Journal of Law and Policy

Volume 14
Issue 2
SCIENCE FOR JUDGES VI:
Techniques for Evidence-Based Medicine

Article 10

2006

Is What's Yours Really Mine? *Shmueli v. Corcoran Group* and Penumbral Property Rights

Lee Nolan Jacobs

IS WHAT'S YOURS REALLY MINE?: *SHMUELI V. CORCORAN GROUP* AND PENUMBRAL PROPERTY RIGHTS

Lee Nolan Jacobs[*]

> *As technology advances, the government has attempted to enact policy that protects the delicate balance between the demands for technological change and the need to protect an individual's right[s] . . . . As a nation, we have supported laws that protect us from our neighbors and our government spying on us and invading our privacy, everywhere but in the workplace.*[1]

INTRODUCTION

As computer use increasingly permeates all aspects of society, including both high level and menial employment, the notion of a legitimate property right in the ownership of both personal and work products is in a state of flux.[2] No clear doctrine exists to

---

[*] Brooklyn Law School Class of 2007; B.A. The George Washington University, 2002; M.S. The George Washington University, Information Science Technology, 2004. The author wishes to thank his parents, Ilona and Jeffrey Jacobs; grandparents, Dorothy and Al Sacks; brothers and sister, Lance and Austin Jacobs and Kara and Faran Fagen for their constant love and support. He would also like to thank "The Firm," H.H., and all of his friends that stood by him through this entire process. He would also like to express his gratitude to Prof. Wendy Seltzer, Meghan Towers, Jessica Gary, Victoria Szymczak, Kevin Morrissey, and the members of the *Journal of Law and Policy* for all of their help and hard work in creating this final product.

[1] 139 CONG. REC. S6122 (daily ed., May 19, 1993) (statement of Sen. Paul Simon).

[2] H. Joseph Wen and Pamela Gersuny, *Computer-Based Monitoring in the American Workplace: Surveillance Technologies and Legal Challenges*, 24 HUMAN SYSTEMS MANAGEMENT 165, 166 (2005). As of September 2001, 174

determine who maintains the rights to and interests in documents created and maintained with the assistance of computer networks.[3] In essence it must be asked, what happens to the employee who is able to write the great American novel during his or her unpaid break periods, while still satisfying all work requirements? Who maintains rights over the document, the employee or employer? Under the current law, this writer might not be able to retrieve his or her product if he or she was suddenly terminated. That would leave the employer with the rights to a document that is clearly not within the purview of the business and which belongs to the employee.

Recently, the Supreme Court of New York in *Shmueli v. Corcoran Group*[4] ruled that the common law concept of conversion can apply when an employer unlawfully takes a former independent contractor's personal electronic documents.[5]

---

million people—66% of the U.S. population—were using computers in their homes, schools, libraries, and work. In the workplace, 65 million of the 115 million employed adults age 25 and over, almost 57% used a computer at work. U.S. DEPT. OF COMMERCE, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET (2002).

[3] Throughout this Note's entirety, the term computer networks will be used as a catch-all to describe the tools that an employee uses to create documents. This term includes the use of a single computer using basic software applications which is not connected to a network of other computers and servers, to a fully network integrated environment where users share network resources such as file-servers, networked applications, and Internet access. *See generally* JOHN W. SATZINGER ET. AL., SYSTEMS ANALYSIS AND DESIGN 302 (2nd ed. 2002) (defining a computer network as "a set of transmission lines, equipment and communication protocols to permit sharing of information and resources.").

[4] 802 N.Y.S.2d 871 (Sup. Ct. 2005). This decision is a result of the defendant's (Corcoran Group) motion for summary judgment to dismiss Shmueli's complaint.

[5] Electronic documents refer to any type of file that is kept in an electronic format which includes is but not limited to the following: word processing, spreadsheets, and images. However, for the purposes of this Note, electronic documents will be limited to those documents which could be easily printed on paper into a classical tangible form.

> While the handwritten . . . is a 'literal' document, the computerized one is . . . 'virtual' . . . [which can] . . . transform to literal . . . by [using the] printing key function . . . Electronically written 'documents' should not be treated with less dignity . . . than ink written 'documents.' The

Although this court does hold that an independent contractor's electronic documents are subject to the tort of conversion,[6] it does not fully explain the application of property rights concerning electronic documents between traditional employers and employees.

Currently, federal law and most state law recognizes that all employees have a pre-existing personal privacy interest, as well as a security interest, in their electronic documents.[7] However, the law as it stands today affords no property protections over personal electronic documents created or maintained by employees on their employer's computer network. This Note proposes, through reasoning by interpolation (or the logical inference making based on the comparison of two apparent legal doctrines to create a third) as applied at the overlap of privacy and security interests, a property right is generated.[8]

The New York Supreme Court's decision in *Shmueli* represents a microcosm of the shortcomings of the current prevailing law. In granting an electronic document the same level of protections as its hard-copy counterpart, the *Shmueli* court's holding keeps the law somewhat in step with the pace of technological change.[9] However, as this Note argues, greater continued protection is necessary for electronic documents. The decision fails to address how computer use has made it far easier for employers to intrude upon the privacy rights of employees and thereby infringe on employee property rights as well.[10] For instance, before computers, employees had the ability to lock their documents in a file cabinet,

---

> medium of recordation whether ancient or modern should not be deemed germane.

Id. at 2-4.

[6] *Id.*

[7] See *infra* Part III for a further discussion concerning current privacy and security protections afforded to employees in the workplace.

[8] *See e.g.* Brannon P. Denning & Glenn Harlan Reynolds, *Comfortably Penumbral*, 77 B.U. L. REV. 1089, 1092 (1997). Also see *infra* Part VI for an explanation of reasoning-by-interpolation and its application to an employee's property rights in the workplace.

[9] *See infra* notes 20-21.

[10] See *infra* Part II for a further discussion concerning current employee monitoring and surveillance practices.

and if an employer were to go rifle through that file cabinet, it would be fairly easy for the employee to see that something had been moved or was missing. With computers, electronic monitoring and surveillance gives the employer the ability to monitor their employees' computer and view all files, documents—virtually everything that the employee performs on his or her computer—without the employee ever even knowing.[11] The court in *Shmueli* failed to take this into account, and therefore is only paying lip service, instead of advancing the law.

This Note argues that it is inadequate for the law to give employees the same amount of property protection over electronic documents as over paper documents. As computer usage in the workplaces continues to increase and substantially change the manner in which work actually takes place, the law must evolve and recognize the inherent property right that employees maintain over their personal electronic documents. As the rights of employees must be balanced against the rights of employers, legislatures should consider statutory protections and private parties should consider contractual remedies to ensure that the rights of all parties—both employers and employees—are protected.

Part I of this Note evaluates *Shmueli* in the context of the tort of conversion contrasted with property and privacy rights. Part II addresses methods and rationales of workplace surveillance. Further, this section examines "Acceptable Use Agreements," or private contractual agreements entered into by employers and their employees which govern the terms and conditions surrounding the use of an employer's computer network. Part III discusses applicable state and federal statutes which affect workplace monitoring and privacy. Part IV illustrates the standard applied to workplace privacy cases surrounding personal electronic documents created and maintained in the public sphere by analyzing *Haynes v. Office of the Attorney General*. Parts V and VI present the proposition that through reasoning-by-interpolation, employees maintain property rights over their documents. Part VII suggests statutory and private solutions which support the

[11] *Id.*

employer's desire to maintain a productive work environment while taking into consideration the employees' fundamental property rights over their electronic documents.

I. *SHMUELI V. CORCORAN*—THE DECISION

Sarit Shmueli, an independent contractor for the Corcoran Group Real Estate Firm, was terminated on March 18, 2002.[12] Shmueli was summoned into her supervisor's office where she received her discharge, and then returned to her desk to collect her personal belongings, including personal files stored on her computer.[13] Specifically, she sought to gain access to an electronic contact-list detailing the real estate transactions she had participated in, both before and during her tenure at the Corcoran Group.[14] However, she could not collect her file because her computer password[15] had been changed.[16] The court held that Shmueli's password presumably secured her computer documents from being read or sent to others without her consent.[17] Shmueli never gained access to the file and as a result sued the Corcoran Group for conversion—on grounds that this was an unlawful taking of her computerized contact-list.[18]

In his decision, Justice Herman Cahn relied mainly on New York's common law tort of conversion to deny the defendant's

---

[12] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 873 (Sup. Ct. 2005).

[13] *Id.*

[14] *Id.*

[15] A computer password is the unique combination of a "username" and "password" which grants a user access to his or her computer and/or network resources such as printers, file servers, and other network applications. *See* SATZINGER ET. AL., *supra* note 3, at 516.

[16] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 874 (Sup. Ct. 2005).

