial interpretation of the Wiretap Act eradicates statutory provisions that protect privacy in workplace Internet and e-mail use).

12. *Id.* at 515.

13. *See* Watkins v. L.M. Berry & Co., 704 F.2d 577, 581-83 (11th Cir. 1983) (discussing statutory consent exemptions under the Act).

14. *See* O'Connor v. Ortega, 480 U.S. 709, 717 (1987) (holding that "[t]he employee's expectation of privacy must be assessed in the context of the employment relation").

15. *See* Griffin v. City of Milwaukee, 74 F.3d 824, 827 (7th Cir. 1996) (holding that an employee answering phones for her employer had knowledge of possible interception of telephone calls and thus implicitly consented to being monitored).

16. *See* United States v. Rittweger, 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003) (finding that an employee had given his implied consent to his employer's interception of his phone calls where the employer had disseminated a memo and handbooks advising employees "that th[eir] calls were being recorded" and were subject to review); *see also* Jandak v. Brookfield, 520 F. Supp. 815, 824-25 (N.D. Ill. 1981) (upholding consent defense where plaintiff should have known his calls were monitored based on his "training and job situation"); Simmons v. Sw. Bell Tel. Co., 452 F. Supp. 392, 393-94 (W.D. Okla. 1978) (holding that the employee was fully aware of the extent of the monitoring capabilities and deliberately ignored the strong probability of monitoring), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

Circuit Court of Appeals explored the issue of implied consent in cases brought under the Wiretap Act.[17] The court explained, "knowledge of [an employer's] *capability* of monitoring alone cannot be considered implied consent."[18] Nevertheless, when an employee consents to monitoring of their business calls, the employer's permissible zone of consent includes the inadvertent interception of personal calls—even if only for a brief period of time.[19] In short, monitoring an employee's personal calls does not violate the Wiretap Act up to the point when the personal nature of the communication is determined.[20]

Some courts liberally read *Watkins* as expanding the Wiretap Act's safe harbor "depending on the subtleties and permutations inherent in" each case.[21] In *Griggs-Ryan v. Smith*, the First Circuit Court of Appeals held that an employer's zone of consent includes the scope of implied permission based upon the employee's subjective behavior that manifests acquiescence to monitoring.[22] The court explained that:

> [C]onsent inheres where a person's behavior manifests acquiescence or a comparable voluntary diminution of his or her otherwise protected rights. . . . Of course, implied consent is not constructive consent. Rather, implied consent is "consent in fact" which is inferred "from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance." . . . The circumstances relevant to an implication of consent will vary from case to case, but the compendium will ordinarily include language or acts which tend to prove (or disprove) that a party knows of, or assents to, encroachments on the routine expectation that conversations are private.[23]

In the wake of *Griggs-Ryan,* courts have stretched the doctrine of implied consent to further extremes, and reasoned that employers are free from liability if the employee "knew or should have known" that monitoring was possible.[24] In *McLaren v. Microsoft Corp.*, the court rejected a right to privacy claim to stored e-mail messages on a

17. 704 F.2d at 581-82.

18. *Id.* at 581.

19. *See id.* at 582-84.

20. *Id.* at 583-84.

21. Griggs-Ryan v. Smith, 904 F.2d 112, 119 (1st Cir. 1990).

22. *Id.*

23. *Id.* at 116-17 (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)) (internal citations omitted).

24. Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 356 (1995) (noting that many "courts will imply consent when the employee knew or should have known of a policy of constantly monitoring calls").

work computer.[25] McLaren's employment was terminated, allegedly after Microsoft decrypted his password-protected e-mail storage folders.[26] The company investigated McLaren's e-mail activities based upon allegations made against him for sexual harassment.[27] In upholding the trial court's grant of summary judgment to Microsoft, the appeals court held that McLaren had no legitimate expectation of privacy in e-mails that were sent over the company's network, which he knew could be intercepted at any time by his employer.[28] The court also noted that the e-mail messages stored in McLaren's personal folders were first transmitted internally by the company's servers and made available to third parties.[29]

Similarly, in *Griffin v. City of Milwaukee*, the plaintiff operated a telephone switchboard for the Milwaukee police department.[30] She alleged that her employer was illegally monitoring and intercepting her personal telephone calls.[31] In affirming the district court's grant of summary judgment in favor of the employer, the court noted that the plaintiff was informed about the possibility of monitoring "for training, evaluation, and supervision purposes."[32] In fact, she knew her supervisors might monitor her telephone calls at her terminal.[33] Consequently, the plaintiff consented to her employer's monitoring when she used her work phone.[34]

While the need for employers to police employee activities is important,[35] using *Griggs-Ryan's* implied consent reasoning, the courts appear far too eager to carve out exceptions as long as the employer can show a legitimate business purpose for its intrusion.[36] This conclusion is clearly on a collision course with the advancement

25. McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 at *5 (Tex. App. May 28, 1999).

26. *Id.* at *1.

27. *Id.*

28. *Id.* at *4-5.

29. *Id.*

30. Griffin v. City of Milwaukee, 74 F.3d 824, 826 (7th Cir. 1996).

31. *Id.* at 827.

32. *Id.*

33. *Id.*

34. *Id.*

35. Under the tort theories of *respondeat superior* and vicarious liability, employers may face liability for some of the wrongful acts of their employees while at work. Micah Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using* Respondeat Superior *to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 COMPUTER L. REV. & TECH J. 273, 294 (2003).

36. *See, e.g.*, Baggs v. Eagle-Picher Indus., Inc., 750 F. Supp. 264, 272 (W.D. Mich. 1990) (noting that "employers have a right to investigate into areas which would normally be private if the investigation springs from the business relationship").

of modern Internet technologies, which employees utilize simultaneously for personal and business needs.[37]

A. *Does the Current Broad Interpretation of Implied Consent Mean that Nothing is Private on the Internet?*

In today's society, people communicate over the Internet in several ways. Some communications are meant to be public, such as posting a message on a social networking site like Facebook.[38] Others are meant to be private, such as individuals who communicate with personal e-mail accounts or with Internet telephone services.[39] These private communications should be given the same protection as wired phone conversations or letters,[40] but when it comes to the Internet, the courts appear eager to ignore a user's reasonable expectation of privacy.[41]

In extreme cases, when a user engages in e-mail conversations over the Internet, courts have expressed a willingness to find that the user implicitly consents to having his communications recorded.[42] In *State v. Lott*, the Supreme Court of New Hampshire explored the nature and characteristics of electronic mail.[43] Justice Dalianis argued that e-mail is the equivalent of leaving a message on an answering machine.[44] As such, "'a person who sends an e-mail

---

37. *See* Echols, *supra* note 35, at 288.

38. *See* J.S. ex rel. H.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 425 (Pa. Commw. Ct. 2000) (finding no reasonable expectation of privacy in content posted on a public Web site).

39. *See* Peter Svensson, *Skype's Online Phone Calls May Give Wiretappers Fits*, SEATTLE TIMES, Feb. 17, 2006, at D1 (explaining that encrypted phone calls over voice Internet services like Skype are "practically impossible to break by current means").

40. Mail transported via the United States Postal Service is given a high level of protection against unauthorized inspection. *See* United States v. Van Leeuwen, 397 U.S. 249, 251 (1970) (letters and packages are "free from inspection by postal authorities"); United States v. Hernandez, 313 F.3d 1206, 1209 (9th Cir. 2002) ("It has long been established that an addressee has both a possessory and a privacy interest in a mailed package.").

41. The United States Court of Appeals for the First Circuit explained that:

> We believe that the language of the [Wiretap Act] makes clear that Congress meant to give lesser [privacy] protection to electronic communications than wire [or] oral communications. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology. We observe . . . that the language [of the Wiretap Act] may be out of step with the technological realities of computer crimes. However, it is not the province of this court to graft meaning onto the statute where Congress has spoken plainly.

