PRIVACY CONCERNS REGARDING THE MONITORING OF INSTANT MESSAGING IN THE WORKPLACE: IS IT BIG BROTHER OR JUST BUSINESS?

*Ira David**

I. INTRODUCTION

As the world of technology explodes with new communication media and vehicles for interpersonal exchange, concerns over privacy, or lack thereof, continue to grow, as evidenced by the attention paid the subject in the scholarly journals.[1] Some articles proselytize, proposing changes to embrace an author's concepts of what the relevant statutes *should* say.[2] Others take a more pragmatic position, analyzing issues and concerns from both user and system perspectives.[3]

---

* J.D. candidate 2005, University of Nevada, Las Vegas, William S. Boyd School of Law. The author would like to thank the faculty of UNLV for helping him through this project, in particular, Professor Lynne A. Henderson, who ripped the work apart when it needed ripping, and helped put it back together.

He would especially like to thank his family for putting up with random monologues on privacy, privacy laws, and other random topics, generally without any prompting on their part. However, he takes full credit for any errors, typographical or otherwise, contained herein.

[1] *See e.g.*, Antonia M. Apps & Thomas M. Dailey, *Non-Regulation of Advanced Internet Services*, 8 GEO. MASON L. REV. 681 (2000); John Bentivoglio et al., *Global Privacy Law Update*, 20 NO. 6 COMPUTER & INTERNET LAW. 1 (2003); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L.REV. 439 (2003); Darla W. Jackson, *Protection of Privacy in the Search and Seizure of E-Mail: Is the United States Doomed to an Orwellian Future?*, 17 TEMP. ENVTL. L. & TECH. J. 97 (1999); Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357 (2003); Richard A. Mann & Barry S. Roberts, *Cyberlaw: A Brave New World*, 106 DICK. L. REV. 305 (2001); Frank C. Morris, Jr., *The Electronic Platform: Email and Other Privacy Issues in the Workplace*, 20 NO. 8 COMPUTER & INTERNET LAW. 1 (2003); Donald H. Nichols, *Window Peeping in the Workplace: A Look Into Employee Privacy in a Technological Era*, 27 WM. MITCHELL L. REV. 1587 (2001).

[2] *See e.g.*, Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995); *See also, e.g.*, Julia Turner Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923 (1992); Laurie Thomas Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139 (1994).

[3] *See e.g.*, Hall Adams, III et al., *E-mail Monitoring in the Workplace: The Good, The Bad and The Ugly*, 67 DEF. COUNS. J. 32 (2000); Thomas R. Greenberg, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219 (1994); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic*

As electronic communication technologies have evolved, published articles have shifted focus from wiretapping phone lines, to capturing pager messages, to monitoring of electronic mail ("E-mail"), and now to the realm of Instant Messaging, or simply "IM," particularly within the workplace.[4,5]

IM injects new issues into the analysis. Claimants have alleged violations of Title I of the Electronic Communications Privacy Act of 1986 (ECPA), which, among other things, prohibits interception of "electronic communications."[6] However, courts have held this portion of the ECPA inapplicable to E-mail monitoring as the data access in question was not contemporaneous with its transmission.[7]

An E-mail system logically collects, sorts, and distributes messages ("store and forward"). Sending a message routes and adds that message to a specialized electronic database. Subsequent message delivery retrieves the data from database storage, and thereby falls, not under wiretap statutes,[8] but under the less restrictive statutes governing stored communications data,[9] where contents of an employer-provided system may be considered to be the employer's "property."[10]

This logic potentially fails in the arena of IM. Unlike the store and forward staging of E-mail delivery, IM works more like a direct phone connection, with messages sent immediately and commonly never stored.[11] The specific

Privacy in the Workplace, 54 FLA. L. REV. 289 (2002); Douglas M. Topolski & Albert W. Palewicz, *Employee Privacy Rights in the Electronic Workplace*, 35-FEB MD. B.J. 40 (2002).

[4] Apps & Dailey, *supra* note 1, at 709-10.

[5] Within the realm of privacy in the electronic age, articles may focus on a number of particular issues, frequently in protection of personal information in user databases, and the privacy concerns of identity theft and individual profiling. Writers such as Fred Cate have written extensively in this area, *see generally* Fred H. Cate, *The Changing Face of Privacy Protection in the European Union and the United States*, 33 IND. L. REV. 173 (1999); Fred H. Cate, *The First Amendment and the National Information Infrastructure*, 30 WAKE FOREST L. REV. 1 (1995), but only peripherally addressing privacy of communications as a separate and distinct topic. Cate's very definition of privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (FRED H. CATE, PRIVACY IN THE INFORMATION AGE, 22 (1997) (citing ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)) indicates that his emphasis is on exposure of personal data, not personal communications. However, even though such broader-based articles may not be exactly on point, their positions may nonetheless be relevant and are cited herein.

[6] 18 U.S.C. § 2511(1)(a) (2000).

[7] Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461-62 (5th Cir. 1994); *see also*, Bohach v. City of Reno, 932 F. Supp. 1232, 1237 (D. Nev. 1996); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 877 (9th Cir. 2002).

[8] Title I of the ECPA, 18 U.S.C. §§ 2510-2522 (2000).

[9] Title II of the ECPA, 18 U.S.C. §§2701-2711 (2000).

[10] When a Los Angeles Superior Court judge dismissed the suit brought by Alana Shoars alleging violations of privacy in her employer's reading of employees' E-mail, the judge's spokesperson commented that "[i]n essence, the judge said companies have the right to manage their E-mail system." Jim Nash & Marua J. Harrington, *Who Can Open E-mail; Nissan Latest to be Sued for Privacy Invasion*, COMPUTERWORLD, January 14, 1991 at 1.

[11] Apps & Dailey, *supra* note 1, at 709. There may be some question of whether or not a message appearing on a computer screen, or retained fleetingly in computer RAM (random access memory) suffices as a storage. The Ninth Circuit, in *MAI System Corporation. v. Peak Computer, Inc.*, 991 F.2d 511, 518-29 (9th Cir. 1993), held that a copy loaded into

architecture of the messaging system, particularly whether a message is stored and how its contents may be disclosed, determines the standard to be applied.

As a further "wrinkle", while employers often provide E-mail services to their employees, and rely on it as a critical business tool, they less commonly provide IM. Instead, individual employees often install IM themselves, albeit on PCs provided by their employer.[12] Absent a clear and *enforced* corporate policy on installation of "personal software" on company computers, the employer may have no ability to examine IM traffic by any means other than interception.[13]

This Note evaluates the state of the law regarding privacy of IM, both as to traffic and content.[14] IM is new, even within the mercurial world of electronic communications, conceptually falling between the postal service nature of E-mail (collect the mail, sort the mail, distribute the mail) and the conversational characterization of a phone call. Thus, understanding or interpreting the law applicable to IM necessitates extracting and analogizing from other, similar, fields, drawing on cases involving privacy of E-mail, chat rooms, web sites, pagers and the like.

Part II provides a historic perspective and identifies the conflict between the privacy interest of the individual, and the business needs of the employer. Part III looks at the statutes and judicial history relevant to privacy of electronic communication and attempts to synthesize the law being applied for the various electronic media, particularly IM. Part IV uses the similarities and differences of IM and E-mail to develop a heuristic approach to analyze employer accessing of Instant Messages. Part V recommends procedures to protect against claims of violation of privacy, as well as of inappropriate behavior and failure to cure. Finally, Part VI recaps and looks at possible future issues and directions.

RAM could constitute enough of a fixation to be considered a copyright violation, which by extension, could be enough to distinguish such access from an interception.

[12] U.S. v. Wong, 334 F.3d 831, 839 (9th Cir. 2003) (citing U.S. v. Cormier, 220 F.3d 1103, 1108 (9th Cir. 2000)) to assert "a person does not have a reasonable expectation of privacy in an item in which he has no possessory or ownership interest." If an employee has no possessory interest in the PC provided by the employer, that employee therefore would not have a reasonable expectation of privacy.).

[13] While application storing of messages requires some facility in the IM application itself, there are software packages commercially available which will allow an employer to simply access *all* messages sent or received, or images of all screen displays. Such access may result in logging of screens (i.e. maintaining a recorded, serial record of screen images), or even in direct visual monitoring of employee computers. Products such as pcAnywhere® from Symantec Software, LapLink® from Traveling Software or WideScope® from RazLee Products, Ltd. are marketed as help desk or software demonstration tools, but provide the ability to audit any user screen attached to the system, potentially without alerting the monitored user.

[14] In some cases, an employer may simply want to know if employees are using IM, and if so to whom they are communicating. In others, the actual content of the messages may be the issue.

II. History of the Confrontation

A. *Historical Contex*

In 1890, Warren and Brandeis published what many consider to be the seminal work on rights of privacy.[15] Even after more than a century, this work remains a springboard for analyses of privacy rights.[16] Asserting that "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others,"[17] Warren and Brandeis posit that this includes the right to "fix the limits of the publicity" of such personal communications *regardless of the method of expression.*[18] Such right survives until surrendered by the author by publication to the public.[19] In 1890, Warren and Brandeis feared the threat to personal privacy posed by the advances of technology, to wit the ability to take photographs surreptitiously, without need for a sitting, and without permission of the subject.[20] Today, these concerns have been replaced by concerns regarding the ability of an employer to "electronically eavesdrop" or "censor" the communications of the employee.