[17] *Id.* at 877. The expectation of privacy that a user may have concerning the secrecy of his or her password and the documents that he *secretly* stores with that password is not guaranteed. *Id.*

[18] *Id.* at 873. Shmueli also sought relief on the following causes of action: intentional infliction of emotional distress, breach of bailment, misappropriation of proprietary information, and interference with prospective business relations. *Id.* However, these additional claims will not be discussed in this Note.

motions for summary judgment.[19] In essence, Justice Cahn asked:

> [D]oes the common law tort of conversion become an extinct vestige of the past as to documents maintained on a computer, merely because traditional definitions of documents evolve over time to the point where wood pulp is no longer the only required medium upon which to record data? Does not the concept of conversion . . . [the] . . . wrongful exclusionary retention of an owner's physical property, apply to an electronic record created by a plaintiff and maintained electronically as much as it does to a paper record so created?[20]

To these questions, Justice Cahn held that the common law tort of conversion does indeed apply to electronic documents; however, he applies old law to new technology.[21] The *Shmueli* opinion traces the evolution of conversion in New York from only allowing the conversion of tangible property, such as real property, to more intangible forms like stock certificates and bank books.[22] The opinion continues to assert that just as owners still control property rights over misplaced tangible property, the same rule applies to intangible property. [23] Furthermore, Justice Cahn opined that there is no practical reason why the same level of property protections should not be applied to both tangible and intangible property.[24]

---

[19] *Id.* at 875-76.

[20] *Id.* at 874-75.

[21] *Id.* at 876.

[22] "As the nature of personal property evolved to the point where tangible documents represented highly valuable rights, such as promissory notes, stock certificates, insurance policies, and bank books, the tort of conversion was expanded by common law courts to include such documents . . . ." Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 875 (Sup. Ct. 2005) *relying on* Restatement (Second) of Torts § 242, comment d.

[23] *Shmueli*, 802 N.Y.S.2d at 875 *relying on* Hartford Accident & Indem. Co. v. Walston & Co., Inc., 234 N.E.2d 230, 232 (N.Y. Ct. App. 1968) (citation omitted) (holding that "an owner does not forfeit his ownership for failure to take good care of intangible personal property any more than he forfeits it for failure to take good care of his watch.").

[24] "There should be no reason why [a] practical view should not apply equally to the present generation of documents . . . which are just as vulnerable to theft and wrongful transfer as paper documents, if, indeed, not even more so."

In upholding the notion that intangible property can be subject to conversion, the court relied on two federal cases: *Kremen v. Cohen*[25] and *Astroworks Inc., v. Astroexhibit, Inc.*[26] Both cases present and defend the proposition that certain types of intangible property are susceptible to the tort of conversion despite the common law notion that the tort of conversion applies only to tangible property.[27] In *Kremen,* the Ninth Circuit Court of Appeals explained how tort law once delineated between tangible and intangible property[28]—namely, that conversion was originally a remedy for the wrongful taking of another's tangible property.[29] However, virtually every jurisdiction has discarded this rigid limitation to some degree.[30] In *Astroworks*, the Southern District of New York held that, while an idea itself is incapable of being converted, the tangible expression of an idea is capable of being converted.[31] Thus, an important aspect of the *Kremen* and *Astroworks* decisions is the notion that intangible property can be converted and its storage, either on paper or in electronic medium, is immaterial.[32]

Finding the aforementioned federal cases analogous to the situation presented in *Shmueli*, the New York court held that the contact-list in question was covered by the common law tort of conversion.[33] The court believed that if it did not find the contact-

---

Shmueli, 802 N.Y.S.2d at 875.

[25] 337 F.3d 1024 (9th Cir. 2003) (holding that the defendant was liable for the theft of plaintiff's Internet domain name).

[26] 257 F. Supp. 2d 609 (S.D.N.Y. 2003) (reasoning that the plaintiff sued former business partner for the conversion of business ideas for his own gain).

[27] *See Kremen*, 337 F.3d at 1030 and *Astroworks*, 257 F. Supp. 2d 609.

[28] *Kremen*, 337 F.3d at 1030.

[29] *Id.*

[30] *Id. See also* Courtney W. Franks, *Analyzing the Urge to Merge: Conversion of Intangible Property and the Merger Doctrine in the Wake of Kremen v. Cohen*, 42 HOUS. L. REV. 489, 524 (2005) (stating that "as of 1999, every state except North Dakota [had] enacted some legislation addressing electronic records . . . indicating the inroads that technology has made on our laws and society.") (citations omitted).

[31] *Astroworks*, 257 F. Supp. 2d at 618.

[32] Kremen v. Cohen, 337 F.3d 1024, 1033-34 (9th Cir. 2003).

[33] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 875 (Sup. Ct. 2005).

list convertible, then an entire class of property—electronic property—would fail to benefit from remedies of the tort of conversion.[34] Ultimately, the court held that electronic documents should not be excluded from the remedies of conversion suits just because a document was kept in electronic format rather than on paper.[35] In essence, Justice Cahn attempted to keep the law in check with the pace of technological change, but failed to actually do so. Rather than apply antiquated standards to a new breed of property, the court should have continued its forward-thinking policy and applied new law and new criterion to new technology.

Although Justice Cahn ultimately concluded that Shmueli did maintain property rights over her electronic contact-list, the holding is limited to the specific facts of this case.[36] Most notably, the court's reliance on the fact that Shmueli was an independent contractor likely signifies that the holding is inapplicable to employees in general.[37] In essence, the court is only helping Sarit Shmueli retrieve her document, and is providing little guidance to employers or employees on how to settle issues involving property rights over personal documents kept at work.[38] Under the holding in *Shmueli*, employees in traditional "at-will" work relationships have no rights to secure their personal electronic documents.[39] Limiting the *Shmueli* holding to the specific facts of the case forecloses any and all possible remedies for potential-plaintiff "at-will" employees who are aware that their electronic documents have been taken as well as those who are unaware that their documents have been taken.[40]

---

[34] *Id.* at 877. Justice Cahn continued to opine that the public would perceive that the law would be unable to evolve at the same pace as technology. *Id.*

[35] *Id.* at 876 n.4.

[36] *Id.* at 876.

[37] *Id.* at 876 n.5. "The within holdings are not intended to extend to cases involving employees (as opposed to independent contractors), as it is generally held that an employee's work product is proprietary to the employer." *Id.*

[38] *Id.* at 876.

[39] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 876 n.5 (Sup. Ct. 2005).

[40] *Id.* See *infra* Part II for a further discussion concerning how current technology affords the possibility that documents could be taken from an owner without their consent. Furthermore, the tort of conversion may be an unavailable

II. WORKPLACE SURVEILLANCE

Although *Shmueli* supports the proposition that electronic documents are susceptible to the tort of conversion,[41] the opinion lacks guidance on how employers can balance the need to protect company work product while shielding themselves from a conversion suit for an employee's personal property. Without proper guidelines as to who maintains property rights over electronic documents created or maintained on a computer, employers have begun electronically monitoring their employees in an effort to protect company work product.[42] Electronic surveillance comes in many different shapes and sizes, some of which is regulated by contracts between employers and employees. The sheer act of monitoring and the later taking of an employee's document is in effect how employers usurp an employee's property right over the electronic document.

A. How and Why Monitoring Takes Place

Lurking behind the computer that an employee uses is a set of eyes that is able to monitor almost everything that takes place during the work day.[43] The most common methods of general workplace surveillance include: recording and reviewing employees' telephone conversations; storing and reviewing employees' voicemail messages, computer files, and e-mail

---

remedy for employees whose documents are taken without their knowledge or for those employees who are aware that their documents have been taken, but who suffer no damage or losses. However, employees may be able to claim a lesser tort, such as trespass to chattels. *Compare* BLACK'S LAW DICTIONARY, Conversion (8th. ed. 2004) ("The wrongful possession . . . of another's property as if it were one's own; an act or series of acts of willful interference, without lawful justification, with an item of property in a manner inconsistent with another's right, whereby that other person is deprived of the use and possession of the property."), *with* BLACK'S LAW DICTIONARY, Trespass (8th. Ed. 2004) ("The act of committing, without lawful justification, any act of direct physical interference with a chattel possessed by another.").

[41] *Shmueli,* 802 N.Y.S.2d at 875.

[42] *See infra* Part II.A.

[43] *See* Wen, *supra* note 2, at 166.

messages; monitoring employees' Internet connections; and videotaping employees in the work environment.[44] Rather than passively copying the files, emails, or telephone calls that a user may make, employers in a networked environment can actively monitor everything that employees do at their computer. [45] This happens without an employee's knowledge because employers utilize such methods as keystroke monitoring,[46] events timeline logging,[47] application usage tracking,[48] window activity tracing,[49] and remote desktop viewing[50] which are not evident to users of the computer.

On the surface, companies may present plausible reasons for monitoring their employees, such as the protection of propriety information or the prevention of sexual harassment.[51] However, employee monitoring has generated apprehension from various groups, including libertarians, corporations, and labor unions.[52]

---

[44] AMA RESEARCH, 2001 AMA SURVEY: WORKPLACE MONITORING & SURVEILLANCE (American Management Association 2001), http://www.amanet.org/research/pdfs/ems_short2001.pdf.

[45] *See* SATZINGER ET. AL., *supra* note 3, at 302.

[46] Wen, *supra* note 2, at 167. A keystroke is the action of striking a key on the keyboard and keystroke monitoring "maintains a record of [those] keystrokes along with the window they are typed in and time stamp." *Id.* Keystroke monitoring also allows an employee to "*recreate* a 'deleted' document because the keystrokes are logged and stored even if deleted." *Id.* (emphasis added).