United States v. Councilman, 373 F.3d 197, 203-04 (1st Cir. 2004), *withdrawn and vacated*, 385 F.3d 793, *rev'd en banc*, 418 F.3d 67 (1st Cir. 2005).

42. State v. Lott, 879 A.2d 1167, 1170-72 (N.H. 2005).

43. *Id.*

44. *Id.* at 1171.

message anticipates that it will be recorded. That person thus implicitly consents to having the message recorded on the addressee's computer.'"[45] The court concluded that by using the Internet for communication, "as a matter of law, [one implicitly consents] to the recording of his communications" because recording on a computer is an inherent function in such communications.[46]

With the advent of electronic communication in the workplace, the problem of adopting implied consent becomes even more apparent.[47] Under the doctrine, some courts find that an employee implicitly consents to monitoring based merely on his use of his employer's equipment.[48] The reason usually being that plaintiffs fail to show that they "had an expectation of privacy [in their work e-mail], which was a required element for an invasion of privacy action."[49] Similarly, many employers argue that "[i]f the corporation owns the equipment and pays for the network, that asset belongs to the company, and it has a right to look and see if people are using it for purposes other than running the business."[50]

Although these early electronic privacy cases are not controlling, they are indicative of the lack of judicial response to the monitoring of employees by their employers. The court's inaction should be troubling for most, if not all, employees who use the Internet while at work.[51] In the current economic recession, employers demand more from employees such as longer hours, weekend work, and the loss of vacation time.[52] As a result, being at work consumes most of the average employee's life. The convenience of Web technology allows employees to balance the demands of work with the pressures of their personal lives. If employees feel that their every Internet step is

45. *Id.* at 1171-72 (quoting State v. Townsend, 57 P.3d 255, 260 (Wash. 2002)).

46. *Id.* at 1170.

47. *See generally* Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1898 (1991) (arguing that with "the introduction of computer technology in the workplace" current privacy laws are inadequate in protecting employees from abusive practices).

48. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 98-101 (E.D. Pa. 1996) (holding that even in the absence of a company e-mail policy, employees would not have a reasonable expectation of privacy in their work e-mail).

49. Gantt, *supra* note 24, at 399 (citing Flanagan v. Epson Am., Inc., No. BC007036 (Cal. Super. Ct. Jan. 4, 1991)).

50. Glenn Rifkin, *Do Employees Have a Right to Electronic Privacy?*, N.Y. TIMES, Dec. 8, 1991, § 3, at 8 (internal quotations omitted).

51. *See* Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 440 (Sup. Ct. 2007) ("[T]he effect of an employer e-mail policy . . . is to have the employer looking over your shoulder each time you send an e-mail.").

52. *See generally Employee Morale in US Low: Survey*, REDIFF.COM (Nov. 18, 2009), http://business.rediff.com/report/2009/nov/18/employee-morale-in-us-low-survey.htm (describing increased workloads and strained resources).

tracked and traced, this could lead to increased stress, high blood pressure, depression, and other forms of non-productive reactions.[53] Ironically, this would nullify a few of the justifications for monitoring in the first place.[54]

B. *Making the Case that Implied Consent Should be Narrowly Tailored*

An employer's use of technology to monitor employees is a well-known concept, which in many cases is a pre-condition of employment.[55] Today, with the use of modern electronic surveillance technologies, employers are also able to invade their employees' privacy with little chance of detection.[56] From the employees' perspective, grave privacy concerns are implicated.[57] Unfortunately, legislators have been unable to keep pace with new technology and the "courts seem either unwilling or unable to protect employees from purely electronic invasions of privacy."[58] For example, when interpreting the Wiretap Act, some courts, more often than not, liberally construe the consent exception in favor of the employer's interest.[59]

Breaking from the pack, a growing number of courts reason that the Wiretap Act "expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may

---

53. *See* Bahaudin G. Mujtaba, *Ethical Implications of Employee Monitoring: What Leaders Should Consider*, NOVA SOUTHEASTERN UNIVERSITY, H. WAYNE HUIZENGA SCHOOL OF BUSINESS AND ENTERPRISE, http://www.huizenga.nova.edu/jame/employee monitoring.htm (discussing cyber-loafing and other adverse employee reactions to employer monitoring) (last visited Aug. 23, 2010).

54. One argument for employee monitoring has been that "inappropriate or personal use of e-mail on company time" adversely affects productivity. Echols, *supra* note 35, at 278.

55. Drug and alcohol testing are a very common form of employer-mandated technologically-based intrusion into employee privacy. *See* Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123, 1133-35 (Alaska 1989).

56. *See Fact Sheet 7: Workplace Privacy and Employee Monitoring*, PRIVACY RIGHTS CLEARINGHOUSE, http://www.privacyrights.org/fs/fs7-work.htm (revised June 2010).

57. A major privacy concern is that unlike the Wiretap Act, the Storage Act contains no prohibition against using information obtained in violation of its provisions. *See* Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) ("Because [the Storage Act] prohibits only unauthorized access and not the misappropriation or disclosure of information, there is no violation of [the Act] for a person with authorized access to the database no matter how malicious or larcenous his intended use of that access. [The Storage Act] outlaws illegal entry, not larceny.") (alteration in original). Thus, if a company can show that its agents were acting in contravention to its direct instructions or goals, the company may still be able to use against its employees the information unlawfully obtained. *See id.*

58. Gantt, *supra* note 24, at 346.

59. *See* discussion *supra* Part II.A.

lawfully take place."[60] Furthermore, the Act's protection would be frustrated if "consent could routinely be implied from [the] circumstances."[61] In *Deal v. Spears*, the employer-defendant warned employees that he might start monitoring the phone system in order to reduce the number of employee personal calls made in his store.[62] The employer argued that employee consent should be implied because of his previous warnings.[63] In rejecting the employer's arguments, the Eighth Circuit held that consent should not be "cavalierly implied," emphasizing that employees were only notified that they might be monitored.[64] Hence, the mere "[k]nowledge of the *capability* of monitoring alone cannot be considered implied consent."[65]

Following the same line of reasoning used by the court in *Deal*, the Eleventh Circuit strongly cautioned against imprudently applying the doctrine of implied consent in cases brought under the Wiretap Act.[66] In *Anderson v. City of Columbus*, the court held the city liable under the Act where a city employee was unaware that the system for recording her work telephone calls continued to record statements she made through her headset after her calls were terminated.[67] Even if the employee gave prior consent to the recording of her business calls, her consent did not constitute implied consent to the recording of her private conversations.[68]

Berry v. Funk represents yet another case where a court narrowly tailored the consent exception.[69] In *Berry*, the plaintiffs claimed that they did not have sufficient notice that their employer was monitoring their calls.[70] The plaintiffs knew that their Watch Officers could listen to conversations and perform other functions as part of their duties.[71] Nevertheless, the operations center "explicitly directed Watch Officers not to monitor unless the parties to the

60. Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983); *see also* Zweibon v. Mitchell, 606 F.2d 1172, 1182 (D.C. Cir. 1979) (noting that the dominant purpose of Wiretap Act was to prevent improper privacy invasions); United States v. Harpel, 493 F.2d 346, 351-52 (10th Cir. 1974) (holding that surreptitious recording of private conversation by use of an extension telephone violated the Wiretap Act).

61. *Watkins*, 704 F.2d at 581.

62. 980 F.2d 1153, 1155-56 (8th Cir. 1992).

63. *Id.* at 1156-57.

64. *Id.* at 1157 (quoting *Watkins*, 704 F.2d at 581).