Herbert Spencer Hadley rebutted the Warren and Brandeis position regarding privacy rights of the individual in 1894,[21] asserting

> [T]he arguments in favor of [a right of privacy] are based on a misunderstanding of the authorities cited in support; that the jurisdiction of courts of equity does not on principle recognize the right to privacy; . . . that equity has no concern with the feelings of the individual . . . except as the inconvenience or injury that a person may suffer is connected with the enjoyment or possession of property.[22]

Hadley's objection is technical and jurisdictional, as the principles of equity must be "defined and invariable"[23] and could not be amended, regardless of the personal wishes of the court.[24] Hadley asserts that the cases on which Warren and Brandeis rely[25] were decided on grounds of contract and property rights[26] and that anything further stated in the opinions was simply dicta.[27] Establishment of a right of privacy "can only be furnished by statutory legislation."[28]

---

[15] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

[16] Scanning Westlaw's TP-ALL database for references to this article [(Warren +5 Brandeis) /p privacy] shows over 170 references between 2000 and 2003.

[17] *Id.* at 198 (citing Millar v. Taylor, 4 Burr. 2303, 2379 (1769) (Yates, J.).

[18] *Id.* at 198-199.

[19] *Id.* at 199-200.

[20] *Id.* at 211.

[21] Herbert Spencer Hadley, *The Right to Privacy*, 3 Nw. U. L. Rev. 1 (1894).

[22] *Id.* at 4.

[23] *Id.* at 6.

[24] *Id.* at 6-7.

[25] *Inter alia*, Prince Albert v. Strange, 1 MacN. & G. 25 (1849); Pollard v. Photograph Co., 40 Ch. Div. 345 (1888).

[26] Hadley, *supra* note 21, at 8-13.

[27] *Id.* at 2.

[28] *Id.* at 20.

Not surprisingly, early cases disagreed on whether rights of privacy existed.[29] However, in the last century, federal and state legislatures have enacted a framework for general and specific privacy rights,[30] and today courts look to these foundations, as well as judicial precedent, to decide issues of privacy. This Note addresses privacy in a specific environment, and in a particular medium. It is to that situation that attention must be paid, starting with an understanding of the conflict itself.

Electronic messaging, or E-mail, began pervading the workplace before the explosion of the Internet. Initially, E-mail systems addressed specific business requirements, without regard for individual privacy issues. One such system was developed in 1976-77 for P&C Foods in Syracuse, New York.[31] This system provided both the store-and-forward capability seen today in standard E-mail systems, and the conversational communication facility of IM. Functions were not called E-mail or IM, but were referred to as "queued" and "quick send." The system was designed around the physical or geographic location of a recipient, the specific terminal and terminal model being used, and even included a facility to monitor either quick-send or queued message traffic, including message content.[32] This prototype system routed product orders as part of a complete business system, and privacy issues did not arise. Managers monitored message traffic as part of their job function.

Until the mid-1980s designs for E-mail systems varied, but the mainframe/database orientation remained standard.[33] System personnel had access to messages, in either encrypted or unencrypted form, on the corporate host. User

---

[29] *See generally* Roberson v. The Rochester Folding Box Co, 171 N.Y. 538, 64 N.E. 442 (1902) (holding that as the right of privacy was not enforceable by injunction, the court was unable to stop the unauthorized use of plaintiff's likeness in defendant's advertising). *Cf. generally* Pavesich v. New England Life Ins. Co., 122 Ga. 191, 50 S.E. 68 (1904) (granting plaintiff the right to withdraw from the public view and enjoining defendant from intruding thereupon by using plaintiff's likeness in defendant's advertising).

[30] *See infra* Part III. A.

[31] This system was developed specifically to the specifications provided by the targeted users, but later became generalized and marketed as Messenger by On-Line Software International, Inc. It included both a queued messaging facility which stored messages on a database for retrieval by receiving user and a "quick-send" function which sent directly to a user, if that user was signed on to the system, but contained no ability to save a quick-send message for later delivery, or re-delivery. The author of this Note can attest to the specifications of this software, as he was also the author of the prototype product.

[32] The designers requested a "pose" facility, allowing the system administrator to have terminal A "pose" as terminal B and receive a copy of all terminal B message traffic. Care was taken to inform users that this function was included in the system, and that therefore their messages were not to be considered confidential. Again, the software product, and this Note, have the same author.

[33] Commercially marketed products competing with Messenger, such as (what is today) Interpost offered by Fischer International Systems Corp., employed functionally similar designs, although omitting the "quick-send" function. The earlier version was unique in that it ran on more than just IBM mainframes and UNIX servers. The database and supervisory facilities, however, remained. The author of this Note became privy to the internal design when offered the job of managing the development of this product for Fischer. Even non-mainframe products such as Orion, developed in the mid-80's and marketed by Orion Network Solutions, Ltd. of Ilkley, England, has a similar design. The author has marketed and supported this product for the North American midrange market since 1995.

privacy concerns did not emerge until years later when complaints over management audit and review of messages and message traffic first arose.[34]

Initial claims of privacy violations were made on ethical grounds. Alana Shoars, plaintiff in the first claim of violation of E-mail privacy,[35] said in bringing her case against Epson America: "You don't read other people's mail, just like you don't listen to their phone conversations."[36] Interestingly, Ms. Shoars's claims fell largely on deaf ears in the data processing world. The CIO of Bank of Boston Corporation quipped that a discussion of ethics among Information Systems ("IS") professionals "would be a very short meeting."[37] Bank of Boston found one employee using the corporate computer to handicap horse races and another running a side business, and terminated them without worry or concern for any invasion of privacy in identifying such abuses.[38] In 1990, the director of the Electronic Mail Association asserted that the majority of U.S. corporations agreed with Epson that privacy rights take a back seat to the needs of the body corporate.[39]

B. Employer Justification

While one may question the morality of monitoring personal communications, it is difficult to ignore the corporate justification. First, the employer provides the system on which E-mail is processed, and has the right to maintain its own system. Such a right includes the right to monitor activity. So held the California Appellate Court in *Shoars v. Epson America, Inc.*,[40] which holding has been used as a defense against subsequent claims.

Second, a 1998 survey reported that forty-five percent (45%) of the employees surveyed reported they had engaged in unethical actions related to technologies such as E-mail, of which 60% (27% of the total) admitted they had committed a "highly unethical or illegal act."[41] A 1999 survey by the American Management Association concluded that sixty-seven percent (67%) of U.S. companies conduct some form of electronic monitoring.[42] Remedial and punitive action often results when abuses are detected[43] and, while one

---

[34] *See infra* cases cited in Part III. B.

[35] Shoars v. Epson America, Inc., No. B073243 (Cal. Ct. App. 1991), review denied, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994). Claim was brought for wrongful termination after Ms. Shoars was fired for questioning the alleged corporate monitoring of employee messages.

[36] Glenn Rifkin, *The Ethics Gap; Despite Growing Attention, Many IS Managers Say It's Not My Job*, COMPUTERWORLD, Oct. 14, 1991, at 83.

[37] *Id.*

[38] *Id.*

[39] Jim Nash, *E-mail Spurs New Privacy Debate*, COMPUTERWORLD, Oct. 15, 1990, at 78.

[40] Shoars v. Epson America, Inc., No. B073243 (Cal. Ct. App. 1991), review denied, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994).

[41] *See* DAVID M. SAFON, ESQ. & WORKLAW NETWORK, WORKPLACE PRIVACY: REAL ANSWERS AND PRACTICAL SOLUTIONS 93 (2000) (Neither unethical nor illegal is defined therein).

[42] *See id.*

[43] *See id.* (Abuses include diversion of corporate resources for personal uses, sexual harassment, and transmission of unapproved material, be it pornography of corporate secrets).

might liken such action to bailing the ocean with a teaspoon, if there is enough publicity for the detected offenders, the deterrent effect may justify the effort.[44]

Third, an employer sued for harassment may assert an affirmative defense if that employer has taken all reasonable measures to avoid or correct a problem.[45] This assertion requires diligence in policing the workplace, including the communications to which employees may be subjected. If an employer could reasonably have known of a problem, and failed to take action, a harassed, discriminated against, or simply disgruntled employee could bring an action for failure to implement a reasonable level of detection and control.[46]

C. *Employee Considerations*

Of course, there is another side to the issue, namely the negative effects of monitoring. Three concerns must be addressed, each weighing against such activity.