[47] Timeline logging records all events users performed and allows the viewing of all events in a chronological order as well as the ability to track all program initiations, website visits, document viewings and printings. *Id.*

[48] Application usage monitors and logs all applications ran by users as well as when it was started, stopped, and how long it was used. *Id*

[49] Window activity records all documents and files opened and viewed by users as well as all windows in which the user directly interacts with on the desktop, chat sessions, and username and password combinations. *Id.*

[50] Remote desktop viewing "takes snapshots of every desktop at set intervals of time, allowing managers to virtually see what is happening . . . [and allows for the] . . . remote view[ing of] what the user is doing in *real-time*." *Id.*

[51] *See* Shari C. Lewis, *Internet Monitoring: Wide Implications in Ruling on Employee Visits to Pornographic Sites*, N.Y. LAW JOURNAL, Feb. 7, 2006, at col. 1.

[52] Wen, *supra* note 2, at 166.

Each argument put forth by these different groups opposing employee surveillance relies on varied ethical, legal, or economic arguments which present managerial and moral dilemmas.[53]

Despite the lack of a conclusive argument in favor of employee surveillance, employers continue to proffer various important reasons for favoring monitoring. For example, the taping of certain activities[54] in regulated industries affords both the consumer and the company some legal protection, while the sheer act itself may merely be the simplest way for a company to maintain adequate business records.[55] Other employers report that they monitor their employees in order to keep the company's proprietary information secure because e-mail and Internet access can easily permit the information to leave company walls.[56] Joseph Wen and Pamela Gersung, noted organizational business scholars, report that disgruntled employees have the ability

> to e-mail trade secrets and confidential documents quickly and easily to a large audience. . . . [I]n fact, most security breaches come from *knowledgeable insiders*—not random hackers from the outside. By monitoring . . . usage and content, corporations argue that they are able to detect and halt security breaches. Plus the mere knowledge of increased surveillance may deter potential employee theft.[57]

In total, more than three quarters of major U.S. firms record and review the actions of their employees.[58] These employers posit

---

[53] *Id.*

[54] Employers can raise an affirmative defense against sexual harassment, when the company monitors the computer network to prevent the creation of a hostile work environment. Furthermore, states such as New Jersey are now mandating that "an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties." Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005).

[55] AMA RESEARCH, *supra* note 44, at 1.

[56] *Id.*

[57] Wen, *supra* note 2, at 167.

[58] AMA RESEARCH, *supra* note 44, at 1. The American Management Association's survey of workplace surveillance included data from almost 1,700 major U.S. firms. More than 75% of responding firms gross more than $50

that businesses that do not adequately monitor their systems leave themselves open to the unlawful and undiscovered loss or modification of proprietary business information.[59]

In addition to protecting proprietary information from abuse and theft, monitoring employee work performance allows employers to secure increased employee productivity; objective job performance-related decisions concerning hiring, firing and promotions, as well as liability protection from sexual harassment charges.[60] Most commonly, the decision to monitor frequently occurs because an employer desires to limit the amount of time their employees spend utilizing the computer for personal uses, such as sending personal e-mails or browsing the Internet.[61] Employers recognize that each moment spent using the company computer for personal use is a waste of the company's time and money.[62] Furthermore, the ability of employees with Internet access to use instant messaging services,[63] send personal emails, or participate in chatrooms[64] has caused the computer to top the coffee room or talking on the telephone as the largest waste of an employee's on-the-job time.[65] The average American worker

---

million in annual sales. Moreover, 13% of respondents gross annually more than one billion dollars. *Id.* at 2. Furthermore, an additional study in 2003, found that 92% of employers reported that they utilize some form of electronic surveillance to monitor their employees. CENTER FOR BUSINESS ETHICS, Survey: 'You've Got Mail . . . And the Boss Knows'" (Bentley College) (2003).

[59] Wen, *supra* note 2, at 167.

[60] *Id.*

[61] *Id.*

[62] *Id.*

[63] Instant messaging ("IM") software "allows users to send brief remarks that pop up on the recipient's computer screen." Frank C. Morris Jr. & Jennifer S. Recine, *The Electronic Platform: The Implications of Technology in the Workplace*, SK033 ALI-ABA 875, 892 (2004). In 2001, Americans spent over 4.9 billion minutes per month instant messaging one another, and "likely at least doubled over the next two years." *Id.*

[64] Chatrooms allow users to "instantly communicate with each other by typing a message that is instantly transmitted to others participating in the chatroom." Jennifer Kathleen Swartz, *Beyond the Schoolhouse Gates: Do Students Shed Their Constitutional Rights When Communicating to a Cyber-Audience?,* 48 DRAKE L. REV. 587, 589 n.15 (2005).

[65] Wen, *supra* note 2, at 167-68. A 2005 survey revealed that "American

admits to wasting 2.09 hours per eight-hour workday, not including lunch and other breaks.[66] Surfing the Internet was the largest time wasting activity, with almost 45% of all respondents reporting that they waste time at work browsing the Internet.[67] In total, almost $340 billion per year will be spent on paying workers for surfing the Internet while at work.[68] Additionally, because electronic monitoring and surveillance is objective,[69] it allows for employee evaluations and decisions concerning promotions and terminations based on the results—free from prejudice, favoritism, or other subjective reasons.[70] Objective decisions discourage disgruntled or former employees from claiming unfair treatment or wrongful termination.[71]

Besides the need to protect the corporation itself, in terms of trade secrets or productivity, businesses and corporations nowadays must take a proactive approach to protecting their employees from sexual harassment by other employees, as

---

workers are wasting more than twice the time Human Resource managers expect." Dan Malachowski, *Wasted Time at Work Costing Companies Billions*, SALARY.COM, July 11, 2005, http://www.salary.com/careers/layoutscripts/crel_display.asp?tab=cre&cat=nocat&ser=Ser374&part=Par555.

[66] *Id.*

[67] *Id.*

[68] In total, $759 billion will be spent on paying employees salary for expected work which will never be preformed. The total of $340 billion was arrived at by taking the total amount spent, $759 billion divided by 44.7%, the percentage of browsing the Internet, which equals $339.9 billion. *See id*. Regionally, employees waste the most amount of time in the Midwest, while the least amount of time in the South. Overall, employees who reside in Missouri, Indiana, and Kentucky waste the most amount of time, as compared to residents of South Carolina, Rhode Island and Hawaii who waste the least. An average employee of Missouri, Indiana, and Kentucky wastes 3.2, 2.8, and 2.8 hours respectively, whereas residents of South Carolina, Rhode Island and Hawaii waste only 1.3 hours per working day. *Id.* Workers in California on average waste almost two and a half hours per day of work time wasting almost $38 billion, while New York employers pay their employees more than $25 billion per year for their wasted time at work. *Id.*

[69] R.L. Worsnop, *Privacy In the Workplace,* CQ RESEARCHER, Nov. 11, 19, 1993, at 1011-25.

[70] Wen, *supra* note 2, at 168.

[71] *Id.*

opposed to the previous reactive practice of addressing claims of sexual harassment only after the alleged incidents occurred.[72] One method of preventing sexual harassment fostered by a hostile work environment is to monitor the company's computer networks for potentially offensive or explicit material.[73] Electronic monitoring and surveillance can "catch" offensive or explicit materials before they can be transmitted.[74] More or less, the issue comes down to a question of duty, that is, in which situations the employer must monitor in order to protect its own interests. In *Doe v. XYC Corp*, a recent decision by the New Jersey Superior Court, the court relied on the Restatement (Second) of Torts in holding that the employer must control an employee, even while the employee is not acting within the scope of his or her employment, in order to ensure that other employees are not harmed.[75] The court went so far as to hold that "[n]o privacy interest of the employee stands in the way of this duty on the part of the employer."[76]

Thus, companies engage in surveillance for various reasons ranging from legal compliance and liability, to security concerns.[77] Whether the company engages in monitoring to protect the company itself or its protected proprietary information, companies employ various modes and methods of monitoring their employees' electronic actions taking place on the company computer network. Although the employer's justification may be clear as to why, where, when and how monitoring should take place, the sheer act of monitoring itself still continues to raise questions of fairness and privacy, and in essence forces employers to serve two masters—the interests of the company and the interests of its employees.

---

[72] *Id.* at 167-68. *See also* Doe v. XYC Corp., 887 A.2d 1156 (N.J. Sup. Ct. App. Div. 2005).

[73] Wen, *supra* note 2, at 168.

[74] *Id.*

[75] *Doe,* 887 A.2d at 1168.

[76] *Id.*

[77] AMA RESEARCH, *supra* note 44, at 1.