65. *Id.*

66. 374 F. Supp. 2d 1240, 1250 (M.D. Ga. 2005).

67. *Id.* at 1251.

68. *Id.*

69. 146 F.3d 1003, 1011 (D.C. Cir. 1998).

70. *Id.*

71. *Id.* at 1005.

conversation so requested."[72] In agreeing with the plaintiffs, the court concluded that "[w]ithout actual notice, consent can only be implied when '[t]he surrounding circumstances [ ] *convincingly* show that the party knew about and consented to the interception.'"[73]

Deal, Anderson, and *Berry* represent clear examples of judicial restraint in applying the implied consent doctrine. They demonstrate an insightful reasoning that illustrates clarity during the confusion in interpreting consent, and uphold the foremost concerns of Congress in protecting personal privacy.[74] For as long as employers continue to monitor employees, courts should continue to carefully weigh the competing interests between them in the hopes of finding the proper balance between privacy and protection.

C. *The Legislative Intent Behind the Wiretap Act is at Odds with a Broad Interpretation of Implied Consent*

Although the legislative history of the Wiretap Act does provide some support for the doctrine of implied consent,[75] the loss of personal privacy was an overriding congressional fear.[76] "Congress was . . . concerned with the potential for widespread abuse of the tremendous scientific and technological developments in electronic surveillance techniques, and so broadly prohibited, with narrow exceptions, all interception of oral and wire communications."[77] Given the widespread use of computers in the workplace and electronic forms of communications over the Internet,[78] in conjunction with the development of sophisticated monitoring tools for electronic surveillance,[79] the concerns expressed by Congress

---

72. *Id.* at 1011.

73. *Id.* (quoting United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995)) (alterations in original).

74. *See, e.g.*, Gelbard v. United States, 408 U.S. 41, 48 (1972) (observing that the protection of privacy was a major concern in congressional passage of the Wiretap Act).

75. *See* S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182 (1968) [hereinafter S. REP. 90-1097] ("[C]onsent may be expressed or implied. Surveillance devices in banks or apartment houses for institutional or personal protection would be impliedly consented to.").

76. *Gelbard*, 408 U.S. at 48.

77. Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 819 (N.D. Ill. 1981); *see* S. REP. 90-1097 at 2154 ("No longer is it possible, in short, for each man to retreat into his home and be left alone. Every spoken word relating to each man's personal, marital, religious, political, or commercial concerns can be intercepted by an unseen auditor and turned against the speaker to the auditor's advantage.").

78. *See* Jarrod J. White, *E-Mail@Work.Com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1079 (1997) ("[E]merging technology at the sunset of the twentieth century, particularly the pervasive use of electronic mail (E-mail) by private sector companies, has unleashed new uncertainty concerning privacy rights in the workplace.").

79. *See* Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the*

appear more like prophecies.

The Supreme Court's decision in the recent case of *Kyllo* v. *United States* demonstrates a similar concern with the "power of technology to shrink the realm of guaranteed privacy."[80] In *Kyllo*, the Court struck down as unconstitutional the government's use of thermal imaging (infrared) scanners to peer into homes looking for evidence of a crime.[81] In his dissenting opinion, Justice Stevens agreed with the majority that the technology in this case threatens privacy, but argued that the protection of privacy should be left to the legislature and not the courts.[82] Therein lies the rub that even in the absence of a Congressional mandate, the Court will react quickly when government actions threaten personal privacy.[83] Yet, when called upon to protect that same privacy from employers, their response is often more sedate.[84]

In 1993, Congress directly addressed its concerns about the privacy of American workers by introducing the Privacy for Consumers and Workers Act ("PCWA").[85] The PCWA would have created the first legal framework around workplace privacy by outlining the rights of employees and "the ability of employers to conduct monitoring."[86] The purpose of the PCWA was to prevent employers from abusing electronic monitoring.[87] Supporters of the bill questioned the sad irony of requiring the Federal Bureau of Investigation "to obtain a court order to wiretap a conversation, even in cases of national security," while employers are allowed to spy on their employees at will.[88] They explained that other industrialized countries strongly protect employee privacy by tightly confining employer-monitoring activities.[89]

Workplace, 19 N.Y.L. SCH. J. INT'L & COMP.L. 379, 379 (2000) ("The growth of electronic surveillance in the workplace has been phenomenal and has created a global problem.").

80. 533 U.S. 27, 34 (2001).

81. *Id.* at 40.

82. *Id.* at 51 (Stevens, J., dissenting).

83. *See id.*

84. *See id.*; *see also* discussion *supra* Part II.A.

85. Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331, 343 (2010).

86. Julie A. Flanagan, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1257-58 (1994).

87. *Id* at 1257.

88. *Privacy for Consumers and Workers Act: Hearing on S. 516 Before the Subcomm. on Emp't and Productivity of the S. Comm. on Labor and Human Res.*, 102d Cong. 3 (1991) (statement of Sen. Paul Simon, Chairman, Subcomm. on Emp't and Productivity of S. Comm. On Labor and Human Res.).

89. *See Privacy for Consumers and Workers Act: Hearing on S. 984 Before the Subcomm. on Emp't and Productivity of the S. Comm. on Labor and Human Res.*, 103d

Compelling arguments by compassionate advocates for employee rights helped the PCWA gain support in the Senate.[90] In spite of this, the Senate bill was never forwarded and eventually died in committee.[91] The death of the PCWA was mostly attributed to Republican opposition that was supported, at the time, by employer lobbyists.[92] Since then, there has been a dramatic shift in American government with the historic election of President Barack Obama and a Democratically controlled Senate.[93] Accordingly, the employee privacy rights movement might finally find traction in today's Congress, given President Obama's overwhelming support for American workers.[94]

III. MAKING THE LEAP FROM CONSENT TO AUTHORIZATION

Without specific legislation to protect electronic privacy rights in the workplace,[95] employees have turned to provisions in the Wiretap Act and Storage Act to shield them from their employer's unlawful electronic intrusions.[96] In pursuing this legal recourse, employees are often confounded because "the Wiretap Act 'is famous (if not infamous) for its lack of clarity,' . . . [and its intersection with the Storage Act] is a complex, often convoluted, area of the law."[97] However, it is clear that the paramount objective of the Wiretap Act is to protect the privacy of communication transmissions, while the

---

Cong. 2-3 (1993) (statements of Sen. Paul Simon).

90. *See* Levinson, *supra* note 85, at 343; *see also* White, *supra* note 78, at 1099.

91. *See* White, *supra* note 78, at 1099.

92. *See* Judith Lockhart & Gerald W. Griffin, *Monitoring Employee E-mail, Voice Mail and Computer Files Without Violating Employees' Privacy Right*, CARTER LEDYARD & MILBURN LLP (Nov. 8, 1999), http://www.clm.com/pubs/pub-914447_1.html (noting that after the PWCA was introduced in Congress, it "remain[ed] inactive due to [R]epublican opposition"); *see also* Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy In The Workplace* 54 FLA. L. REV. 289, 299-300 (2002) (explaining why employers opposed the PCWA).

93. *See* Scott Helman & Michael Kranish, *Historic Victory Obama Elected Nation's First African-American President in a Romp*, BOSTON GLOBE, Nov. 5, 2008, at A1.

94. *See* Ross Colvin, *Obama Says Will Reverse Bush Labor Policies*, REUTERS (Jan. 30, 2009), http://www.reuters.com/article/idUSTRE50P6MB20090130 (explaining that President Obama pledges "to bolster unions in the workplace and strengthen workers' rights").

95. *See* discussion *infra* Part III.C.

96. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 873, 876 (9th Cir. 2002); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 459 (5th Cir. 1994); Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437, at *5 (D.N.J. July 25, 2008).