First is the ethical question of electronic monitoring per se. Ms. Shoars contended that "right is right, and wrong is wrong. There is no in-between."[47] She found support from Mike Godwin, legal counsel for the Electronic Frontier Federation, who opined "that monitoring E-mail or searching through electronic files is flat-out wrong. 'It's inconceivable to think of a circumstance where you should look at anybody else's electronic mail.'"[48] While some companies place corporate concerns above those of the employee,[49] other firms agree with Shoars. "If it's not addressed to you, it's not yours."[50]

Second, pragmatic employers must consider the morale effect of monitoring (particularly of E-mail/IM). While some commentators simply rant about sweatshop methods,[51] others look at (a) the need to allow some non-business use of employer-provided messaging systems, and (b) the negative effects of treating non-business use as "criminal" behavior.[52] Employers must also weigh the effects of the very act of monitoring, the implication that the employee needs to be "babysat," and the resultant blow to the self-esteem of the workforce on which an employer's productivity may be based.[53] Whether monitoring is used or abused, the employee response is often a feeling of non-trust, and such policies thereby risk the workforce behaving to justify such non-trust. A work environment which labors under such tension may attract a lesser caliber of employee, an employee who works solely to collect a paycheck.[54]

---

[44] To analogize: the IRS audits less than 2% of individual tax returns. Given this minimal probability of a personal audit, there is no substantial likelihood that an instance of tax abuse will be detected, yet a deterrent effect posed by the fear of the audit is created.

[45] *See generally*, SAFON, *supra* note 41, at 93-94.

[46] *Id.*

[47] Rifkin, *supra* note 36.

[48] *Id.*

[49] *See id.*

[50] Nash, *supra* note 39.

[51] *See* Gantt, *supra* note 2, at 345.

[52] *See* Kesan, *supra* note 3, at 315-17.

[53] *See id.* at 319-21.

[54] Rifkin, *supra* note 36 (quoting Mike Godwin, general counsel for the Electronic Frontier Foundation, "If I worked in a place where they reserved the right to look at my E-mail, I'd be less happy.").

Third, monitoring of E-mail is a "two-edged sword." On the one hand, "[e]lectronic documents are no less subject to disclosure than paper documents."[55] Failure to monitor may deprive an employer of a "reasonable efforts" defense to a claim of workplace harassment. On the other hand, monitoring, and not acting, may leave the employer in worse shape, having received (at least) constructive notice of a problem, but having failed to take corrective steps.

D. *Balancing of Interests*

There is a clear tension between the needs of the employer and those of the employee. There is also a dearth of precedent specific to IM. One must look elsewhere to analogous cases in the E-mail and telephony arenas, and then synthesize the rules for IM. It is important to do so with all due speed as the uncertainty of the law gives direction to neither the employer nor the employee, so the one lacks guidance as to what protection measures are legally permissible, and the other may never be confident of the privacy of her communications. The parameters of the arena need to be defined.

Clarifying the laws relating to privacy of IM serves the twin legal goals of certainty and equity. Unclarity leaves employers in a quandary over whether monitoring of employee communications is permissible while employees remain uncertain as to whether their employer is taking unfair advantage. At the same time, when laws permit multiple interpretations, such laws encourage inconsistent enforcement, which in turn equates to inequity. Clarification allows employers to plan, employees to react, and courts to behave predictably.

III. LEGAL RESPONSES

A. *Electronic Privacy Statutes*

Both Federal and state legislatures have enacted privacy statutes. In addition, claims may be brought under the common law right to privacy. A review of such statutes, and a comparison with equivalent statutes found in other countries, helps put into perspective the state of the law today. Many states modeled their statutes on federal law, and so it is instructive to commence at the federal level, and then move to the additions and changes effected by the individual states.

1. *Federal Statutes*

Any review of Federal electronic privacy statutes must perforce commence with The Electronic Communications Privacy Act (ECPA).[56] Additionally, claims have been brought under the Fourth Amendment. Furthermore, while not statutory, the CONTU report[57] provides analysis useful in analyzing both statutes and cases.

---

[55] Rowe Entertainment, Inc. v. William Morris Agency, 205 F.R.D. 421, 428 (S.D.N.Y. 2002). *See also* Anti-Monopoly, Inc. v. Hasbro, Inc., 1995 WL 649934, *2 (S.D.N.Y. 1995) ("[t]hus, today it is black letter law that computerized data is discoverable if relevant.").

[56] 18 U.S.C. §§ 2510-2522 (2000).

[57] *See infra* note 90.

a. ECPA

The Electronic Communications Privacy Act protects against unwarranted interception or retrieval of electronic communications. Title I governs interception of communications in transmission, such as wiretaps and "bugs."[58] Title II protects data post-transmission, typically once a message has been received and stored.[59] Originally enacted in 1968 as part of the Omnibus Crime Control and Safe Streets Act of 1968, the 1986 amendment specifically incorporated electronic communications, ensuring applicability to E-mail as well as telephonic communications.[60] This applies equally to both traditional E-mail and IM, as either transmission qualifies as "transfer of [information] transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric or photooptical system . . . ."[61] Also, as storage performed as part of either an E-mail or an IM function would be a "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,"[62] Title II applies as well.

i. Title I - The Wiretap Act[63]

Section 2511 of the ECPA makes it a criminal offense to "intentionally intercept[ ], endeavor[ ] to intercept, or procure[ ] any other person to intercept or endeavor to intercept, any wire, oral or *electronic* communication."[64] The code defines intercept in the prior section,[65] omitting clarification of whether interception must be made during transmission, or if subsequent retrieval from file storage is also protected. This distinction is important as Title I has more stringent exceptions than does Title II.[66] Specifically, Title I exempts (a) switchboard operators in the course of providing service,[67] (b) service providers, given judicial or executive authorization,[68] (c) law enforcement,[69] (d) parties to the communication or with the consent of one or more parties,[70] or (e) where communications may be accessible to the general public.[71] To put "teeth" into this protection, the code authorizes and enumerates fines and imprisonment for offenders.[72]

While this appears to protect against unauthorized access of E-mail, courts have held that interception requires data be captured *in transmission*, "in flight"

---

58 18 U.S.C. § 2511.
59 18 U.S.C. § 2701 (2000).
60 Pub. L. No. 99-508, 100 Stat. 1860 (1986).
61 18 U.S.C. § 2510(12).
62 18 U.S.C. § 2510(17).
63 18 U.S.C. §§ 2510-2522.
64 18 U.S.C. § 2511(1)(a) (emphasis added).
65 18 U.S.C. § 2510(4).
66 18 U.S.C. §§ 2701-2711 (2000).
67 18 U.S.C. § 2511(2)(a)(i).
68 18 U.S.C. § 2511(2)(a)(ii).
69 18 U.S.C. § 2511(2)(b)-(c), (e)-(f).
70 18 U.S.C. § 2511(2)(d) (limited to exclude interception for the purpose of criminal or tortious acts).
71 18 U.S.C. § 2511(2)(g).
72 18 U.S.C. § 2511(4).

as it were.[73] Before message transmission or after message receipt, where the data is held in electronic files, courts have held data access, rather than message interception, to be the issue,[74] in which case the Stored Communications Act controls.[75]

ii. Title II - The Stored Wire and Electronic Communications and Transactional Records Act[76]

The Stored Wire and Electronic Communications and Transactional Records Act ("the Stored Communications Act") makes it illegal to "intentionally access[ ] without authorization a facility through which an electronic communication service is provided; . . . and thereby obtain[ ] . . . access to a wire or electronic communication while it is in electronic storage . . . ."[77] As the majority of the E-mail cases[78] involved retrieval of communications after transmission and receipt, this becomes the most applicable statute. Penalties provided by the Stored Communications Act are roughly parallel to those of the Wiretap Act.[79] However, the statute's very wording provides additional exceptions. Allowing "authorized" access, rather than requiring that "one of the parties has given prior consent," permits of a wide range of interpretation,[80] and courts have found implied authorization in many cases, in particular wherever the environment provides no "reasonable expectation of privacy."[81]

Indeed, from *Shoars v. Epson America, Inc.*[82] on, courts have consistently held that E-mail, retained on an employer's computer system, creates no reasonable expectation of privacy.[83] Even where an employer assured employees that messages *would* be considered to be private, presumptions of privacy were lost once messages were sent and received.[84] Password protection and labeling files as "personal" does not suffice to trigger the requisite level of expectation.[85] For E-mail, the protection of the Stored Communications Act has been diluted by the low standard imposed by the courts in recognizing implied authorization, and the absence of any requirement for an affirmative act to grant permission.[86] How IM fares is less clear, and is discussed in greater detail in subsequent parts of this Note.

---

[73] Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 460-62 (5th Cir. 1994) (endorsing United States v. Turk, 526 F. 2d 654 (5th Cir.), *cert. denied* 429 U.S. 823 (1976)).

[74] *See infra* cases recapped in Part III. B.

[75] 18 U.S.C. §§ 2701-2711.

[76] *Id.*

[77] 18 U.S.C. § 2701(a).

[78] *See infra* cases recapped in Part III. B.

[79] 18 U.S.C. § 2701(b) (2000).

[80] *Compare* § 2701(a)(1) *with* § 2511(2)(d).

[81] *See infra* cases recapped in Part III. B.

[82] Shoars v. Epson America, Inc., No. B073243 (Cal. Ct. App. 1991), review denied, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994).