B. Monitoring—Serving Two Masters

Businesses monitor while serving two masters—the company itself, and its employees.[78] Monitoring protects the corporation by ensuring employee productivity and the security of proprietary information.[79] However, monitoring creates the perception of a diminished sense of employee trust because of jeopardized employee privacy.[80] When monitoring takes place, two needs must be reconciled—the need to protect company information and resources while maintaining employee morale and trust.[81]

Almost twenty years ago, the federal government recognized the growing need to study the amount of workplace surveillance, and as a result, the Office of Technology Assessment (OTA) published *The Electronic Supervisor*.[82] This book forecasted the effects of workplace supervision in the face of the increasing use of technology.[83] Even twenty years ago, the federal government acknowledged that by monitoring employees, questions will be raised relating to technology and its effects on "privacy, civil liberties, and quality of working life."[84]

Privacy in the workplace is the "right to be left alone and to not

---

[78] John J. Sheridan, *Minimizing the Risk of Security Threats to Proprietary Information*, 29 EMPLOYMENT RELATIONS TODAY 41 (2003). Sheridan argues that

> a company's true competitive advantage lies in its people. Whether they are customer service representatives . . . or CEOs, people make things happen. But in order to elicit the best work there must be a free exchange of information . . . [which] . . . can be accomplished only if there is an established trust that proprietary information will remain confidential.

Id. at 41.

[79] *Id.*

[80] *Id.*

[81] *See id.*

[82] U.S. Congress, OFFICE OF TECHNOLOGY ASSESSMENT, THE ELECTRONIC SUPERVISOR: NEW TECHNOLOGY, NEW TENSIONS (U.S. Government Printing Office 1987).

[83] *Id.* at 1.

[84] *Id.*

be intruded upon."[85] However, the OTA noted that electronic monitoring creates in employees a constant feeling of "being watched" different from the temporary reactions generated when a supervisor is monitoring in person.[86] Workers who are continually monitored report feelings of paranoia and increased negative health side effects.[87] Companies that constantly monitor their employees destroy the innate sense of trust and cooperation that keeps a company and its employees together.[88] Studies have shown that monitoring in the workplace can cause stress-related illnesses and negative psychological effects.[89] Specifically, employees who are monitored describe a decline in workplace productivity and morale caused from increased occupational health problems, tension and anxiety.[90] These problems ultimately result in increased operating costs for the company and lower workforce productivity.[91]

Even though companies are aware of surveillance's negative effects, they still continue to monitor in order to protect the company. An example of the severe effects of computer surveillance and its repercussions took place at the *New York Times* in 2001.[92] After an employee complained of receiving an

---

[85] *Id.* at 8.

[86] *Id.*

[87] Hazel Oliver, *Email and Internet Monitoring in the Workplace: Information Privacy and Contracting-Out*, 31 INDUS. L.J. 321 (2002). In 1993, the American Civil Liberties Union reported that workplace stress costs American companies almost $50 billion per year in increased health costs and lost productivity. 139 CONG. REC. S6122, S6123. (daily ed., May 19, 1993) (statement of Sen. Simon).

[88] Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employee's E-Mail?*, 20 U. HAW. L. REV. 165, 167 n.18 (1998).

[89] Oliver, *supra* note 87, at 32.

[90] Beeson, *supra* note 88, at 167 n.18.

[91] *See generally id.*

[92] James M. Rosenbaum, *In Defense of the Hard Drive*, 4 GREEN BAG 2d 169 (2001). However, most companies report that the total number of investigations that actually take place, as compared to the total number of employees with access to the Internet, computer files, or emails, is rather small. U.S. GEN. ACCT. OFF., EMPLOYEE PRIVACY: COMPUTER-USE MONITORING AND POLICIES OF SELECTED COMPANIES 8 (2002).

offensive e-mail, the *Times*, without notice to its employees, proceeded to scan every computer and its contents within the corporate office.[93] The search revealed items ranging from tasteless jokes to pornography.[94] As a result, almost 10% of *New York Times* employees of one particular department were summarily terminated while others were reprimanded and warned.[95] Nonetheless, in spite of all of these negative consequences and plausible fair reasoning behind electronic monitoring, employers still monitor under the charge, "You can—and should—monitor."[96]

The evidence is clear: monitoring is a necessary corporate tool to protect the corporation.[97] However, compelling facts show that the act of monitoring is not protecting employees, but is rather hurting them physically, psychologically, and socially.[98] Yet, surveillance can be tempered, and indeed serve the needs of both the company and the employee, through the utilization of agreements which clearly set out the guidelines and expectations of both parties.

C. Acceptable Computer/Network Use Policies

Employers have recognized the sheer amount of inherent risk involved with computers in the workplace.[99] Thus, employers have begun to institute Acceptable Use Policies (AUP), which set forth

---

[93] Rosenbaum, *supra* note 92, at 170.

[94] *Id.*

[95] *Id.* Similar occurrences happened at Dow Chemical and Xerox. In 1999, Xerox fired more than 40 employees for viewing pornographic websites for almost eight hours a day. William G. Porter & Michael C. Griffaton, *Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace*, 70 DEF. COUNS. J. 65, 76 (2003). In 2000, Dow Chemical fired 74 employees, including executives, and punished 435 others for distributing and viewing sexually explicit and violent materials via company e-mail. Rosenbaum, s*upra* note 92, at 170.

[96] NATIONAL INSTITUTE OF BUSINESS MANAGEMENT, You & the Law: Quick, Easy-to-Use Advise on Employment 2 (2002).

[97] *See supra* Part II.A.

[98] Oliver, *supra* note 87.

[99] *See supra* Part II.A.

permissible and prohibited computer, network, and Internet usage.[100] An AUP is an agreement signed by employee and employer which contains guidelines of how an employee can access and use the employer's computer system.[101] AUPs also set forth appropriate computer behavior,[102] use,[103] and governance responsibilities of both management and employees.[104] AUPs are designed to protect both the employer and employee because they prevent an employee from claiming a privacy violation by clearly stating the expectations and responsibilities.[105] Employees are explicitly aware of their expected computer use behavior, while these policies reaffirm the employer's right to monitor the employee's use of company computers by explaining acceptable computer use, and placing employees on notice of the penalties for misuse.[106] In essence, by instituting usage guidelines, supervisors inform their employees of what conduct is approved and forbidden on the corporate computer network.[107] In general, an AUP should explain what type of data will be monitored, why surveillance is necessary, and how and when the surveillance will take place.[108] Furthermore, the policy should clearly inform employees of what the repercussions will be if they break the rules.[109] Also, it should

---

[100] FPMI COMMUNICATIONS, FOR OFFICIAL USE ONLY: MANAGING CYBERSPACE IN THE WORKPLACE (2000).

[101] *Id.* at 149. The policy usually includes the requirements for user's logon information and its maintenance. *See supra* note 9, for further discussion concerning a user's logon information.

[102] SCOTT BARRMAN, WRITING INFORMATION SECURITY POLICIES 150 (2002).

[103] *Id.*

[104] *Id.* at 150-53.

[105] *Id* at 48.

[106] U.S. GEN. ACCT. OFF., *supra* note 92, at 9.

[107] BARRMAN, *supra* note 102, at 150.

[108] *Id.* at 152.

[109] Porter, *supra* note 95, at 75. Some sample provisions that might be included in an AUP under use guidelines are as follows:

> (1) Systems and network are to be used for business purposes only. Incidental personal use is permitted as long as it is not more than a trivial amount of time and does not interfere with your tasks.
>
> (2) Users may not use the systems, network, or Internet connection to

be noted that like other contracts which are unfairly slanted toward the person or corporation writing the contract, if an AUP does not contain the employer's responsibilities as a part of fair bargain, courts will invalidate it as unfair.[110]

The use of AUPs is now common and widespread and in 2002, the United States General Accounting Office (GAO) addressed the almost ubiquitous use of AUPs by filing a report with the House of Representatives Committee on Education and the Workforce's Subcommittee on 21st Century Competitiveness.[111] The report focuses on how the wide discretion private employers have in their ability to monitor what their employees are doing on the computer network impacts the workplace.[112] Private employers enjoy overly broad discretion because of the wide variance in federal and state laws, as well as differing judicial decisions.[113] The GAO surveyed fourteen Fortune 1000 private sector companies spanning five different industries.[114] The survey found that all of the companies

---

play games.

(3) Users are reminded that organizational information is proprietary and may not be shared with any outsider.

(4) Users are reminded that Internet connections are not private. While online, users must be careful as to what they disclose to others. Users should refrain from sending out any information that may be damaging to the organization or themselves.

Id. at 150-51.

[110] BARRMAN, *supra* note 102, at 151.

[111] U.S. GEN. ACCT. OFF., *supra* note 92.

[112] *Id.* at 1.