97. United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) (quoting *Steve Jackson Games, Inc.*, 36 F.3d at 462); *see, e.g.*, United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003) (quoting same); Konop, 302 F.3d at 874 ("Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.").

Storage Act is directed at the unauthorized and intentional accessing of stored communications.[98]

Although provisions of the statutes "appear . . . to be mutually exclusive . . . (with mutually exclusive remedial schemes),"[99] because of their intersections, courts have analogized certain terms in order to define ambiguous language.[100] A few definitions, nevertheless, have still proved to be very elusive with little guidance offered from Congress.[101] In *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit noted that in determining whether use of a competitor's Web site constituted unauthorized access, "Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves."[102] The parties in *EF Cultural Travel BV* argued that the court should narrowly read into the definition of the term, or, conversely, view it broadly by determining whether the use is in line with the Web site owner's reasonable expectations.[103] Content on determining the case on other grounds, the court never ventured to settle the dispute.[104]

The preeminent decision often cited as persuasive authority on resolving this issue remains *In re DoubleClick Privacy Litigation*.[105] The District Court for the Southern District of New York determined that "[i]n reviewing the case law and legislative histories" there was no difference in how authorization (Storage Act) and consent (Wiretap Act) were defined.[106] Furthermore, because consent has been broadly construed, analogously, so should authorization.[107]

Consequently, by liberally construing authorization, the court brushes aside congressional intent, which can be found by examining the Storage Act's legislative history.[108] The congressional committee

---

98. *Smith*, 155 F.3d at 1055-56.

99. *Id.* at 1056.

100. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

101. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

102. *Id.* (quoting 18 U.S.C. § 1030(a)(1) (2006)).

103. *Id.*

104. *Id.*

105. *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437 at *3 (D.N.J. July 25, 2008); *see also In Re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19 (1st Cir. 2003); Kaufman v. Nest Seekers, LLC, 2006 U.S. Dist. LEXIS 71104 at *10 (S.D.N.Y. Sept. 26, 2006); *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. LEXIS 16947, *18 (N.D. Cal. Oct. 9, 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001).

106. *In re* DoubleClick, Inc. Privacy Litigation, 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001).

107. *See id.* at 514 n.23 (noting that "courts have emphasized that consent must be construed broadly under the Wiretap Act") (internal quotations omitted).

108. *See* discussion *supra* Part III.C (discussing the courts' similar disregard for

notes accompanying the Act reflect that it was designed to address "the growing problem of unauthorized persons deliberately gaining access to . . . electronic or wire communications that are not intended to be available to the public."[109] Thus, once again, Congress has spoken loudly about its concerns to protect personal privacy, but sadly, the courts appear not to hear its cries.

A. The Struggle to Understand what Congress Meant by Authorization

In passing the Storage Act, Congress understood that the Internet required different levels of protection because of the technical distinctions between electronic communications that are in storage versus those being transmitted.[110] These differences should have clearly demarked the boundaries of an Internet user's reasonable expectation of privacy, and when that expectation is unfounded.[111] But the ambiguity of the statutory language has led courts to adopt different perspectives on whether an individual has granted authorization for his or her privacy to be invaded.[112] As such, use of the Storage Act is often narrowed because jurists have determined that "the existing statutory framework is ill-suited to address modern forms of communication."[113] It is believed that Congress might have intended for the inherent nature of a communication system's configuration to determine the level of privacy protection it receives.[114] As a result, courts have held that "unauthorized access" is limited to the intentional conduct of an outside intruder, such as computer hacking by a third party.[115]

---

congressional privacy concerns when interpreting the Wiretap Act in employer monitoring cases).

109. S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3589 [hereinafter S. REP. 99-541].

110. *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1567-70 (2004).

111. *See supra* Part III.A. The courts are not clear on whether a user of the Internet for communication has a reasonable expectation of privacy. "One reason for the current disconnect between privacy expectations and the statutory protections of the ECPA is that Congress was drafting legislation in the early stages of a technology that has fundamentally changed the way we communicate, store, and use information." Mulligan, *supra* note 110, at 1572.

112. *See* Nathaniel Gleicher, *Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web*, 118 YALE L.J. 1945, 1952-54 (2009) (discussing the courts' varied understandings of the term authorization).

113. Konop v. Hawaiian Airlines, 302 F.3d 868, 874 (9th Cir. 2002).

114. *See id.* at 879 n.8.

115. *Id.* at 889-91; *see, e.g.*, State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc., 909 F. Supp. 137, 145 (S.D.N.Y. 1995) ("[I]t appears that the [Storage Act] was primarily designed [by Congress] to provide a cause of action against computer

The Senate Report accompanying the Storage Act supports an alternative reading by providing useful congressional insights into the type of conduct, which may constitute an authorized user's unauthorized access.[116] For example, a subscriber to a communal computer mail facility would violate the statute by "[a]ccessing the [electronic] storage of other subscribers [to the facility] without specific authorization to do so."[117]

This theory was recently tested in *Bailey v. Bailey*, where the ex-husband defendant installed keystroke-logger software on a computer he shared with his then wife, which allowed him to learn the password to her Yahoo account.[118] The husband then used the information he gathered from his wife's stored e-mails in their divorce action. Believing that the disclosure of the e-mail messages caused her to lose custody of her children, the wife filed suit pursuant to the provisions provided under the Storage Act.[119] The court denied the ex-husband's motion for summary judgment, concluding that the Storage Act did in fact reach his conduct.[120] Furthermore, these sorts of trespasses, to which the Storage Act applies, "'are [for] those in which the trespasser gains access to information to which he is not entitled to see.'"[121]

The Ninth Circuit tried to fill the Storage Act's legislative void by analogizing authorization to common law tort principles.[122] In reversing the dismissal of a Storage Act claim based on the defendant's lack of authorization to access saved e-mails, the court held that "[p]ermission to access a stored communication does not constitute valid authorization if it would not defeat a trespass claim in analogous circumstances."[123] The court reasoned, "[j]ust as trespass protects those who rent space from a commercial storage facility . . . the Act protects users whose electronic communications

---

hackers.").

116. *See* S. REP. 99-541, *supra* note 109, at 3590.

117. *Id.*

118. Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *1-3 (E.D. Mich. Feb. 6, 2008).

119. *Id.* at *6-7.

120. *Id.* at *17-18.

121. Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Matsuda, 390 F. Supp. 2d 479, 497 (D. Md. 2005) (quoting Educ. Testing Serv. v. Stanley H. Kaplan, Educ. Ctr., Ltd., 965 F. Supp. 731, 740 (D. Md. 1997)). Although Congress did not define the phrase "without authorization" in the Storage Act, it did provide a statutory definition for the phrase "exceeds authorized access" in the Computer Fraud and Abuse Act, which means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2006).

122. Theofel v. Farey-Jones, 341 F.3d 978, 982 (9th Cir. 2003).

123. *Id.* at 983.

are in electronic storage . . . ."[124] The court's view may be an extremely narrow interpretation of authorization, but it exposes the issue that is created when new technologies outpace the law.

The current state of confusion in interpreting the Storage Act is understandable given the statute's vague language such as "conduct authorized."[125] Putting the legislative history aside, Congress appears content either by inaction or ambiguity to let the courts fill in the gaps. To end this confusion, a broader look at congressional committee reports would furnish a better insight for the courts to embrace a narrow definition of "authorization" that upholds the important public policy of protecting personal privacy.

B. Narrowing the Scope of Authorization

When applying the concept of authorization in the context of employer monitoring, federal law provides various exceptions from liability to employers who access stored electronic communications.[126] Communications are considered stored irrespective of whether the storage is permanent, temporary, or incidental to transmission.[127] Under the Storage Act, employers can seek to be released from civil and criminal liability for "conduct authorized . . . by the person or entity providing a wire or electronic communications service."[128] Accordingly, if an employer searches the electronic storage of the equipment it provides, the company and its agents might be immune from prosecution.[129]

---

124. *Id.* at 982.