[83] *See infra* cases recapped in Part III. B.

[84] *See* Smyth v. Pillsbury Company, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

[85] *See* McLaren v. Microsoft, No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999).

[86] *See infra* cases recapped in Part III. B.

b. Fourth Amendment

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[87] While the state action requirement prohibits claims against private actors, public actors have invoked its protection, above and beyond that provided by the ECPA.[88] However, such claims have failed as courts found no reasonable expectation of privacy, and that such invasions of privacy did not rise to a level warranting protection under the Constitution.[89]

c. CONTU Report[90]

The 1978 report of the National Commission on New Technological Uses of Copyrighted Work (CONTU) addresses one fact of the distinction between interception and access in IM environments, where messages are *not* stored on computer disk files. Related to copyright's fixation requirement, CONTU concludes that loading software into a computer qualifies as the making of a copy. While no distinction is made between copying into random-access-memory (RAM) and copying to retrievable disk, or even into read-only-memory (ROM), courts have held the copy in RAM to constitute a copy, at least for the fixation requirement.[91] It is not unreasonable to then assert that RAM, or potentially even the PC terminal buffer, constitutes an electronic storage device from which an electronic message may be accessed, further weakening 18 U.S.C. § 2510. This is discussed in greater detail in Section IV, *infra*.

2. State Statutes

Over thirty states have enacted statutes limiting interception or retrieval of electronic communications, generally based on the ECPA, and providing little additional protection.[92] A few such statutes warrant individual mention, addressing the tension between the needs of the employer and those of the employee at the state level.[93]

---

[87] U.S. CONST. AMEND. IV.

[88] U.S. v. Maxwell, 45 M.J. 406 (1996); U.S. v. Simons, 29 F. Supp. 2d 324 (E.D. Va. 1998).

[89] *Id.*

[90] Final Report of the National Commission on New Technological Uses of Copyrighted Works (hereinafter "CONTU") (1978).

[91] MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511, 519 (9th Cir. 1993) (using the definition of "fixed" in 17 U.S.C. § 101 where "[a] work is fixed . . . when its embodiment . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for more than transitory duration," the court held that the ability to access, and process, data so held was sufficiently non-transitory.).

[92] Adams, *supra* note 3, at 40-41.

[93] Many states, like the federal government, have considered or enacted laws governing the protection of confidential electronic information, information such as name or social security number. Some use nomenclature which makes them appear applicable to this Note, but in fact they cover different ground, and therefore are not discussed.

a. Nevada

Nevada legislated "Interception and Disclosure of Wire and Radio Communications or Private Conversations" through Chapter 200 of Title 15.[94] This statute parallels the Wiretap Act,[95] and is likewise restricted to interception of actual transmission. The statutes, however, lacks an analog to the Communications Storage Act, and so provides less protection.

Bohach v. City of Reno[96] illustrates the privacy exposure. The court found no reasonable expectation of privacy for policing officers using a city-provided computerized paging system.[97] The Police Department retrieved information from the electronic files of the paging service provider, which act did not constitute an interception.[98] Further, absent any reasonable expectation of privacy, the found that an authorization to view these files could be implied.[99] In dicta, the court commented that the lack of privacy expectation could constitute an implied prior consent, not simply an implied authorization.[100] This would seem to eviscerate even the limited protection of The Federal Wiretap Act.

b. Maryland

The Maryland statute on Wiretapping and Electronic Surveillance[101] closely parallels the Wiretap Act. Like the federal statute, the state statute protects electronic communications with wording akin to the ECPA's 1986 amendment.[102] The state statute however, provides no protection of communications post-transmission, i.e. once placed in electronic storage.[103] As is the case in Nevada, the Maryland state statute provides less employee protection than the federal statute.[104]

c. Connecticut

Atypical of state enactments, Connecticut's general statutes require notification of any monitoring.[105] The "Protection of Employees" statute requires, absent reasonable expectation of criminal misconduct or other improper behavior, specific notification be provided to employees subject to monitoring, informing them of the type, or types, of monitoring to which they may be sub-

---

[94] NEV. REV. STAT. 200.620 (2003).
[95] 18 U.S.C. §§ 2510-2522 (2000).
[96] 932 F. Supp. 1232 (D. Nev. 1996).
[97] *Id.* at 1236-37.
[98] *Id.* at 1236.
[99] *Id.* at 1237 (continued use absent reasonable expectation privacy implies consent to employer retrieval and viewing).
[100] *Id.*
[101] MD. CODE ANN., Cts. & Jud. Proc. § 10-402 (2003).
[102] 18 U.S.C. §§ 2510-2522 (2000).
[103] Elise M. Bloom et al, *Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety*, 29 WM. MITCHELL L. REV. 897, 914 (2003).
[104] *See generally,* Douglas B. Topolski, *Employee Privacy Rights in the Electronic Workplace*, 35-FEB MD. B.J. 40, 42 (2002) (citing Ferman v. Sheppard, 130 Md. App. 67, 73 (1998), reverting to the reasonable expectation of privacy test, and asserting that, regardless of apparent protection by statute and common law, careful employers can reduce or eliminate the E-mail privacy rights of their employees).
[105] Bloom, *supra* note 103, at 914.

ject.[106] Use of employer-provided facilities after notification may indicate consent to monitoring or interception. Nonetheless, the affirmative notification by the employer alerts the employee to the monitoring or interception activity.

While this notification provision does not specifically affect access to stored messages, it does at least constitute a level of privacy protection for the employee by eliminating clandestine monitoring. By extension, absent notification, the employee has a raised standard of expectation, justifying a reasonable expectation of privacy.

d. Delaware

Delaware's "Notice of Monitoring of Telephone Transmissions, Electronic Mail and Internet Usage" statute goes beyond the Connecticut statute,[107] requiring that notice of monitoring either be provided on a daily basis, or in writing and acknowledged by the employee.[108] Further, employers violating this requirement "*shall be* subject to a civil penalty,"[109] unlike the Connecticut statute where a fine *may be* levied.[110]

e. Massachusetts

Massachusetts takes a far more general approach, providing that "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right in connection therewith to award damages."[111] This parallels the protection against "unreasonable searches and seizures" provided in the Fourth Amendment.

The Massachusetts statute refers specifically to oral and wire communications, not electronic.[112] However, while federal statutes define wire communications as "aural transfer," i.e. transmission of sound,[113] the Massachusetts definition is broader, including "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception."[114] Whether this definition includes electronic communications is not clear, especially with the advent of wireless networking.

f. State Law Recap

While many states have enacted statutes addressing privacy of communications, such statutes provide minimal additional protection above and beyond the federal code. State statutes either parallel the Wiretap Act, providing no protection for stored communications, or omit mention of electronic communications altogether. Even statutes such as those enacted in Connecticut and Del-

[106] C.G.S.A. § 31-48d(b)(1)-(2) (2003).
[107] DEL.CODE ANN. tit. 19, § 705 (2003).
[108] DEL.CODE ANN. tit. 19, § 705(b).
[109] DEL.CODE ANN. tit. 19, 705(c) (emphasis added).
[110] CONN. GEN. STAT. § 31-48d(c) (2003) (emphasis added).
[111] MASS. GEN. LAWS ch. 214 § 1B (2003).
[112] MASS. GEN. LAWS ch. 272 § 99.
[113] 18 U.S.C. § 2510(1) (2000).
[114] MASS. GEN. LAWS ch. 272 § 99(B)(1).

aware, requiring employer notification of monitoring to be performed, exclude access of stored communication records, i.e., mail already sent and received.

3. *State Constitutions*

While many states have constitutional protections paralleling those of the Fourth Amendment, these provisions generally only apply to actions committed by state actors.[115] California has extended these constitutional protections to include the behavior of private employers,[116] but cases alleging violations of E-mail privacy in California have been dismissed due to the absence of a reasonable expectation of privacy.[117] New Jersey has recognized a state constitutional right of privacy and the Alaska Supreme Court articulated a basis for a "public policy supporting privacy,"[118] potentially foreshadowing a trend toward "state constitutional privacy protections for private sector employees,"[119] but such changes come slowly, when they come at all.

4. *Common Law*

Plaintiffs have asserted claims under the common law "right of privacy" to circumvent the limitations of the ECPA and state equivalents.[120] However, to assert invasion of privacy by "intrusion into seclusion," plaintiffs must meet a three-part test, demonstrating (1) an intrusion, which (2) is "highly offensive," and that (3) "the employee had a reasonable expectation of privacy."[121] The second prong has proven to be the difficult hurdle, particularly as electronic monitoring typically involves no physical invasion.[122,123]

The Alabama Supreme Court declined to hold an invasion "offensive or objectionable" where the employer demonstrated a business need for the monitoring.[124] California courts have held likewise, denying tort claims of invasion

---

[115] Lee, *supra* note 2, at 149-50; Gantt, *supra* note 2, at 389-90; SAFON, *supra* note 41, at 101-02; Jarrod J. White, *E-Mail@Work.com: Employer Monitoring of Employee E-Mail*, 48 ALA. L. REV. 1079, 1188 (1997).