[113] *Id.*

[114] *Id.* at 2. The GAO surveyed fourteen companies from the financial services, general services, manufacturing, professional services, and wholesale/retail industries, involving interviews with representatives from the general counsel's office, human resource departments, as well as internal audit and computer security administrators. *Id.* These administrators further reported that a successful AUP depends on its successful implementation. The following list, selections from, the Ten Commandments for Avoiding Workplace E-xposure, has become the standard-bearer of what steps should be taken to secure the successful implementation of an AUP:

1) Publish policies regarding employee use of e-mail, the Internet, instant messaging and any employer issued hardware or software . . . .

had some form of AUP that informed employees that there is no expectation of privacy while using the corporate computer network.[115] Experts agree that employers should notify employees of the organization's responsibilities and disclose what will be

---

> 2) Secure employee acknowledgement of each of these policies in writing or electronically at hire or promulgation and preferably re-execute or bring to employees' attention on a regular periodic basis.
>
> 3) Inform all employees of the employer's explicit intention to monitor e-mail, Internet use and any other use of employer issued computers and electronic devices as deemed necessary for business purposes. Include the right to inspect any hardware issued to employees. Be sure to update the list of hardware items.
>
> 4) Train all employees on how to write appropriate business e-mails. Evidence suggests that you cannot assume that even high-ranking officials know how to use e-mail appropriately in a business setting . . . .
>
> . . . .
>
> 6) Create a written document retention policy that includes monthly or semi-monthly deletion of e-mails. Include a policy of recycling backup tapes. Be sure that any document retention policy complies with any . . . legislation or [court] rulings . . . .
>
> 7) Inform all employees of your intention to turn over any evidence of possible legal wrongdoing to the authorities. Also stress that you will cooperate with law enforcement officials seeking evidence of illegal activity, including evidence of terrorist related activities.
>
> 8) Be sure to enforce all policies. Do so in an even-handed manner that treats employees of all levels similarly. Note any exceptions to the policy.
>
> 9) Keep current on new technology in the market place. Assess how new software, hardware or innovations in devices issued to or owned by employees may be affecting the workplace.
>
> 10) Re-evaluate all technology-related policies annually, adjust them as necessary and inform employees of any changes and secure their affirmative consent to any important change.

Morris Jr., *supra* note 63, at 913.

[115] U.S. GEN. ACCT. OFF., *supra* note 92, at 10. The GAO continued to report that "courts have consistently upheld companies' monitoring practices where the company has a stated policy that employees have no expectation of privacy on company computer systems." *Id.*

monitored, while making clear that no expectation of privacy exists while using a company computer.[116] In the face of the amount of monitoring that takes place and the lack of statutory guidance, Congress and varied state legislatures have begun to make strides at providing business with limitations and procedures as to how and when monitoring can take place in the workplace which together with an employee's right of privacy and security of documents lead to an ultimate right of property.

III. WORKPLACE SURVEILLANCE STATUTES

In response to increasing workplace surveillance, attempts have recently been made to ensure a worker's right to privacy in the workplace.[117] However, a dichotomy exists within the current law.[118] Both federal and state law grant a modicum of privacy rights to public employees over their work and communications.[119] Unfortunately, because no federal law exists to provide employees and employers in the private sector with uniform standards concerning the ownership of electronic documents, companies must rely on piecemeal state statutes which vary from state to state, if they exist at all. As a result the private sector utilizes employment procedures, manuals, and privacy agreements to preserve an employee's privacy and the employer's work

---

[116] BARRMAN, *supra* note 102, at 150. The GAO observed that:

> Some companies directly inform employees that they should under no circumstances expect privacy. For example, once policy stated, "All users should understand that there is not right or reasonable expectation of privacy in any e-mail messages on the company's system." Somewhat less explicit, another policy stated, "Our personal privacy is not protected on these systems, and we shouldn't expect it to be." Some companies generally implied the principle of "no expectation of privacy" with statements like, "[company] reserves the right to audit, access, and inspect electronic communications and data stored or transmitted on its Computer Resources.

U.S. GEN. ACCT. OFF., *supra* note 92, at 12.

[117] *See* Wen, *supra* note 2, at 166.

[118] *See infra* Part III.A-B.

[119] *See infra* Part III.A-B.

product.[120] The current state of the law regarding employee surveillance is "an amalgam of legislation, federal and state, that resonates against a body of state common law governing individual dignitary interests—the torts of defamation, infliction of emotional distress, and invasion of privacy—the content of which can vary considerably from state to state."[121]

A. State Statutes

Reacting to the possibility that computer surveillance will allow employers to exploit their employees' privacy,[122] state legislatures have begun to address the issue that as the use of more sophisticated technology in the workplace increases, so does the risk of employer abuse.[123] Although states have previously passed legislation to protect individuals and corporations from computer crimes such as identity theft and hacking,[124] the past three years have seen a watershed movement for states to attempt to protect the electronic communications, and thereby the privacy, of private

---

[120] *See infra* Part III.B.

[121] Matthew W. Finkin, *Information Technology and Workers' Privacy: The United State Law*, 23 COMP. LAB. L. & POL'Y J. 471, 472 (2002).

[122] *See generally* Harvard Law Review Association, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991) (forecasting that although federal and state legislatures have addressed computer crime, in 1991, there was a lack of protection for employees from employer abuse of privacy rights infringement).

[123] *Id.* at 1899. States across the nation have made various attempts to pass legislation to protect employees. In 1997, the Georgia Assembly proposed the Georgia Privacy for Consumers Workers Act, which would have required employers to notify employees when and why workplace surveillance was taking place. HB 566 Ga. 1997 (proposed in 1997) (as of the date of publication, this bill was not carryovered from the 1997 session). In 2001, The California Legislature, submitted for a third time to Governor Gray Davis, a law which would have required employers to give employees notice of electronic monitoring. *See* Wen, *supra* note 2, at 170. The Massachusetts Senate in 2005, proposed the Communication and Information Privacy Act which would have also required employers to notify employees when they are being monitored. 2005 Mass. S.D. 1117 (proposed Jan 05) (as of the date of publication, this bill is still in Mass. Senate Committee).

[124] *See* Harvard Law Review Association, *supra* note 122.

citizens in the workplace.[125] Recently, states such as Florida, Connecticut, and Delaware have taken steps to protect workers' privacy by enacting various statutes.[126] Although each statute was designed to protect consumers and businesses from electronic communications fraud, or individuals from wiretapping, each state also included employee protections from secret monitoring by their employers.[127]

In 1978, Florida led the nation by becoming the first state to pass statutes that allowed corporations and businesses to seek a legal remedy for acts of computer crime.[128] In doing so, the Florida Legislature took the first steps toward protecting an employee's electronic communication at work; that protection was finally secured in 2003 when the Florida Legislature passed the Security of Communications Act.[129] Under the statute, it is a felony to "intentionally intercept or endeavor to intercept . . . any wire, oral, or electronic communications."[130] However, interception is allowed if it takes place during the normal course of employment, while engaged in any activity that is a necessary incident to the rendition of his or her service, such as in the service of police investigatory work.[131] Therefore, in Florida, if an employer electronically monitors its employees, the interception of any email or Internet usage must take place in the normal course of business and be done in order to secure the employer's property rights.[132]

---

[125] *See infra* notes 129-141 for a further discussion.

[126] *See infra* notes 129-141 for a further discussion.

[127] *See* FLA. STAT. ANN. § 934.03(1) (2003) and CONN. GEN. STAT. ANN. § 31-48d (2005).

[128] *See Florida Computer Crimes Act*, FLA. STAT. ANN. § 815.01-.07 (1976 & Supp. 1991).

[129] FLA. STAT. ANN. § 934.03(1) (2003).

[130] FLA. STAT. ANN. § 943.03(1)(a) (2003).

[131] FLA. STAT. ANN. §§ 943.03(1)(e)-(g)(2003). Although statutes exist on both the federal and state level that prevent wiretapping, this section of this statue specifically protects communications in the private workplace. *Id.*

[132] Wen, *supra* note 2, at 170. Further, it should be noted that in Florida, an employer would be able to employ the monitoring tools discussed earlier, *see supra* Part III.A, to protect against the theft of proprietary information or suit liability, for instance from sexual harassment. Otherwise, under Florida statute, an employer has no right to monitor the work of his employees without the

Following Florida's lead, in 2001, Delaware passed a statute requiring all employers, both public and private, to notify their employees of monitoring.[133] Under this provision, "no employer . . . shall monitor or otherwise intercept any telephone conversation or transmission, electronic mail or transmission, or Internet access or usage . . . unless the employer has provided some form of notice to the employee."[134] Notice is effectuated by either (1) providing an electronic notice of monitoring to an employee at least once a day when the employee accesses electronic resources, or (2) giving the employee a one-time written notice concerning the scope and types of monitoring.[135] The written notice must be maintained and securely kept by the company and both the employee and supervisor must consent.[136]

In 2003, Connecticut passed the Communications Technology in the Workplace Act.[137] Connecticut's statute only permits the gathering of information detailing an employee's activities through direct observation.[138] Employers are defined as any business that operates within the state—both public and private.[139] However, if an employer provides written notice to an employee of all forms of monitoring, both through direct and electronic surveillance that is taking place, and posts notice in a conspicuous place, monitoring is allowed.[140]

B. Federal Statutes

The federal government has done little lately to protect the rights of individuals from secret electronic monitoring. The

written consent of all parties engaged in the monitoring—both employee and supervisors. Wen, *supra* note 2, at 170.

[133] 19 DEL. C. § 705 (2005).

[134] 19 DEL. C. § 705(b) (2005).

[135] *Id.*

[136] 19 DEL. C. § 705(b)(1)(2) (2005).

[137] CONN. GEN. STAT. ANN. § 31-48d (2005).

[138] CONN. GEN. STAT. ANN. § 31-48d(a)(3) (2005).

[139] CONN. GEN. STAT. ANN. § 31-48d(a)(1) (2005).

[140] CONN. GEN. STAT. ANN. § 31-48d(b)(1) (2005).