125. *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437, at *3 (D.N.J. July 25, 2008) (quoting 18 U.S.C. § 2701(c) (2006)).

126. 18 U.S.C. § 2701(c)(1) (2006); *see also* 18 U.S.C. § 2701(c)(2) (2006). The Storage Act provides broad immunity from liability for what has become widely known as the "service provider" exception. *See* Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

127. In *Steve Jackson Games, Inc. v. United States Secret Service,* the court affirmed the district court's finding that the Secret Service violated the Storage Act's proscription against unauthorized access to electronic communication while in storage. 36 F.3d 457, 462 (5th Cir. 1994). In making its conclusion, the court cited the definition of "electronic storage" as "'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.'" *Id.* at 461 (quoting 18 U.S.C. § 2510(17) (2006)).

128. *See* 18 U.S.C. § 2701(c)(1).

129. To qualify for this exception, the employer must be the provider of the communications service used to store the electronic communication. *See, e.g.*, Bohach, 932 F. Supp. at 1236 (holding that the police department is immune from suits by its officers for accessing their text messages where the department provided the equipment on which the text messages were stored). *But see* Steinbach v. Forest Park, No. 06c4215, 2009 U.S. Dist. LEXIS 59907, at *6 (N.D. Ill. July 14, 2009) (holding that a third party was the service provider for the purposes of the Storage Act exception, not the city who used the service); *In re* Jet Blue Airways Corp. Privacy Litg., 379 F.

In addition, the Storage Act affords immunity for "conduct authorized . . . by a user of [a wire or electronics communication] service with respect to a communication of or intended for that user."[130] In other words, if an employee or any authorized user of a private Web site gives an employer the right of entry, the employer could seek immunity for accessing that Web site.[131] In this instance, liability usually turns on how the employer obtained authorization.[132] In *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp*, the employer-plaintiff, Pure Power, sued former employees for breaching their non-compete agreements.[133] After resigning from Pure Power, the former employees "opened a competing fitness center."[134]

To compile evidence that the former employees were establishing a competing business, Pure Power accessed and reviewed e-mails from one of the employee's Hotmail and Gmail accounts.[135] The employee allegedly "left his username and password" stored on his work computer.[136] According to Pure Power, the accounts opened automatically when the e-mail Web sites were accessed.[137] The employer argued that because they distributed an e-mail monitoring policy, they put all employees on notice that their work computers could be monitored.[138] As a result, when the defendant left "his

---

Supp. 2d 299, 307 (E.D.N.Y. 2005) (internet service provider exception only applies when the defendant itself provides the communication service, not a middleman).

130. 18 U.S.C. § 2701(c)(2).

131. In *Konop v. Hawaiian Airlines*, the plaintiff created a Web site that was critical of the airline. 302 F.3d 868, 872 (9th Cir. 2002). The plaintiff then authorized several pilots to use the Web site. *Id.* Two of the pilots gave their passwords to a Hawaiian Airlines Executive, who then accessed the site. *Id.* at 873. The court determined that the employer was not entitled to immunity because the two pilots who provided the executive with access had never used the site themselves. *Id.* at 880. As a result, they were not "users" of the service, and, consequently, could not authorize a third party's access. *Id.*

132. On June 16, 2009, a federal jury in New Jersey imposed compensatory and punitive damages on a company whose managers monitored employee postings in a private MySpace chat room. Charles Toutant, *Restaurateurs Hit With Damages for Infiltrating Waiters' MySpace Forum*, N.J.L.J., June 22, 2009, at 7. The managers allegedly required an employee to surrender the chat room's password and subsequently terminated the employees responsible for the chat room's creation. *Id.* In refusing to dismiss the plaintiff's wrongful termination claim, the court allowed the case to reach the jury to determine whether access to the employees' site by the managers was unauthorized. *Id.* The jury found that the managers' access of the chat-room was unauthorized because they obtained the chat-room password under duress. *Id.*

133. 587 F. Supp. 2d 548, 553-54 (S.D.N.Y. 2008).

134. *Id.* at 552.

135. *Id.*

136. *Id.*

137. *Id.*

138. *Id.* at 559.

username and password" on his work computer, he implicitly gave authorization to his employer to access his accounts.[139]

Despite the company's monitoring policy, which covered personal e-mail accounts accessed via the company's computer system, the Southern District Court of New York prohibited Pure Power from using the employee's personal e-mails as evidence.[140] The court rejected the employer's alleged authority to inspect e-mails that were not stored on the employer's computers but merely accessed from them.[141] The magistrate's report, adopted by the district court, determined that since the e-mails were not stored on the company's system, and not necessarily created or sent from Pure Power, the policy did not apply.[142] Judge Katz explained that the employee did not authorize access to his private e-mail just by simply leaving his password on his work computer.[143] By analogy, "If he had left a key to his house on the front desk . . . one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings."[144]

Judge Katz's findings logically infer that a company's investigative authority ends at the doorsteps of its premises,[145] and if you are an employer you may want to limit your inquiries to cyber activities that occur on your own equipment.[146] In the digital age, however, electronic-snooping technologies are so advanced that employers are able to invade an employee's security protocols with little chance of detection.[147] For this reason, federal courts are urged to follow Judge Katz's lead by narrowly interpreting the occasions when an employee's conduct could have allegedly authorized his

---

139. *Id.*

140. *Id.* at 571.

141. *Id.* at 559.

142. *Id.*

143. *Id.* at 561.

144. *Id.*

145. *See id.*

146. *See* Molly DiBianca, Comment to *Job Candidates Made to Submit Facebook Pages for Background Checks*, DELAWARE EMPLOYMENT LAW BLOG (Nov. 18, 2009), http://www.delawareemploymentlawblog.com/2009/06/job_candidates_made_to_submit.html (discussing how some employers are now requiring prospective candidates to provide their online passwords as part of the job application). *But see* Martha Neil, *Mont. Town Rescinds Rule Requiring Job Seekers to Reveal Social Web Passwords*, ABA JOURNAL (June 23, 2009 4:01 P.M.), http://www.abajournal.com/news/article/mont._town_rescinds_rule_requiring_job_seekers_to_reveal_social_web_passwor/. Bozeman, Montana required job applicants to provide their logons and passwords for personal social networking sites and private e-mail accounts. *Id.* The city told job applicants that the information would be used to perform background checks. *Id.* Concerned about workplace privacy issues and possible lawsuits, the town rescinded the controversial policy. *Id.*

147. Gantt, *supra* note 24, at 346.

employer to snoop for electronically secured information beyond the workplace.

C. Plugging the Authorization Hole in the Storage Act

To determine what type of access to electronic storage Congress considered an exception to violating the Storage Act, we must examine the meaning of the term "conduct authorized" in the context of the statute.[148] The Senate Committee Report accompanying the Storage Act does provide a glossary—however, this phrase was conspicuously left unattended.[149] In fact, in the past twenty years since the Act's passage, Congress has not attempted to finally end the current confusion surrounding the term's interpretation.[150]

When interpreting the Storage Act, we are guided by the fundamental principle of statutory construction "that the language of the statute must be given its plain meaning and common usage; the language must be read as a whole to arrive at its significant meaning, and an isolated word or term cannot be invoked to defeat a reasonable and fair construction."[151] In deconstructing the phrase "conduct authorized," we learn that the word "authorize" means "to give a right authority to act,"[152] while the term "conduct" derives meaning from several interpretations, such as to manage, direct or lead.[153] When read together in the context of the Storage Act, the phrase "conduct authorized" implies that Congress required active rather than passive approval to transfer to an accessor in order to enable his lawful entry to electronic storage.[154]

In the context of computer security, most systems authorization protocols "are based on a two step process: (1) Authentication to ensure that the entity requesting access to the system is what or who it claims to be, and (2) Authorization to allow access only to those

---

148. 18 U.S.C. § 2701(c) (2006).