[116] Gantt, *supra* note 2, at 389.

[117] *See infra* discussion of *Shoars v. Epson America, Inc*; *Flanagan v. Epson America, Inc*; and *Bourke v. Nissan Motor Co.* in Part III. B. 1.

[118] Lee, *supra* note 2, at 150.

[119] *Id.*

[120] Kesan, *supra* note 3, at 302-04; White, *supra* note 115, at 1094-98.

[121] *Id.* citing Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI-KENT L. REV. 285, 290 (1996).

[122] *Id.*; Lee, *supra* note 2, at 162-63.

[123] Alternatively, a four-prong test is often referenced, where plaintiff is required to show a. intentional intrusion, b. upon a private activity, which is c. "highly offensive to a reasonable person," and that d. such intrusion violated a reasonable expectation of privacy. Such test is equally difficult to meet. Adams, *supra* note 3, at 41-42.

[124] White, *supra* note 103, at 1096 (analyzing the holding in *Nipper v. Variety Wholesalers, Inc.*, 638 So. 2d 778 (Ala. 1994)).

of privacy,[125] and directing issues of E-mail privacy to the jurisdiction of the legislature.[126]

5. International Law

The United States is not alone in facing this issue; other industrialized countries are facing the same tensions and uncertainties.

The U.K. provides protection much like that of Title I of the ECPA, solely covering interception, and leaving access unprotected. However, within the British interception statute, consent to publication requires acquiescence from *all* parties, including non-employees,[127] providing a higher level of protection in one aspect, while totally excluding instances of data retrieval.

France goes further in their notification requirement, obligating employers to notify labor representatives of *any* monitoring in the workplace. Data that could identify an individual may only be collected subsequent to a filing with the Commission Nationale de l'Informatique et des Libertes, an agency created by France's Law on Data Processing and Liberty.[128] Furthermore France, the source of the *droit morale*, stresses in its Civil Code that individual privacy "trumps" an employer's economic concerns.[129]

Moving "up the protection ladder," Germany goes yet one step further, eliminating distinctions between interception and access, and only allowing interference with the rights of personal privacy when permitted by legislation, collective bargaining agreement, or authorization from the company works council. Monitoring is prohibited absent employee consent, unless either a compelling interest or the prevention of a crime is involved.[130]

At the top rung is Italy, where worker dignity trumps property rights.[131] Statutes bar monitoring of particular individuals, and even general monitoring for safety or productivity requires the approval of work councils.[132] As an employer's property rights are secondary, retrieval of private files (potentially including E-mail) from an employer's computer system is prohibited.[133]

Outside of the United States, employee rights and dignity receive greater emphasis. These concerns for the interests of the employee typically emerge as limitations on implied consent and notice requirements. Inconsistency predominates. However, this Note discusses the situation in the United States, and

---

[125] HR Advisor, July-Aug. 1995, at 15, 18 (1990 decision of California Superior Court, Los Angeles County) (referring to *Flanagan v. Epson America, Inc.*, No. BC007036 (Cal. Super. Ct. 1991)).

[126] HR Advisor, July-Aug. 1995, at 15, 18 (1990 decision of California Superior Court, Los Angeles County) (referring to *Shoars v. Epson America, Inc.*, No. B073243 (Cal. Ct. App. 1991), review denied, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994)).

[127] Regulation of Investigatory Powers Act (RIPA), 2000, c.23 (Eng.).

[128] Kesan, *supra* note 3, at 308.

[129] *Id.* at 308-09.

[130] *Id.* at 309-10.

[131] *Id.* at 310 (citing GINO GIUGNI, LO STATUTO DEI LAVARATORI [COMMENTARIO OF THE LABOR STATUTE], Giuffre', Milano (1979)).

[132] *Id.* at 310 (citing Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 394 (2000)).

[133] *Id.* at 310.

international law provides merely perspective and guidelines to such discussion.

B. Case Law

As there is a dearth of judicial precedent governing privacy of IM, history must be derived by analogy from cases of intrusions into E-mail and other electronic data. From the seminal cases in the early 1990's to today, decisions generally focused on questions of reasonable expectation of privacy, interception vs. access, and implied consent.

1. Seminal Cases

In the early 1990's, California courts decided three cases of E-mail intrusion (described below).[134] The trade press in the computer industry showed both pragmatism and outrage,[135] foreshadowing the need to provide guidance and direction in both the ethics and the mechanics of E-mail privacy, while anticipating the antipathy towards doing so.[136]

Whether reading E-mail constitutes interception of electronic communications or retrieval of communications storage determines the choice of applicable statute. Finding that interception requires capture of data in flight, courts decided these cases on the communications storage statutes, statutes decidedly more favorable to the employer.[137]

a. *Shoars v. Epson America, Inc.*[138]

In 1990, Epson America, Inc. fired Alana Shoars for protesting the corporate monitoring of employee E-mail messages.[139] Ms. Shoars took a very moral-based stand. "Right is right, and wrong is wrong. There is no in-between."[140] Shoars brought a wrongful termination suit under the common law right to privacy, but the court dismissed it, finding that Shoars had no reasonable expectation of privacy, and observing that any such expectation must be established by the legislature.[141]

b. *Flanagan v. Epson America, Inc.*[142]

Seven hundred workers at Epson filed a class action suit, alleging a violation of their right to privacy when their employer reviewed their E-mail absent

---

[134] Gantt, *supra* note 2, at 398-401; Lee, *supra* note 2, at 142; White, *supra* note 115, at 1096-97.

[135] Rifkin, *supra* note 36.

[136] *Id.* ("[W]e have to be leaders in ethical issues . . ." but "[t]here is no evidence that the IS community is willing . . . to do that.") (quoting J. Jeffrey Smith, assistant professor at Georgetown University, School of Business Administration.)

[137] Gantt, *supra* note 2, at 399.

[138] Shoars v. Epson America, Inc., No. B073243 (Cal. Ct. App. 1991), *review denied*, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994).

[139] Rifkin, *supra* note 36.

[140] *Id.*

[141] White, *supra* note 115, at 1096-97 (citing *Shoars v. Epson America, Inc.*, No. B073243 (Cal. Ct. App. 1991), *review denied*, No. S040065, 1994 Cal. LEXIS 3670 (Cal. 1994)).

[142] Flanagan v. Epson America, Inc., No. BC007036 (Cal. Super. Ct. 1991).

employee consent.[143] A Los Angeles Supreme Court judge dismissed the suit, ruling that there was no violation of privacy, and that companies are entitled to manage and maintain their systems.[144]

c. *Bourke v. Nissan Motor Co.*[145]

Employees terminated after their supervisor discovered that their E-mails contained "inappropriate jokes and language" brought suit for invasion of privacy.[146] Like *Shoars* and *Flanagan*, this case failed for lack of a reasonable expectation of privacy on the part of the employees, particularly as the employees had been informed that computer use should be limited to business purposes.[147]

2. *Cases of Retrieval vs. Interception*

Claims brought under Title I of the ECPA are more difficult to maintain than those brought under Title II,[148] highlighting the importance of categorizing the claimed infringing activity as either interception (subject to Title I), or retrieval (subject to Title II). The contemporaneous access requirement attributable to interception has proven key,[149] even in cases beyond the scope of E-mail.[150]

a. *Garrity v. John Hancock Mutual Life Insurance Co.*[151]

Defendant investigated plaintiff's E-mail folders subsequent to a complaint by a co-worker of receiving sexually explicit E-mail from plaintiff's husband.[152] Plaintiff asserted violation of the Massachusetts Wiretap Statute[153] prohibiting interception of specified types of communications. However, as the messages had already been transmitted and stored prior to employer's access, the court held that such access did not qualify as an interception, and denied the claim. While applying state law, the court analogized to the ECPA for its analysis.[154] Further, the court opined in dicta that, even had the Wiretap Statute applied, so would the "ordinary business exception," and the action would have been lawful in any event.[155]

---

[143] Jim Nash, *E-mail Lawsuit Cranks Open Privacy Rights Can of Worms*, COMPUTERWORLD, Aug. 13, 1990, at 7.
[144] Jim Nash & Marua J. Harrington, *Who Can Open E-Mail?; Nissan Latest to be Sued for Privacy Invasion*, COMPUTERWORLD, Jan. 15, 1991, at 1.
[145] No. B068705 (Cal. Ct. App. 1993).
[146] Nash & Harrington, *supra* note 144.
[147] White, *supra* note 115, at 1097.
[148] *See supra* discussion in part III.A.1.a.
[149] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876-79 (9th Cir. 2002).
[150] *E.g.* Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (involving the use of a digital paging system provided by the City of Reno).
[151] No. Civ.A.00-12143, RWZ, 2002 WL 974676 (D. Mass. May 7, 2002).
[152] *Garrity*, 2002 WL 974676, at *1.
[153] MASS. GEN. LAWS ch. 272 § 99(B) (2003).
[154] *Garrity*, 2002 WL 974676, at *3.
[155] *Id.* (citing *Restuccia v. Burk Tech., Inc.*, 1996 WL 1329386, at *2-3 (Mass. Super. 1996).