Electronic Communications Privacy Act of 1986[141] (ECPA) stands as the controlling legislation that "prohibits the interception, disclosure, or use of wire, oral or electronic communication."[142] Congress twice attempted to pass more comprehensive and protective pieces of legislation: in 1990 the Privacy for Consumers and Workers Act[143] (PCWA) and in 2000 the Notice of Electronic Monitoring Act[144] (NEMA). However, both of these Congressional attempts have failed,[145] and to date, only the twenty-year-old ECPA provides protections to employees who are being monitored.[146]

1. The Electronic Communications Privacy Act[147]

Fifteen years ago, the Harvard Law Review Association argued that laws designed to protect individuals and companies from computer crimes were not enough to protect employees from abuse by their employers[148]—specifically referring to the Electronic Communications Act of 1986.[149] Harvard raised the following "age-old workplace" conflict in light of the ECPA—"how much access employers should have to their employees' workspace, and how much freedom employees should have to use workplace

---

[141] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508 (1986), 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.) [hereinafter ECPA].

[142] NATIONAL WORKRIGHTS INSTITUTE, Privacy Under Siege: Electronic Monitoring in the Workplace 14 (2005), *available at* http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

[143] Privacy for Consumers and Workers Act of 1990, H.R. 2168 (1st Sess. 1990).

[144] Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2nd Sess. 2000).

[145] *See infra* Part III.B.1-3.

[146] *See infra* Part III.B.1.

[147] ECPA, Pub. L. No. 99-508 (1986).

[148] *See* Harvard Law Review Association, *supra* note 122, at 1899.

[149] ECPA, Pub. L. No. 99-508 (1986), 100 Stat. 1848. The Act was originally passed into law as an amendment to the Omnibus Crime Control and Safe Streets Act of 1986. NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 14

resources for their own purposes."[150] The ECPA prohibits the "interception and disclosure of wire, oral or electronic communication, with certain exceptions."[151] The protections afforded by the ECPA apply to all businesses involved in interstate commerce.[152]

The Act as originally passed in 1986 deals only with the electronics, technology and circumstances contemporary to its time. The main focus and purpose of this law is to protect businesses and corporations from computer crime and individuals from wiretapping.[153] This focus is biased in favor of the employer, and the only remedy given to employees is the common law tort of invasion of privacy.[154] However, proving the tort of invasion of privacy is a difficult task to undertake because an employee has to first show that the company's interception of his or her communication could not be excused as a legitimate business practice.[155] Then the employee has to prove that his or her communication was never intended to be distributed to the public, let alone to his or her employer.[156] Furthermore, the employee must demonstrate that a reasonable expectation of privacy in the communication existed.[157]

2. Privacy for Consumers and Workers Act[158]

In 1990, Senator Paul Simon and Representative Pat Williams introduced the PWCA, respectively, in the United States Senate and House of Representatives.[159] From 1990 to 1993, Sen. Simon,

---

[150] Harvard Law Review Association, *supra* note 122, at 1911.

[151] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 14.

[152] *Id.* at 14.

[153] *See* ECPA, Pub. L. No. 99-508 (1986), 100 Stat. 1848.

[154] Harvard Law Review Association, *supra* note 122, at 1911.

[155] *Id.*

[156] *Id.*

[157] *Id.* However, public sector employees are virtually barred from claiming Fourth Amendment violations because it is nearly impossible to prove the elements of privacy and reasonableness. *Id.*

[158] H.R. 2168 (1st Sess. 1990).

[159] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 19.

Rep. Williams, and over 150 bipartisan cosponsors continued to reintroduce the bill after each failed attempt to bring the bill out of committee and onto the floor for a full vote in each respective chamber.[160] The PCWA would have provided employees with a "right to know" when and where monitoring would take place and mandated advanced notice of what would be collected and how it would be used.[161] Sen. Simon characterized the unrestrained surveillance of workers as turning the "modern office into [an] electronic sweatshop."[162]

The PCWA would have required employers to allow their workers to have unfettered access to the data that was collected through workplace surveillance.[163] Under this law, employers would have to set out their policies and inform prospective employees of their monitoring practices.[164] Furthermore, the PCWA would have prohibited companies from storing, gathering, utilizing, or distributing data obtained by electronic surveillance.[165] It would also require that employers inform their employees when monitoring is actually taking place through a signal light, beeping tone, verbal notification, or other forms of notification.[166] A crucial issue in the PCWA was that an employee would never be able to waive his or her First Amendment rights.[167] If an employer were to enter into a private agreement concerning approved computer network usage, that agreement could never take away his or her protected constitutional right of freedom of expression.[168]

When the proposed legislation was first debated in committee, Senator Simon characterized employee monitoring as an

---

[160] *Id.*

[161] 139 CONG. REC. S2430 (daily ed., Feb. 6, 1991) (statement of Sen. Simon).

[162] *Id.*

[163] H.R. 2168 (1st Sess. 1990).

[164] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 19.

[165] H.R. 2168 (1st Sess. 1990).

[166] 137 CONG. REC. E709 (daily ed., March 1, 1991) (statement of Rep. Williams).

[167] *Id.*

[168] *See id.* (stating that the act "prohibits the waiver of rights and procedures provided by this act.").

"electronic whip that drives the fast pace of today's workplace."[169] He stated, that "it is an unfortunate irony that the Federal Bureau of Investigation is required to obtain a court order to wiretap a telephone, even in cases of national security, but that employers are permitted to spy at will on their own personnel and the public."[170] He also noted at the time, that the United States and South Africa were the only countries that failed to have some of protections that safeguarded an employee's privacy in the workplace.[171] At the time, the PCWA's opponents were successfully able to argue the PCWA's impracticality and ineffectiveness in face of tort law and other remedies.[172] During the PCWA's final debate, Sen. Simon prophesized that:

> Just over the horizon are more technology breakthroughs and refinements that we can't even envision today. Unless we begin now to define privacy—and in particular workplace privacy—as a value worth protecting, these new technologies will be upon us before we are ready for them. Weighing these issues will allow us to be the masters of technology, instead of its slaves.[173]

---

[169] 139 CONG. REC. S6122 (daily ed., May 19, 1993) (statement of Sen. Simon).

[170] 137 CONG. REC. S2430 (daily ed., Feb. 6, 1991) (statement of Sen. Simon).

[171] *Id.* Also the International Labour Organization (ILO), adopted The ILO Code: The Standard for Workers' Rights, a basic set of employee protections which include:

> Coverage for both public and private sector employees; That employees should have notice of data collection processes; That data should be collected and used lawfully and fairly . . . That data should be used for reasons directly relevant to employment . . . That data should be held securely; That workers should have access to data . . . That workers cannot waive their privacy rights . . . .

ELECTRONIC PRIVACY INFORMATION CENTER, Workplace Privacy, *available at* http://www.epic.org/privacy/workplace.

[172] Kristen B. DeTienne, *The Boss's Eyes and Ears: A Case Study of Electronic Employee Monitoring and the Privacy for Consumers and Workers Act*, 12 LAB. LAW. 93, 98 (1996).

[173] 139 CONG. REC. S6122, S6123 (daily ed., May 19, 1993) (statement of Sen. Simon).

At the end of the 1993 Congressional term, the PCWA died in committee in both houses and has yet to be introduced.[174]

3. Notice of Electronic Monitoring Act[175]

Ten years after the failed attempt to pass the PWCA, Senator Charles Schumer and Representative Charles Candy introduced the NEMA in 2000.[176] This bill also failed to receive a vote on the floors of both houses of Congress.[177] Under NEMA, any "employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication, or electronic communication of an employee, without first having provided the employee notice . . . shall be liable to the employee for relief."[178] The notice requirement would be satisfied so long as the employer told the employees which communications or computer uses would be monitored, how the monitoring would take place, and how the information obtained would be maintained.[179] Furthermore, employers would be required to disclose the monitoring and collection of "non-work related information."[180] This provision would have also allowed employees to seek damages in federal courts for violations.[181] Specifically, employers would be liable for attorney's fees, punitive and actual damages, and other costs, with the total not exceeding $500,000, should the employee be successful in a lawsuit against the employer for a NEMA violation.[182]

Both federal and state governments have begun to make strides in limiting how, when, and why monitoring takes places. The actual notice of when and where monitoring takes place as afforded by some states, is a first step in affording workers

---

[174] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 19.

[175] H.R. 4908, 106th Cong. (2nd Sess. 2000).

[176] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 19.

[177] *See* H.R. 4908, 106th Cong. (2nd Sess. 2000).

[178] *Id*. at 277(a)(1).

[179] *See id.*

[180] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 19.

[181] *Id.*

[182] *Id.*

adequate protections at work, yet still does nothing to help determine property rights over personal electronic documents created or maintained on a corporate computer network. However, until a unified national policy is in place, states will attempt to fill in the gap, and in the absence of no legislation, companies alone are left to set their own individual surveillance policies. Just as guidance exists for the federal government and its employees, some form of unifying policy must come into existence.