149. *See* S. REP. 99-541, *supra* note 109, at 3562-65.

150. *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437, at *9 (D.N.J. July 25, 2008) (discussing the "dearth of case law" interpreting the term and a lack of legislative guidance).

151. Twp. of Delaware v. Neeld, 144 A.2d 801, 803 (N.J. Super. Ct. App. Div. 1958) (citing Giles v. Gassert, 127 A.2d 161, 166-67 (N.J. 1956)). *See, e.g.*, United States v. Daas, 198 F.3d 1167, 1174 (9th Cir. 1999) ("If the statute uses a term which it does not define, the court gives that term its ordinary meaning.").

152. BLACK'S LAW DICTIONARY 133 (6th ed. 1990).

153. *Id.* at 295 .

154. *See* 18 U.S.C. §§ 2701(c)(1)–(2) (2006). Although the term consent was used in drafting the Wiretap Act and it is possible to re-word the phrase "Conduct Authorized" using the term, Congress instead chose not to use it when they decided to protect electronic storage. *See id.* Legislators perhaps realized the damaging exposure from protection passive actions could imply, and rationally chose a wording that inferred the necessity of obtaining explicit direction. *See* discussion *supra* Part IV.A.

resources which are appropriate to the entity's identity."[155] This only further demonstrates that Congress could not have intended for "consent," which implies a passive definition,[156] to be equated with "authorization," two words that clearly conflict in "plain meaning and common usage" when applied to the computer industry.[157]

To interpret the will of Congress, "'[t]he fairest and most rational method . . . is by exploring [its] intentions at the time when [a] law was made . . . .'"[158] In 1986, Congress passed the Storage Act in response to a growing concern about the privacy of information stored on the Internet.[159] Legislators argued that "Congress must act to protect the privacy of our citizens," and that a failure to do so would erode their fundamental rights.[160] Today, more than ever, the protection of private data on the Internet is needed not only to ensure our seclusion from offensive intrusions, but to safeguard our identity and personal information from theft and misuse.[161] Just as Congress foresaw the dangers of technology in protecting electronic communications, the widespread use of the Internet foretold that technology would eventually invade the private sphere of our personal data, and would obligate Congress to enact prospective legislation.

As discussed in Part II of this Note, judicial restraint in interpreting the phrase "conduct authorized" would effectuate the legislative intent behind the Storage Act.[162] Federal courts, however, are not bound by the persuasive opinions of a few district judges.[163]

---

155. *Authorization*, BUSINESSDICTIONARY.COM, http://www.businessdictionary.com/definition/authorization.html (last visited Aug. 27, 2010).

156. A common passive definition of consent is "[v]oluntarily yielding to the proposition of another; acquiescence or compliance therewith." BLACK'S LAW DICTIONARY 305 (6th ed. 1990). In other words, consent can be granted by mere acquiescent silence to the actions of another. *See* United States v. Barragan, 379 F.3d 524, 530 (8th Cir. 2004) (citing United States v. Martel-Martinez, 988 F.2d 855, 858 (8th Cir. 1993)) (upholding that a "defendant's prior consent to search, and [his] passive conduct and silence while officers" extended the search to hidden compartments validated the officer's reasonable belief that further consent had been granted).

157. See *supra* note 155 and accompanying text; Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL6085437, at *3 (D.N.J. July 25, 2008).

158. District of Columbia v. Heller, 128 S. Ct. 2783, 2838 (2008) (quoting 1 COMMENTARIES ON THE LAWS OF ENGLAND 59-60 (1765)).

159. Gleicher, *supra* note 112, at 1945.

160. S. REP. 99-541, *supra* note 109, at 3559.

161. *See* Stephen J. Dubner and Steven D. Levitt, *Identity Crisis: Counting the Cost of a "Chargeback"*, N.Y. TIMES, March 11, 2007 § 6 (Magazine), at 24 (discussing the ramifications and growing trends in computer identity theft).

162. *See* discussion *supra* Part III.B.

163. *See* Higgins v. E. I. Du Pont de Nemours & Co., 671 F. Supp. 1055, 1060 n.3 (D. Md. 1987) ("While decisions of the federal courts in other circuits may be persuasive . .

Hence, a more suitable solution would be for Congress to finally include in the Act a definition of "authorization" that requires active direction from the owner of the stored information being accessed. This fix would be in accord with the important public policy, especially in the case of password-protected data, of protecting an Internet user's reasonable expectation of privacy.

IV. PROTECTING EMPLOYEE PRIVACY

Although the United States Constitution contains no explicit privacy provision, the United States Supreme Court has long recognized an implied right of privacy.[164] This concept is argued to have originated from a law review article, which urged that an individual has the fundamental right "to be let alone," and enjoy life free from unseemly intrusions.[165] Unfortunately, for the employee, it appears that the quid pro quo for accepting employment is to relinquish your fundamental rights in acquiescence to your employer's best interest.[166]

Of course, in certain circumstances, employers are allowed to monitor an employee's performance or their potentially tortious activities.[167] All the same, it should be noted that employer actions have not been without limits and bounds.[168] Employers can neither install video cameras inside of restrooms nor deploy audio surveillance equipment at the water cooler.[169] In forbidding such conduct, courts have emphasized that "[a] person may have a subjective expectation of privacy that is objectively reasonable in

---

. , this Court is not bound by such decisions.").

164. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479 (1965) (striking down a statute restricting purchase of contraceptives on privacy grounds).

165. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

166. *See* Schowengerdt v. United States, 944 F.2d 483, 488 (9th Cir. 1991) (noting that the "operational realities" of the employee's workplace precluded any reasonable expectation of privacy and justified his employer's constant surveillance of employee activities).

167. *See* Echols, *supra* note 35, at 278 (arguing that employers should be able to legally make use of new technologies to monitor web-based e-mail accounts when they are accessed in the workplace by employees).

168. *See* Luedtke v. Nabors Alaska Drilling, 768 P.2d 1123, 1133 (Alaska 1989) ("[T]here is sufficient evidence to support the conclusion that there exists a public policy protecting spheres of employee conduct into which employers may not intrude.").

169. Cramer v. Consol. Freightways, Inc., 209 F.3d 1122 (9th Cir. 2000) (holding that an employment contract which arguably allowed video surveillance behind bathroom mirrors could not supersede the mandatory provisions in state privacy laws), *rev'd en banc*, 255 F.3d 683 (2001); State v. Bonnell, 856 P.2d 1265, 1279 (Haw. 1993) (holding that the defendants had an objectively reasonable expectation of privacy in their break room because access to the room was limited to employees).

some area of his or her workplace."[170] To assess "the reasonableness of an [employee's] expectation of privacy," what should be considered is "the nature of the area involved, [and] the precautions taken to insure privacy."[171] In considering "electronic" privacy in the workplace, the road has been far from clear and direct,[172] forcing many employees to explain why their privacy expectations are not inherently unreasonable.[173]

A. Common Law Invasion of Privacy

Throughout this Note, I have discussed a number of lawsuits brought against employers to redress the injuries they allegedly caused by cyber snooping on employee activities.[174] In addition to federal statutory provisions,[175] employees can assert common law claims for a tortious invasion of privacy.[176] However, many of these claims have failed because employees are unable to demonstrate an "objectively" reasonable expectation of privacy.[177]

In the workplace setting, the test most commonly used to determine whether a reasonable expectation of privacy exists turns on two factors: first, the employer's intrusion must be intentional; and second, it must be "highly offensive to the reasonable person."[178]

---

170. *Bonnell*, 856 P.2d at 1276.