b. Konop v. Hawaiian Airlines, Inc.[156]

Plaintiff claimed the defendant had unlawful accessed the plaintiff's secure website in violation of, *inter alia*, the Wiretap Act[157] *and* the Stored Communications Act.[158] Although this case involved access to the plaintiff's website, not E-mail, the court analogized to facts to those of prior E-mail cases,[159] denying the wiretap claim because the data was not intercepted during transmission, but was rather accessed from electronic storage, thereby making Title I of the ECPA inapplicable.[160]

Having held that Title I did not control, the court then turned to the Stored Communications Act, Title II of the ECPA.[161] Defendant used a sign-on, a user ID and password, obtained from a third party under false pretenses.[162] As plaintiff had not provided the sign-on, the court did not find the access to be authorized, leaving that issue to be resolved at trial.[163]

c. Steve Jackson Games Inc. v. United States Secret Service[164]

Unlike several other cases brought against the federal government, in this case the plaintiff asserted no Fourth Amendment violations, claiming only violations of the Wiretap Act.[165] Referring both to definitions contained within the statute and the legislative intent of the ECPA, the court held that "Congress did not intend for 'intercept' to apply to electronic communications when those communications are in electronic storage."[166] Further, the court analyzed the reasons that plaintiffs might prefer to bring claims under Title I rather than Title II of the ECPA.

> Stored wire communications are subject to different treatment than stored electronic communications. Generally, a search warrant, rather than a court order, is required to obtain access to the contents of a stored electronic communication. *See* 18 U.S.C. § 2703(a) . . . . *See* James G. Carr, *The Law of Electronic Surveillance*, § 4.10, at 4-126–4-127 (1994) (citing H.R. Rep. No. 99.647, 99th Cong., 2d Sess. 67-68 (1986)).[167]

In other words, the standard of authorization has been lowered, at least according to the Fifth Circuit.

d. Bohach v. City of Reno[168]

Plaintiff police officers alleged violations of Title I of the ECPA and the Fourth Amendment when the City of Reno investigated their message traffic on

---

156 236 F.3d 1035 (9th Cir. 2001), *withdrawn and filed* 302 F.3d 868 (9th Cir. 2002).
157 18 U.S.C. §§ 2510-2522 (2000).
158 18 U.S.C. §§ 2701-2711 (2000).
159 *See Konop*, 302 F.3d at 876-77.
160 *Id.* at 879.
161 *Id.* at 879-80.
162 *Id.* at 873.
163 *Id.* at 880.
164 36 F.3d 457 (5th Cir. 1994).
165 18 U.S.C. §§ 2510-2522 (2000).
166 *Steve Jackson Games*, 36 F.3d at 462.
167 *Id.* at 462, n. 7.
168 932 F. Supp. 1232 (D. Nev. 1996).

the city's "Alphapage" text messaging system.[169] Holding that messages retrieved from electronic storage are de facto *not* intercepted, the court ruled that the city could not be liable for interception, and that any claims had to be viewed under Title II rather than Title I of the ECPA.[170]

3. Claims of Fourth Amendment Violations

The Fourth Amendment only protects against unreasonable searches or seizure by government actors.[171] While the U.S. Government as an employer would be subject to suit under this protection, courts have held that a search of electronic media is only unreasonable if reasonably unexpected, and so to assert a claim of a violation of the Fourth Amendment for impinging on the privacy of E-mail or other electronic data, a plaintiff must establish a "'subjective expectation of privacy' which is objectively 'reasonable.'"[172]

a. United States v. Maxwell[173]

Plaintiff asserted that his employer, the U.S. Air Force, accessed his E-mail in violation of his Fourth Amendment protection against unreasonable or unwarranted searches.[174] The court did not deny that the plaintiff may have had a reasonable expectation of privacy, violation of which might be actionable.[175] However, the court held that, once E-mail messages are sent to a growing number of recipients, privacy expectations diminish and soon disappear.[176] While this reasoning only provided the Air Force with access to those E-mails which had been broadcast, the material found in those E-mails in turn provided sufficient grounds for further search under a valid search warrant.[177]

b. United States v. Simons[178]

Defendant Simons, employed by the Federal Bureau of Information Services within the CIA, was charged with dealing in child pornography. Defendant asked the court to exclude evidence found on his office computer, asserting that searching his computer was a violation of his Fourth Amendment protection against unreasonable searches.[179] The court held that, to assert protection under the Fourth Amendment, a claimant must first have an actual or "subjective expectation of privacy [which] society recognizes as reasonable."[180] As defendant was aware of the employer's official policy regarding Internet use, including the potential of audit, defendant had no such expectation of privacy.[181]

---

169 *Id.* at 1233.
170 *Id.* at 1236.
171 U.S. CONST. amend. IV.
172 U.S. v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996).
173 *Id.* at 406.
174 *Id.* at 415.
175 *Id.* at 417.
176 *Id.* at 418-19.
177 *Id.* at 419.
178 29 F. Supp. 2d 324 (E.D. Va. 1998).
179 *Id.* at 326.
180 *Id.*
181 *Id.* at 327.

Additionally, the defendant claimed that his employer had violated Title I of the ECPA, as the search had been performed without a search warrant.[182] The court held that, as data was not being transmitted at the time of its access, no interception had been committed, and therefore no warrant had been required.[183]

4. *"Other" Cases*

Several other cases establish or illustrate specific points of importance in this discussion.

a. *Smyth v. Pillsbury Company*[184]

The plaintiff's employer terminated plaintiff for making inappropriate and unprofessional comments in E-mail messages to his supervisor, including a threat to "kill the backstabbing bastards" and a reference to a company party as the "Jim Jones Koolaid affair."[185] The plaintiff sued for wrongful termination, claiming the invasion of privacy "threaten[ed] clear mandate[ ] of public policy,"[186] "an especially narrow" exception to the at-will employment policy.[187] Although the employer had affirmatively assured employees that the privacy of communications would be respected, the court nonetheless held the voluntary transmittal of messages across a system commonly accessible to employees deprived the sender of any expectation of privacy that sender might have held.[188] So, even where an employer provides promises of confidentiality, subsequent events may negate the effect of such assurances.

b. *Wesley College v. Pitts*[189]

This case differs from the other cases discussed in that the employer brought the claim for wrongful access by the employee, rather than the reverse. Evidence indicated that the defendant had read E-mail which was displayed on a user's screen despite not being its intended recipient.[190] The court ruled this did not violate the ECPA, despite the plaintiff's attempt to classify the screen as the interception device rather than simply a display vehicle.[191] The court concluded that such unintentional action could not constitute the affirmative action required under the statute.[192] Further, as the E-mail was accessed after it had been transmitted (and received), no interception had occurred.[193] Interception

---

182 *Id.* at 329.
183 *Id.* at 329-30.
184 914 F. Supp. 97 (E.D. Pa. 1996).
185 *Id.* at 98.
186 *Id.* at 99.
187 *Id.*
188 *Id.* at 101.
189 974 F. Supp. 375 (D. Del. 1997).
190 *Id.* at 381.
191 *Id.* at 384-87.
192 *Id.* at 382.
193 *Id.* at 386-87 (as communication was not captured *"en route* to its intended recipient" interception did not occur).

must occur before a message reaches electronic storage.[194] This did not occur; therefore, there was no interception.[195]

c. McLaren v. Microsoft[196]

Microsoft confiscated plaintiff's office computer, and reviewed and disseminated E-mail stored in a "personal folder," for which action the plaintiff asserted an invasion of privacy.[197] The court held such a claim required demonstrating either an invasion of plaintiff's physical domain, or behavior rising to the level of spying. Neither was shown here.[198] The court noted that Microsoft provided the computer on which the messages were stored, and so the E-mails were not plaintiff's "personal property but . . . an inherent part of the office environment."[199] Files on the plaintiff's computer were also stored on the defendant's routing computer (i.e., the server), transmitted over a public network, and at some point handled by at least one third party, and so no reasonable expectation of privacy existed.[200] Finally, even if the messages were private, defendant had not committed what a reasonable person would consider a "highly offensive invasion," and so the court ruled that no invasion of privacy had occurred.[201]

d. Deal v. Spears[202]

Title I of the ECPA provides exceptions and exemptions to the prohibition on electronic interception and disclosure.[203] Where the interception uses facilities obtained from the provider of communication services, and occurs in the "ordinary course of business," the "telephone extension" exemption applies.[204] However, where the employer purchases the device from a third party (here, Radio Shack) and installs that equipment itself, this exemption is not applicable.[205]

e. Schmerling v. Injured Workers' Insurance Fund[206]

The Maryland Wiretapping and Electronic Surveillance Act[207] closely parallels Title I of the ECPA, even to the "telephone extension" exemption.[208] In *Schmerling*, the defendant purchased a third party recording device solely

194 *Id.* at 389.
195 *Id.* at 390.
196 No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999).
197 *Id.* at *1.
198 *Id.* at *3.
199 *Id.* at *4.
200 *Id.*
201 *Id.* at *5.
202 980 F.2d 1153 (8th Cir. 1992).
203 18 U.S.C. § 2511(b); 18 U.S.C. § 2510 (by restrictive definitions, *see* note 204 *infra*).
204 18 U.S.C. § 2510(5)(a)(i) exempts interception where the intercepting device is "furnished . . . by a provider of wire or electronic communication service in the ordinary course of its business" and the employer uses the device "in the ordinary course of its business."
205 *Deal*, 980 F.2d at 1158.
206 795 A.2d 715 (Md. App. 2001).
207 MD. CODE ANN., Cts. & Jud. Proc. § 10-401 (2003).
208 *Schmerling*, 795 A.2d at 716.

for intercepting conversations, which device added no functionality to the operation of the telephone system.[209] The court followed the reasoning of *Deal*[210] and refused to recognize an exemption to the prohibition on message interception.[211]

5. Summary

Generally, courts have found Title I of the ECPA inapplicable to E-mail communications. Categorizing access as "retrieval" rather than "interception" lowers the standard required by the courts of an employer to avoid being found to have acted improperly. Similarly, courts have hesitated to find E-mail "snooping" to be the sort of "highly offensive invasion" which would lead to a finding of invasion of privacy. Only in those cases where the technical details permit a finding of interception do the courts appear willing to find the offending party culpable.