IV. AN EXAMPLE WITHIN THE PUBLIC SPHERE: *HAYNES V. OFFICE OF THE ATTORNEY GENERAL*[183]

Government employees maintain a privacy right over their personal belongings at the workplace.[184] When analyzing government employees' privacy rights, courts engage in a Fourth Amendment analysis.[185] However, this Fourth Amendment analysis only applies to public sector employees.[186] Private sector employees can not claim Fourth Amendment violations when their private employers seize their electronic documents.[187]

O'Connor v. Ortega[188] provides the groundwork for analyzing a government employee's inherent privacy and property rights over his or her computer and contents when juxtaposed against classical Fourth Amendment analyses. Under *O'Connor*, employees in the government sector may gain a full expectation of privacy over their work, if similar expectations of privacy existed when the document was first created.[189] The expectation of privacy is even further bolstered if the document is stored under conditions where access is granted only to selected users.[190]

The *O'Connor* framework begins with the Fourth Amendment, which guarantees "the right of the people to be secure in the

---

[183] 2005 WL 2704956 (D. Kan. Aug. 26, 2005).

[184] *Id.*

[185] *See* O'Connor v. Ortega, 480 U.S. 709 (1987).

[186] *See e.g. id.*

[187] *See e.g. id.*

[188] *Id.*

[189] *Id.*

[190] *Id.*

persons, houses, papers, and effects, against unreasonable searches and seizures."[191] A Fourth Amendment violation is established when a "legitimate expectation of privacy"[192] exists. To determine if a legitimate expectation of privacy exists, a two-part inquiry must take place, which requires: (1) a showing of a subjective expectation of privacy in the area searched, and (2) an expectation of privacy that society is prepared to recognize as reasonable.[193] The Supreme Court has acknowledged that governmental employees may have a reasonable expectation of privacy, but this expectation may be reduced by what takes place in the office place.[194] However, resolving whether or not an expectation of privacy exists remains a fact specific problem which must be viewed in a reasonable light concerning all of the surrounding circumstances of a specific case.[195]

An important aspect in determining whether or not an expectation of privacy exists involves the use and maintenance of computer passwords,[196] as well as the general security of an employee's workspace.[197] *U.S. v. Slanina* held that when public agencies mandate that their employees use passwords to secure their computers and keys to secure their offices, those actions may be evidence of a subjective expectation of privacy.[198] Further, when employers fail to notify employees that their computer use can be monitored, in conjunction with the absence of evidence that

---

[191] U.S. CONST. amend. IV.

[192] Rakas v. Illinois, 439 U.S. 128, 143 (1978).

[193] U.S. v. Anderson, 154 F.3d 1225, 1229 (10th Cir. 1998) (internal citations and quotations omitted). Further, as with the expectation of privacy in one's home, such an expectation in one's place of work is "based upon societal expectations that have deep roots in the history of the [Fourth] Amendment." Oliver v. United States, 466 U.S. 170, 178 n. 8 (1984).

[194] *O'Connor*, 480 U.S. at 716-17. The expectation of privacy may be limited by such things as office practices and procedures, or by legitimate regulation. *Id.*

[195] Haynes v. Office of the Attorney General Phill Kline, 298 F. Supp. 2d 1154, 1161 (D. Kan. 2003).

[196] See *supra* note 15, for a further discussion concerning passwords.

[197] U.S. v. Slanina, 283 F.3d 670, 676 (5th Cir. 2002).

[198] *Id.*

other employees can access each other's computers,[199] the employees' subjective expectation of privacy can rise to an objective level of privacy or one that society is prepared to recognize.[200]

In *Haynes v. Office of the Attorney General*, Carlus Haynes, a former Kansas Assistant Attorney General, sought injunctive relief to prevent his former employer, the Kansas Attorney General, from accessing his private files on his work computer as well as damages.[201] Prior to Haynes' termination he was denied access to both personal and work related files which were stored on his computer.[202] The *Haynes* court relied on the *O'Connor* framework to determine if an expectation of privacy existed.[203] Haynes alleged a legitimate expectation of privacy in the information stored on his work computer, and that the search following his termination violated his Fourth Amendment rights.[204] Further, Haynes claimed a property interest in the personal information stored on his work computer and that the state's actions in preventing him from accessing his personal information deprived "him of property

---

[199] With any computer network, system administrators may have access to even password-protected data; however, when this administrator access is not routine it only further bolsters an employee's expectation of privacy. *See generally id.* at 676-77.

[200] *Id.*

[201] Haynes v. Attorney General of Kansas, 2005 WL 2704956 1. (D. Kan. Aug. 26, 2005).

[202] *Id.* The facts surrounding Haynes' termination and subsequent denial of access are as follows: Haynes was informed that he was going to be fired in two weeks. On the same day, Haynes' supervisor contacted a computer specialist to restrict Haynes' computer access to certain times and to ensure that no data was copied. When Haynes accessed his computer and began to copy his personal files and work product he was approached by his supervisor and accused of stealing. Haynes explained that he was copying his personal files. About an hour later, Haynes was summarily terminated, given fifteen minutes to leave and was not allowed to take anything with him, including personal items. After his termination, certain files on his computer, including personal e-mail messages, were viewed by other employees of the Kansas Attorney General. However, after several months had passed, Haynes was given access to all of his e-mail and documents that remained on his computer. *Id.*

[203] *Id.* at 3.

[204] *Id.* at 1.

without just compensation in violation of the Fourteenth Amendment."[205]

The court focused mainly on whether or not Haynes' expectation of privacy was indeed reasonable. When Haynes' employment began, he signed the Kansas Attorney General's Office's Computer Use Procedures,[206] which set forth the system's privacy expectations.[207] Each time Haynes logged onto his computer he was presented with an explicit warning[208] informing

---

[205] *Id.* The *Haynes* court relied on United States v. Angevine, 281 F.3d 1130 (10th Cir.) *cert. denied*, 537 U.S. 845 (2002), to reach its decision. In *Angevine,* the defendant, an "Oklahoma State University professor, had been prosecuted for possession of child pornography . . . [and] sought to suppress the pornography that had been seized." *Haynes,* 2005 WL 2704956 at 2. In this instance the defendant did not have an objectively reasonable expectation of privacy because of the following: "(1) the university's policy that allowed the university to audit and monitor Internet use and warned that information flowing through the university network was not confidential; (2) the university owned the computer and explicitly reserved ownership of data stored within." *Id.*

[206] Haynes v. Attorney General of Kansas, 2005 WL 2704956, 2 (D. Kan. Aug. 26, 2005). The full policy read as follows:

> Office computer use shall be in compliance with computer use procedures. Obtain full procedures from your deputy or supervisor. Computer use for non-official business is authorized only if kept to minimum duration & frequency & if it does not interfere with state business. This system shall not be used unlawfully nor for any purpose which could embarrass the user, recipient or Attorney General. There shall be no expectation of privacy in using this system; however, intentional access to another user's e-mail without permission shall be prohibited, except as authorized by computer use procedures. Despite deletion, files may remain available in storage. Personal data on the system may be subject to removal. Data may be subject to state public records and records preservation laws. User software installation is prohibited unless specifically authorized. Software may not be copied for use outside this office unless authorized.

Id.

[207] Haynes v. Attorney General of Kansas, 2005 WL 2704956, 2 (D. Kan. Aug. 26, 2005).

[208] *Id.* at 4. Warning messages reminding employees of the pre-existing AUP, have played a significant role in court decisions. *See* United States v. Simons*,* 206 F. 3d 392 (4th Cir. 2000) (holding that a CIA division's Internet usage policy eliminated a reasonable expectation of privacy concerning file

him and all employees that computer use was not confidential, that there was no expectation of privacy, and that personal files stored on the network could be removed at any time, without notice.[209] Despite Haynes' password and private workspace, the warning conveyed to Haynes each time he used his computer was the overwhelming factor in the court's decision to deny the injunction.[210] Ultimately, the court found that Haynes did not sufficiently demonstrate an objectively reasonable expectation of privacy.[211] However, the court did note that the law concerning the expectation of privacy is in a state of "flux with the outcome heavily dependent upon the particular facts of each case."[212]

Even government employees, as exemplified by the *Haynes* decision, have a difficult task of asserting privacy and property rights over their electronic documents. Fourth Amendment protections and its afforded heightened level of security, seems to do little when companies utilize AUPs and notification procedures. Nonetheless, even against a uniform standard of determining how, when, and where a right of privacy exists finding a property right is an intricate determination to make—for both public and private employees.

V. THE *SHMUELI* DECISION AND THE FUTURE

The division between business and personal documents must

---

transfers, all websites history, and all e-mail); Muick v. Glenayre Electronics, 280 F. 3d 741 (7th Cir. 2002) (ruling that an employee has no reasonable expectation of privacy in laptop files where employer announced it could inspect laptops it provides to employees); United States v. Bailey, 272 F. Supp. 2d 822 (D. Neb. 2003) (finding that an employee has no reasonable basis to believe activities on work computer were private "when, through company's screen notification, they have actual knowledge that the computer can be searched"); United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000) (holding that a sergeant has no reasonable expectation of privacy over his government e-mail account because use was reserved for official business and network banner informed users upon login that use was subject to monitoring).

[209] *Haynes*, 2005 WL 2704956 at 4.

[210] *Id.* at 2.