171. *Id.* at 1275.

172. The Fourth, Seventh and Tenth Circuits have held that defendants have no reasonable expectation of privacy in their work computers in light of the employer's computer use policy. *See* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002). But the Second and Fifth Circuits have held on particular sets of facts that employees did have a reasonable expectation of privacy in their office computers. *See* Leventhal v. Knapek, 266 F.3d 64, 73 (2nd Cir. 2001); United States v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002), *vacated*, 537 U.S. 802 (2002).

173. *See* United States v. Ziegler, 474 F.3d 1184, 1189 (9th Cir. 2007) (noting that an employee's expectation of privacy in his workplace must be "objectively reasonable").

174. *See* discussion *supra* Part.IV.

175. *See* 18 U.S.C. § 2701 (2006); 18 U.S.C. § 2510 (2006).

176. *See* Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 620-22 & n.8 (3rd Cir. 1992) (finding that many states have some form of common law tort for invasion of privacy); see also RESTATEMENT (SECOND) OF TORTS § 652 (1977), which sets out different forms of a common law invasion of privacy, and three of these are relevant to employer monitoring. They are: (1) the unreasonable intrusion into the "private affairs or concerns" of another, (2) the unreasonable disclosure of "matter concerning the private life of another," and (3) "publicity [that unreasonably places another] in a false light." RESTATEMENT (SECOND) OF TORTS §§ 652B, D & E.

177. *See* RESTATEMENT (SECOND) OF TORTS § 652B. *But see Bonnell*, 856 P.2d at 1277.

178. *See Borse*, 963 F.2d at 624-25. An employer may be liable under the tort theory found in the Restatement of (Second) of Torts § 652B, Intrusion Upon Seclusion. *See*

As illustrated by the cases I have discussed, the courts are conflicted on whether to recognize that an employee has any reasonable expectation of privacy in electronic communications, which are facilitated by use of their employer's equipment.[179] Even if employees can establish a privacy expectation, they still may lose, in most cases, if the legitimate business interests of the employer outweigh their privacy interest.[180]

B. Redefining the Employee Privacy Boundary

On December 14, 2009, the United States Supreme Court came close to entering the debate when it granted certiorari to decide whether a police officer had a reasonable expectation of privacy in text messages he sent with his department-issued pager.[181] In *Quon v. Arch Wireless Operating Co., Inc.*, the Ninth Circuit Court of Appeals held that the officer had such an expectation that was protected by the Fourth Amendment and provisions in California's Constitution.[182] The issue arose when defendant employer, the City of Ontario, distributed pagers with texting capabilities to its employees, including the Ontario Police Department, which in turn issued a pager to officer Quon.[183] The City then audited the pagers to determine whether the extra billing charges were because of business or personal use.[184] During its audit, the City discovered that Quon had sent several sexually explicit text messages to his wife and others.[185] Quon sued the City claiming, among other injuries, a violation of his right to privacy.[186]

RESTATEMENT (SECOND) OF TORTS § 652B. The theory is based on the psychological distress caused by the intrusion itself. *See e.g.*, Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 WL 6085437, at *4-20 (D.N.J. July 25, 2008) (arguing that if an employee consents to an intrusion under duress, that the defendant employer may be liable). The employer can be found liable for learning or disclosing anything embarrassing or private about the employee. *See id.*

179. *See supra* note 172 and accompanying text.

180. *See* Gordon, *supra* note 11, at 516. In balancing the employer's competing interest, the court will take into account that:

> From the employer's perspective . . . [t]he e-mail system can pose a potential threat by, for example, allowing the transmission of trade secrets off site with the press of a button. In addition, Internet use can interfere with the intended business purposes of the employer's system resources through, for example, the downloading of pornography.

Id.

181. City of Ontario v. Quon, 130 S. Ct. 1011 (2009) (granting certiorari).

182. Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 910 (9th Cir. 2008), *rev'd*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

183. *Quon*, 529 F.3d at 895.

184. *Id.* at 897-98.

185. *Id.* at 898.

186. *Id.* at 899.

The district court dismissed the suit after a jury found the City had a legitimate business interest in accessing the use of its equipment.[187] The Ninth Circuit reversed, holding that the City had violated Quon's constitutional right to privacy by reading his private text messages.[188] The court concluded that even if the City's business interest in its property was legitimate, Quon "enjoy[ed] a reasonable expectation of privacy in areas given over to his exclusive use."[189] In the unanimous opinion, the court reasoned that the City's monitoring policy could not overcome Quon's constitutionally protected privacy interest because he was not given sufficient notice that his text messages could be read by others.[190]

Although the Supreme Court overturned the Ninth Circuit,[191] as expected,[192] employers should take heed from the Court's cautionary statement that a departmental "audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account . . . would have been."[193] In short, by finding that the employer's search was reasonable in this case, the Court narrowed the issue and refused to go further to determine if an employee could have an expectation of privacy in work-provided communication equipment.[194] However, many states have adopted a common law right to privacy that derives from their respective state constitutions.[195] These states could find that employees have such a privacy right, which is so fundamental to our democratic beliefs that it cannot be so easily overcome by an employer's mere legitimate

187. *Id.*

188. *Id.* at 910.

189. *Id.* at 907 (quoting Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987)).

190. *Id.*

191. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

192. "[W]hile many legal experts agree that the [*Quon*] ruling is significant, it is by no means definitive. . . . 'Decisions by the Ninth Circuit Court are regularly overturned by the U.S. Supreme Court because they are so far out of step with the current temperament of the Supreme Court.'" Nikki Swartz, *On the Edge: Bosses Can't Read Employees' Messages, Court Says*, INFO. MGMT. (Sept.–Oct. 2008) (quoting John Montaña, J.D., general counsel at The PelliGroup, Inc.), http://content.arma.org/IMM/SeptOct2008/IMJ0908bossescantreademployeesmessages.aspx. Thus, the battleground for employee privacy rights will continue to be fought by zealous advocates in the courts and jury boxes from state to state.

193. *Quon*, 130 S. Ct. at 2631.

194. *Id.* at 2630.

195. Many states have codified the provisions in their respective constitutions to protect privacy. *See e.g.* CAL. CONST, art. I, § 1 (1974). In California, the constitution states that: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." *Id.*

business interest and, instead, can only be relinquished by the employee's explicit authorization.[196]

C. Expectation of Privacy in the Digital Age

To protect the legitimate business interest of the company, many employers will lay claim to their cyber-dominion by distributing a monitoring policy,[197] which asserts that the employer "reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through [its] system, for any reason, without the permission of any system user, and without notice."[198] While some courts have relied on provisions in federal and state law to rein in unreasonably intrusive employer behavior,[199] others have redefined the employer/employee privacy boundaries by requiring companies to show a more compelling business interest than just merely owning the equipment that the employee is utilizing.[200]

In New Jersey, the Appellate Division directly confronted the perception that an employer's monitoring policy could exclusively turn an employee's private e-mails into company property.[201] In *Stengart v. Loving Care Agency, Inc.*, the defendant-employer, Loving Care, supplied the plaintiff-employee, Stengart, with a company laptop.[202] When Stengart resigned, she returned her work equipment to Loving Care.[203] After Stengart filed suit for employment discrimination, Loving Care reviewed the contents of her laptop's hard drive and discovered e-mails between Stengart and her

---

196. *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) (affirming that an employee "could reasonably expect that [electronic] communications with her lawyer . . . would remain private, and that [transmitting] them via a company laptop did not eliminate the attorney-client privilege").