This may not be the case with Instant Messaging. Since there may be no central message repository for Instant Messages, Title I may be more applicable than Title II. Claimants may invoke specific statutory language rather than trying to justify a reasonable expectation of privacy. This discussion is carried forward in the next Part.

IV. ANALOGIZE AND DISTINGUISH

A. What IM Is, And What IM Is Not

Precedent and judicial interpretation of privacy of electronic communications almost exclusively involve E-mail, private websites, or telephone monitoring. Few cases have involved IM, which is not unexpected given the newness of the technology. Categorizing IM within the statutory framework is therefore problematic. While IM is different than E-mail, it is technically subject to the same sets of regulations.[212] However, Instant Messages are often *not* retained in electronic storage, only residing temporarily on the network and the recipient's screen.[213] It is even likely that unstored Instant Messages may not be discoverable, as cases refer to computer files, and a message that is never stored is not a file.[214] While E-mail is frequently likened to "snail mail," IM is more akin to telephone conversation.

IM qualifies as electronic communication as does E-mail. However, strong differences distinguish them. The requirement for data storage, or lack of such requirement, is likely the major distinction for present purposes. It may

---

[209] *Id.* at 726.

[210] Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992).

[211] *Schmerling*, 795 A.2d at 727.

[212] The ECPA refers to "electronic" communications, and both IM and E-mail fall under this umbrella.

[213] Frank C. Morris, *The Electronic Platform: E-Mail and Other Privacy Issues in the Workplace*, 20 NO. 8 CILW 1, 3 (2003).

[214] *See generally*, Antioch, Co. v. ScrapBook Borders, Inc., 210 F.R.D. 645, 651-53 (D. Minn. 2002), on the analysis of electronic documents and files which may have been stored, but subsequently deleted, finding that such files are still discoverable, but only if they can be reconstructed. For messages never stored, reconstruction would not be available, and hence discovery may be precluded.

be inappropriate to apply the logic of Title II of the ECPA rather than Title I.[215] If a message is not stored, and is observed when sent, the access resembles a wiretap more than a retrieval.

To further complicate matters, one must consider how message content is revealed, i.e. whether visually observed at point of send (or receipt), or captured by appropriate software. If the former, courts must consider surrounding circumstances to determine the reasonable expectation of privacy.[216] Where an employee works in an open area, or reads messages aloud,[217] privacy is not reasonably expected. Where the data is captured by employer-selected software, courts may look to cases where a conversation is captured on an extension phone.[218] Where use of an extension phone is not reasonable, or in the IM scenario, where data capture is either surreptitious or unreasonable, the eavesdropper may be liable.[219]

B. Analysis of IM Disclosure[220]

Due to the multiplicity of options, this analysis must be segmented and approached on a heuristic, procedural, basis. First, one must determine how the communicated message was disclosed to the employer. If disclosure was enabled by electronic data capture, it is necessary to consider where the capture functionality originated, whether within the IM software, the network or operating system, or with a third-party implementation. Then, if disclosure was via electronic capture, it is essential to analyze (a) whether management notified employees of the existence and installation of such a monitor, in conjunction with (b) the employer's policies regarding message monitoring, and (c) adherence to such policies.

1. The Observation Medium

Step one is to determine how the employer became aware of the subject message or messages, and learned of the message content. The simplest case involves one of the parties revealing the communication and its content to the employer. Such action constitutes consent, and no invasion of privacy

---

[215] 18 U.S.C. §§ 2701-2711 and 18 U.S.C. §§ 2510-2522, respectively.

[216] U.S. v. Carroll, 337 F. Supp. 1260 (D.C. 1971) (if conversation can be heard with unassisted ear, no violation is found for recording using a tape recorder no more sensitive than the human ear); Kemp v. Block, 607 F. Supp. 1262 (D. Nev. 1985) (no invasion of privacy for recording conversation which was clearly audible, under circumstances which made such audibility likely); U.S. v. Rose, 669 F.2d 23 (1st Cir. 1982) (listening to point-to-point radio transmission was acceptable where such transmission was not undertaken with reasonable expectation of privacy); U.S. v. Willoughby, 860 F.2d 15 (2nd Cir. 1988) ("recorded conversation between defendants as they stood in public area of prison was not . . . protected by federal wiretap statute").

[217] *Kemp*, 1264 F. Supp. at 1264.

[218] Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992); Schmerling v. Injured Workers' Ins. Fund, 795 A.2d 715 (Md.App. 2001).

[219] *Deal*, 980 F.2d at 1157-58.

[220] For the sake of clarity, the term disclosure is used here to include both interception and access, regardless of presence or absence of storage medium.

occurs.[221] Incidental, inadvertent observation constitutes neither unlawful monitoring, nor unauthorized access.[222] Absent definitive overt action specifically taken to obtain information regarding message content, no claim against an employer would stand.[223] This would preclude any claim in which the message is displayed on a public terminal or in a public area, unless steps had been taken to avoid general availability.

Intentional message disclosure also removes any reasonable expectation of privacy, as a party to the message has affirmatively authorized the dissemination of the message, so that the message is no longer private.[224] Rarely does a recipient guarantee privacy and, even where this does occur, any breach would be committed by the recipient, not the employer.[225]

Only where data is captured through specialized software, or specialized options of the Instant Messaging software, must the analysis proceed to the next step.

2. The Existence, and the Source, of Data Monitoring Software

To electronically monitor or intercept IM traffic, software is needed to collect messages in transmission. IM products may include such functionality, often implemented by setting a software option. Networks may have a data capture feature, which is slightly less tied to the IM application, but still an essential part of the overall operation of the system. Third-party software vendors also market tools to collect screen displays and application data traffic.[226]

The source of the data capture software may determine availability of the analog to the telephone extension exemption. Where recording equipment is integral to the functioning of a communications system, courts have found the interception not unlawful, and within the telephone extension exemption to the Federal Wiretap Act,[227] but where it is a separate stand-alone facility, implemented solely for data interception, courts have denied the exemption.[228]

---

[221] Had the party revealing the message somehow committed to maintaining secrecy, this would still hold, although the disclosing party might be liable for breach of another sort.

[222] Wesley College v. Pitts, 974 F. Supp. 375, 384 (D. Del. 1997).

[223] *Id.* Disclosure other than by data capture or sensory observation will not be considered. This Note address concerns raised by IM, not those triggered by spy cameras or peepholes.

[224] *See generally*, Snyder v. Lamb, Nos. B154091, B159265, 2003 WL 1194903 (Cal. App. Mar. 17, 2003).

[225] Note the only possible exception would be where the message is sent to a confidential branch of the employer, for example a complaint sent to Human Resources, perhaps raising a sensitive personnel issue. However, the issue addressed here is not whether the employer can send the message to a specific individual, herein the one against whom a complaint is lodged, but rather whether the employer can see it at all. A message sent to Human Resources is viewable by the organization corporate, as that organization is the desired recipient.

[226] Leading products in this area include Laplink® from Traveling Software, Inc., pcAnywhere® from Symantec Corp., WideScope® from RazLee, Ltd., and CA-Replay® from Computer Associates, Inc. The first two operate in the PC arena, WideScope in the midrange server market, and CA-Replay for mainframe networks. Each permits either direct monitoring of application screens, or capture of network traffic.

[227] *See supra* note 204.

[228] *See* Schmerling v. Injured Workers' Ins. Fund, 795 A.2d 715 (Md. App. 2002) (reversing a lower court ruling to the contrary); *see also* James v. Newspaper Agency Corp., 591 F.2d 579, 581 (10th Cir. 1979) (device installed by telephone company is presumptively

While such prior cases involved telephone communications, the analogy is strong here, as IM closely resembles telephone conversations.