197. *See* Jeffrey Benner, *Privacy at Work? Be Serious*, WIRED NEWS (Mar. 1, 2001), http://www.wired.com/techbiz/media/news/2001/03/42029. Jeffrey Benner states:

> [I]f an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an "expectation of privacy." In short, once the company stakes its claim over its cyber-dominion, its employees have no right to privacy there.

Id.

198. Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548, 552-53 (S.D.N.Y. 2008).

199. *See* discussion *supra* Part III.B at 27-32.

200. *See supra* note 172 and accompanying text 37-38.

201. Denise J. Pipersburgh & Keyana C. Laws, *"Cyberspace in the Workplace"*, N.J.L.J., December 7, 2009, at 1-2.

202. Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 393 (N.J. Super. App. Div. 2009), *aff'd in part and modified in part*, 990 A.2d 650 (N.J. 2010).

203. *Stengart*, 990 A.2d at 656.

attorneys.[204] Stengart had sent the e-mails via her work computer using her password-protected, web-based e-mail account.[205] Later, in its answer, the company incorporated some of Stengart's e-mail communications with her attorney.[206] Stengart sought an order to prevent Loving Care's use of the e-mails.[207] The trial court denied Stengart's motion, finding that the company's monitoring policy put her on notice that e-mails on her work computer "would be viewed as company property," even those that were sent through an external application.[208]

The Appellate Division reversed the trial court's denial of the restraints, holding that the employer's policy was not controlling on the issue of Stengart's expectation of privacy.[209] Even though the policy clearly stated that the company had "the right to review, . . . access, and disclose all matters on the company's media systems and services," the court determined that Loving Care had no legitimate business interest in accessing Stengart's personal e-mails.[210] The court reasoned that in order to assert a right to access the e-mails, Loving Care must show a more "plausible explanation" than merely owning the computer equipment which Stengart used.[211]

As some legal commentators have noted, the *Stengart* court's decision is not based on the Storage Act, nor is it brought into its analysis.[212] Instead, the court relies on defeating the presumption that by imposing a monitoring policy, an employer is somehow authorized to access an employee's privileged personal e-mails sent via the company's computer system.[213] Moreover, the court rejected the premise that "because the employer buys the employee's energies and talents during a certain portion of each workday, anything that the employee does during those hours becomes company property."[214]

In contrast to other similar opinions discussed in this Note, the New Jersey Appellate Division's view of employee privacy rights in the workplace is much more expansive, and begs the question "whether th[e] holding could be extended to all personal e-mails sent and received through an employer's systems."[215] Arguing against the

204. *Stengart*, 973 A.2d at 393.
205. *Id.*
206. *Id.*
207. *Id.*
208. *Id.*
209. *Id.* at 402.
210. *Id.* at 394, 402.
211. *Id.* at 399.
212. Pipersburgh & Laws, *supra* note 201, at 2.
213. *Stengart*, 973 A.2d at 401.
214. *Id.*
215. Pipersburgh & Laws, *supra* note 201, at 2.

workability of this new rule of law, a number of writers cast doubts on whether the court's conclusions would "withstand further scrutiny."[216] Nevertheless, on March 30, 2010, the New Jersey Supreme Court unanimously affirmed the lower court's decision,[217] thereby adding New Jersey to the growing list of states ready to beckon in a new age of privacy rights for employees.[218]

As other courts around our nation grapple with similar issues and the concerns that technology is shrinking "the realm of guaranteed privacy,"[219] our dependency on electronic communications becomes more ubiquitous every day.[220] For employees, technology has enabled the ability to conduct business and personal affairs simultaneously.[221] For employers, this arguably benefits productivity, but exposes them to potentially severe liabilities.[222] Thus, for the courts, technology has only blurred the line between where business interests end and individual privacy rights begin,[223] forcing many jurists to make tough decisions "in this new digital age."[224]

V. CONCLUSION

In today's society, "the increase in data creation and the resulting collection of vast amounts of personal data" on the Internet raises troubling concerns regarding personal privacy.[225] Congress understood these challenges and reacted by passing the Storage Act. Although the Act is not a perfectly drafted piece of legislation, it does lay a solid foundation to build upon and Congress is well advised to heed this Note's recommendations in order to strengthen its language.

---

216. *Id.*; *see, e.g.*, Brent A. Cossrow, *2010 Is Not 1984:* Stengart v. Loving Care Agency, Inc. *and Cyber Privacy in the Workplace*, FISHER & PHILLIPS, LLP, http://www.laborlawyers.com/files/25149_2010%20is%20not%201984.pdf (last visited Oct. 19, 2010) (describing the Appellate Division's rule of law as unworkable given the technical realties of how web based e-mail portals work).

217. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).

218. *See* discussion *supra* Part IV.B.

219. Kyllo v. United States, 533 U.S. 27, 34 (2001).

220. See Frederick M. Joyce & Andrew E. Bigart, *Liability for All, Privacy for None: The Conundrum of Protecting Privacy Rights in a Perversely Electronic World*, 41 VAL. U. L. REV. 1481, 1481 (2007).

221. *See Stengart*, 990 A.2d at 654-55 (noting that personal Internet use is commnplace in the modern workplace).

222. *See id.* at 666. (ordering sanctions against an employer for accessing an employee's email on a work computer)

223. *See id.* (noting that as "technology evolve[s], the line separating business from personal activities can easily blur").

224. *See* Pipersburgh & Laws, *supra* note 201, at 1-2.

225. Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 291 (2003).

The failure of Congress to define "authorization" under the Storage Act has led some courts to presumptively conclude that employees have in some way abandoned their fundamental right to privacy at the keyboard of their employers' computers.[226] In lawsuits brought against employers in cases such as *Quon, Pure Power Boot Camp,* and *Stengart,* courts have rejected this presumption and challenged those findings.[227] "To be sure, a person can essentially relinquish or lose any right to privacy by revealing"[228] information publicly on the Internet; "[s]ervices like Facebook, Twitter and Flickr are oceans of personal minutiae."[229] But when an Internet user has taken precautions to password-protect his personal communications, courts should forestall any employer who jumps down the proverbial rabbit hole, and, alternatively, give greater weight to an employee's reasonable expectation that those communications will remain private.

Until the Storage Act's language is clarified and thereby strengthened, employers will rely on its ambiguous terminology to validate their ability to electronically investigate employees beyond the workplace, and employees in turn will continue to seek its shelter to protect them from unreasonable intrusions. To resolve these juxtaposed positions, the main question posed by the Act is whether "authorization" has been granted. In answering, courts should be mindful to analyze this question in the same context as an employee's privacy expectations. For the purposes of the Act, it might be logical to find that an employee has authorized access where he did not expect privacy.[230] On the other hand, when these occasions do not arise, just as the federal government needs a compelling reason to overcome our fundamental rights, so too should those who merely sign our W-2 forms.[231]

---

226. *See generally* Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1, 59 (1999) (arguing against this presumption).

227. *See* discussion *supra,* Parts III.B, IV.B, IV.C.

228. State v. Luman, 188 P.3d 372, 377 (Or. Ct. App. 2008), *rev'd*, 223 P.3d 1041 (Ore. 2009), *recons. denied,* 2010 Ore. LEXIS 93 (Feb. 4, 2010).

229. Steve Lohr, *How Privacy Vanishes Online*, N.Y. TIMES, Mar. 17, 2010, at A1 (discussing how technology to track an Internet user's cyber footprints has removed any perception that privacy could exist on the Internet).

230. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 660-61 (N.J. 2010) (noting that "[a] number of courts have tested an employee's claim of privacy in files stored on company computers by evaluating the reasonableness of the employee's [privacy] expectation").

231. *See supra* text accompanying note 83.

***