Ergo, if monitoring is a function of the Instant Messaging software, or of the operating environment, the exemption may apply, but where a separately acquired (and installed) monitoring tool is used, courts would likely reject the exemption.

3. *Employee Notification*

Most users of E-mail know that they may view a message multiple times, and continue to view that message until they affirmatively delete it.[229] This general knowledge constitutes reasonable notice that messages are stored, and while a user may not know where, she knows it is somewhere. This reasonable notice does not extend to IM. As the average IM user likely expects that an already-viewed message is gone from the system, i.e., cannot be retrieved, she does *not* expect to find that message stored in a location accessible to a system administrator. In such a case, a user may in fact have a reasonable expectation of privacy for any message sent, or received, via IM.

Unless the employer has clearly informed all employees that a data capture facility is in place, *and in use*, employees may have a reasonable expectation of privacy in Instant Messages. Lack of this reasonable expectation proved the dispositive factor in many of the cases analyzed herein, but in IM, it appears that the stronger defense may be a demonstration of informed consent, or at least the implication of such consent.[230]

Since constructive or indirect notice may be considered insufficient,[231] direct, confirmed, informed notification is clearly the goal.[232] Such notice resolves any question of privacy, and constitutes valid authorization for employer access of captured data.

V. EMPLOYER PROCEDURES

As outlined above, privacy concerns arise only where message content has been captured by installed software, and potentially only where such software is not intrinsic to the Instant Messaging functionality or the system itself. If employer requirements dictate that Instant Messages must be tracked, then steps must be taken to avoid liability under the ECPA,[233] or under torts such as invasion of privacy.

"telephone equipment"); Deal v. Spears, 980 F.2d 1153, 1157-58 (8th Cir. 1991) (device was not considered "telephone equipment" as it was purchased elsewhere and connected to an extension phone rather than directly to the telephone line).

[229] Some E-mail systems automatically delete messages over a certain age, but that is not important here.

[230] Kesan, *supra* note 3, at 330-32.

[231] Jandek v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981) (police officer making phone call was aware that telephone line was monitored and recorded, negating any reasonable expectation of privacy).

[232] Kesan, *supra* note 3, at 331-32.

[233] . . . or the equivalent state statutes.

A. *Notification of Monitoring*

Decisions in E-mail privacy cases often turn on the distinction between interception and retrieval. As IM typically does not generate any such database, disclosure is more likely to involve interception of messages, or at least that may be the employee's expectation. Where data monitoring occurs, the line gets even grayer between interception (by the monitor) and the subsequent retrieval to disclose the data. However, by providing employees with the proper notification of the employer's ability, and intent, to monitor electronic communications, an employer may avert any confusion.

If the employee has a rational and reasonable expectation that messages can be, and at least periodically will be, monitored, and such monitoring does subsequently occur, courts may reasonably hold that the employees, by continued use of the IM function, have implicitly authorized both the interception of, and the access to, such messages.[234] In these cases, employees would be precluded from asserting invasion of privacy or a violation of the ECPA. The issue then becomes what constitutes reasonable notification, and what steps the employer must take.[235]

B. *The Downside of Notification*

One may also want to remember that no good deed goes unpunished. Electronic data is discoverable, only if such data has been retained and may be retrieved, and court ordered production "trumps" any privacy considerations.[236] Also, employers may be held liable for the actions, or the messages, of their employees.[237] However, if the employer has a policy of *not* monitoring IM traffic, and consistently follows that pattern, then, absent notice of a problem the employer cannot be held liable for offensive messages. This factor must be considered, and employers must select which politically correct position provides the most benefit. On the one hand, the employer may elect to protect employee privacy at the expense of allowing questionable employee behavior;[238] on the other hand, that same employer could reasonably decide to protect employee sensitivities at the expense of employee privacy.[239]

C. *Detecting and Eliminating Unwanted Software*

A reasonable employer may provide network hardware and software, and opt to exclude Instant Messaging functionality, perhaps even ban its use. In

---

[234] *See* U.S. v. Maxwell, 45 M.J. 406, 417-19 (C.A.A.F. 1996).

[235] Kesan, *supra* note 3, at 330-31. There is also the question of grandfathered employees, and whether they can be notified after a. they have been employed, and b. after systems have been installed and put into use.

[236] Star Publ'g v. Pima County Attorney's Office, 891 P.2d 899, 902 (Ariz. Ct. App. 1994) (holding that court ordered documents must be produced absent specific proof of harm and, even should such harm be demonstrable, documents for which no harm has been shown must still be forthcoming).

[237] Kesan, *supra* note 3, at 317-21; ILLINOIS INSTITUTE FOR CONTINUING LEGAL EDUC. MAIN HANDBOOK, Ch. 16, § III.B (2000).

[238] No monitoring, which may improve employee morale but expose the employer to other harm.

[239] Monitoring, which may protect the employer from other harm, but may offend employees.

such cases, what steps may that employer take towards (a) monitoring for unauthorized installation of software such as IM, (b) removal of such software, or (c) monitoring of its use?

Monitoring may be accomplished by examining the files on the systems used by the employees. Since the hardware is owned by the employer, monitoring is permissible, preferably after notification and a stated, enforced, policy.[240] Should an employer find unwanted software to have been installed, the employer may either request the employee to remove an offending application, or perform such removal itself. Alternatively, the employee might be given the option of either removing the software or consenting to the employer's monitoring of message traffic. Provided that consent is informed, in writing, and non-ambiguous, the consent requirement of the ECPA should be satisfied.

D. To IM Or Not To IM: That Is the Question

Before considering the question of IM monitoring, an employer should carefully consider whether IM should be made available at all. While generally less of a drain on corporate computer resources than traditional E-mail, IM may trigger employee misuse and become a tool for sexual harassment, offensive or other non-professional interpersonal communications, theft of corporate secrets, and simple abuse of corporate time and resources.

Only if the benefits of IM outweigh these risks, need an employer adopt IM and then consider whether message monitoring will be beneficial or detrimental. Monitoring allows auditing of employee activity; it may also expose the employer to claims of abuse of privacy and increase employer liability for discoverable behavior by employees.

Finally, should the employer conclude that IM, and monitoring of IM, poses a net benefit, a clear and understandable company policy must be developed, communicated to all employees, acknowledged by all employees, and enforced. Only in this way can the employer minimize the exposure to claims under the ECPA, privacy torts, and statutes.

VI. CONCLUSION

Instant Messaging is the latest in a series of innovative tools arising with the growth of the Internet. While historically most E-mail privacy issues have been decided based on "store-and-forward" technology, where messages are retrieved from data storage rather than intercepted in transmission, this may not apply to IM. With a normal IM operation, the message appears only on the user's screen, and not retained elsewhere. Thus, while employers may be able to apply the findings of the CONTU report, or may install software to record all message activity, unless the user is so informed, statutes applying to data retrieval will be inapplicable.[241] Rather, wiretapping statutes would determine

[240] U.S. v. Wong, 334 F.3d 831, 839 (9th Cir. 2003) (citing U.S. v. Cormier, 220 F.3d 1103, 1108 (9th Cir. 2000) ("a person does not have a reasonable expectation of privacy in an item in which he has no possessory or ownership interest.")).

[241] Even if data capture software is implemented, so that message traffic is recorded and later accessed, if employees are not aware of such software, they may be therefore relying on a reasonable expectation. In such cases, courts are likely to look to the fact that data is

the employee's reasonable expectation of privacy, and whether the employer's business need could outweigh such expectation.

The analysis of such situations hinges on the "reasonable expectation of privacy." Whether such an expectation exists in the IM environment is largely a matter of the employer's stated and enforced policies,[242] the physical logistics of the officeplace,[243] and the behavior of messaging partners.[244]

Finally, in situations where an employer has *not* opted for Instant Messaging software on its corporate network, the employer will always retain the right to detect and delete any such unauthorized software, absent a contrary agreement with its employees.

This Note has examined the history of the law regarding the privacy of E-mail, and how such laws must be interpreted to deal with the technology of Instant Messaging. Monitoring of Instant Messages likely will involve interception of communications rather than access of stored data, and may be judged under the Wiretap Act rather than the Stored Communications Act. This limits the exemptions available to the employer and raises the employee's reasonable expectation of privacy. However, proper procedural steps by the employer may protect against such liability, notifying employees of active policies regarding the monitoring of IM traffic, and thereby gaining at least implied authorization to access any data so captured.

---

actually intercepted during transmission, and subsequently stored, making the Wiretap Act applicable with its higher hurdles for exceptions.

[242] A policy which is stated but never enforced may be more injurious than no policy at all. If employees are aware that the policy is largely ignored, implied authorization may be moot. However, in civil or criminal actions, message traffic which is subject to discovery may be ordered, and failure to produce may constitute contempt.

[243] Messages sent to users at publicly viewable workstations may have no reasonable expectation of privacy. If any casual observer has access to messages, such messages are public and have no assertable protection.

[244] One must consider the effects of "whistle-blowing" by the recipient, as a message recipient is constrained by neither any expectation of privacy on the part of the sender nor any limits on functions which may be performed on received messages, e.g., printing, forwarding, copying, etc.