[211] *Id.* at 4.

[212] *Id.*

have a clear distinction or both employers and employees will suffer significant costs after the employment relationship is severed. It is well established that employers electronically monitor their employees' communication. Protections afforded by statutes, and notifications provided by AUPs which detail an employee's minimal expectation of privacy, are nominal steps toward identifying who maintains property rights over personal electronic documents created or maintained on a work computer. Current protections afforded by statutes and AUPs are designed to ensure the security of proprietary information and employee productivity,[213] as well as the security of electronic communications.[214] AUPs and current statutes, however, never assign property right protections. Just as an electronic communication can be stolen through wiretapping, an electronic document can be illegally taken through various surveillance and monitoring techniques.[215]

Although electronic documents are not communications, they are capable of being viewed, copied, and maliciously stolen though electronic monitoring. As one journalist observed,

> [t]he commingling of personal and business property on company computers [continues to grow] . . . [f]rom personal e-mail to screenplays written on the lunch hour, employers should anticipate the obligation to identify . . . and return personal data 'belonging' to fired employees. Likewise, employees need to tailor . . . personal use of company systems to the possibility of lock out.[216]

All employees have notions that after they are fired they will be given a cardboard box to collect their personal belongings before their final exit. As the issue of electronic property further develops, or as employers seek to avoid litigation, society must decide if it wants to grant former employees "computer visitation rights,"

---

[213] *See supra* Part II.

[214] *See supra* Part III.

[215] See *supra* Part II.A, which describes the surveillance monitoring techniques that take place that give employers the opportunity to take an employee's electronic document.

[216] Craig Ball, *Yours, Mine and Ouch!*, LAW TECHNOLOGY NEWS, Sep. 2005, *available at* http://www.craigball.com/BIYC04-092005.pdf

which would allow employees a window of opportunity to access their computers after they have been terminated.[217] When choosing to grant visitation rights, certain limitations must be considered. For example, if former employees are allowed to "visit" their old computers, the company may run the risk of loosing proprietary information because the former employee now works for a competing firm.[218] Conversely, in a scenario where the former employer will actually give former employees their personal electronic documents, employees must ask if they want their old employer going through their former computer, sifting personal from work product.[219]

Legislation and case law currently guide employees and employers as to the particulars of copyright, trademark or patent infringement, or the theft of trade secrets.[220] Further, restrictive covenants and acceptable use policies entered into between employers and employees can affect the property relationship.[221] Nonetheless, if an employee were to use the company's computer for personal matters, such as writing a novel, during a non-paid lunch hour, no guidance beyond the likely employer-slanted AUP exists to protect the employee's property rights over his or her personal material.[222] Under *Shmueli*, if an employer was to unlawfully take an independent contractor's personal *printed* document, conversion applies.[223] This same remedy does not apply to *electronic* documents because no statutory protections are provided for the benefit of the privately employed worker.[224] To

---

[217] *Id.*

[218] *Id.*

[219] *Id.*

[220] Trade secret protection is extended to "any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." Ashland Mgt. Inc. v. Janien, 82 N.Y.S.2d 912, 918 (Sup. Ct. 1993) (quoting Restatement (Second) of Torts § 757, comment b (1993)). Patent, trademark, and copyright protection will not be discussed in this Note.

[221] *See supra* Part II.C.

[222] *See supra* Part II.C.

[223] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 876 (Sup. Ct. 2005).

[224] *See supra* Part III.

avoid the possible usurpation of employee property rights, some legal experts contend that laws should be passed which limit the conditions and circumstances of monitoring and thereby protect private sector employees' property interest over their electronic documents.[225]

In order to avoid lawsuits by former employees over the property interests in the employees' personal electronic documents, it would benefit employers to follow a set policy that allows both employers and employees to maintain control over the documents that rightfully belong to each respective party. Although a policy may exist which assigns property rights, this policy still does not resolve the problem presented by *Shmueli*, which provides no direction for employees who have had their personal electronic documents taken by their employers.

Similar to the problems Sarit Shmueli faced when her private files were taken by her employer, employees who are denied access to documents stored on their computers have few remedies. Furthermore, because an employer can monitor, see, and even copy what an employee does on his or her company computer,[226] an employee has essentially no avenues of redress when personal files stored on the company computer have been copied, taken, monitored or logged without the employee's knowledge or consent.

VI. DOES THE ANSWER REST IN PRIVACY? STATUTORY PROTECTION? OR BOTH?

A middle line must be drawn which protects business interests as well as personal privacy and property rights. As more and more people rely on computers to perform their work tasks, society faces a conundrum—whether or not to extend privacy rights into the realm of the work computer. Congressional legislative history[227] as well as strides made at the state level,[228] have recognized a desire

---

[225] U.S. GEN. ACCT. OFF., *supra* note 92, at 1.

[226] *See* supra Part II.A.

[227] *See supra* Part III.B.

[228] *See supra* Part III.A.

to extend a level of privacy onto an employee's work computer. This privacy interest must be defined in a consistent national policy that will guide both employers and employees. Reasoning-by-interpolation, or penumbral reasoning, provides one possible answer to the problem. In balancing a reasonable expectation of privacy in the workplace[229] against the need for monitoring,[230] any real solution must confront the following paradox:

> If an employee knows that his employer engages in electronic eavesdropping, he has no subjective expectation of privacy because he knows that his employer can intercept every word he utters. Thus, by notifying employees that eavesdropping is taking place, employers can effectively negate employees' claims to privacy in the workplace under the traditional justifiable-expectation-of-privacy analysis.[231]

Currently, when the two needs are pitted against one another, an employee's expectation of privacy is destroyed in favor of the company's need to monitor. A solution must be found which preserves both interests.

Penumbral reasoning is the "drawing of logical inferences by looking at relevant parts of the Constitution as a whole and their relationship to one another."[232] Although the analogy is not direct, it does provide a basis for interpolation. When an employee's security right over his or her communications and his or her to right privacy in the workplace are placed against one another, as this Note proposes, in the overlap a property right over electronic

---

[229] *See supra* Part IV.

[230] *See supra* Part II.A.

[231] Jonathan J. Green, *Electronic Monitoring In the Workplace: The Need For Standards*, 52 GEO. WASH. L. REV. 438, 445 (1984).

[232] Denning, *supra* note 8, at 1092.

> In most judges' and scholars' minds, the premier contemporary example of penumbral reasoning is *Griswold*. In *Griswold*, Justice Douglas looked at various provisions of the Bill of Rights, include those that protect assembly, freedom from self-incrimination . . . From this survey, he inferred that there was a common thread throughout that government could not intrude into the privacy of individuals absent fairly compelling circumstances.

Id.

documents is generated.

Current statutory protections, both at the state and federal levels, grant public and private employees security over their electronic communications.[233] Case law provides the proposition that an expectation of privacy exists at work.[234] Furthermore, corporate practices support and recognize this notion as well through their use of blanket statements[235] utilized in AUPs. If an employee had no right of privacy at work, these statements would not be necessary, they only serve to negate an employee's affirmative right to privacy in the workplace which effectively removes the traditional privacy expectation.

Returning to the novel written during an employee's lunch hour using work resources, or even Sarit Shmueli's client-list, in the spaces where privacy and the security of electronic communications overlap, a property right appears to exist. This property right is founded in the preexisting affirmative right of privacy and the secured protection over their electronic communications. Therefore, as this Note suggests when an employee is able to create a personal electronic document at work, he or she maintains a property right over that document.

VII. SUGGESTED POLICY

Solutions to this problem can be found on two fronts—through legislation and the continued use of AUPs. Currently, the ECPA[236] is the only national guideline that employers can follow. Unfortunately, this statute is flawed and insufficient to protect an employee's work at the modern company. Additionally, most current AUP contracts fail to address any property rights

---

[233] *See supra* Part III. In order for an employer to violate an employee's protection, an employer must notify the employee. Therefore, the right remains with the employee, and can only be legally violated with the employee's consent.

[234] *See supra* Part IV.

[235] See *supra* notes 116, 196 and 201 for a further discussion concerning explicit warnings given to users concerning expectations of privacy in the workplace.

[236] *See supra* Part III.B.3.

employees may have over their personal electronic documents.[237] Effective AUPs must be drafted which will appropriately guide employers in how and when they monitor their employees in light of current technology, and the inherent property right employees maintain in their personal electronic documents.[238]

A. Statutory Solution

With the continued evolution of technology, any protections afforded by the ECPA have become practically irrelevant.[239] First, the ECPA does not apply to forms of surveillance technologies such as electronic mail monitoring, Internet monitoring, and video surveillance.[240] Also, because the ECPA requires an active interception of a communication, viewing communications and documents that are stored on a computer or file server is not a violation.[241] Additionally, aside from piecemeal state regulation, the ECPA as a national standard benchmark "does not require an employer to give notice of electronic monitoring practices, nor is there any other [federal] statute that requires an employer to give notice of monitoring practices, no matter how invasive the monitoring may be."[242]

If a secured privacy and property right is guaranteed at work, then an employee would maintain an inherent right over expressions created at work, utilizing work resources. The protections afforded by Florida, Connecticut and Delaware provide

---

[237] *See supra* Part II.C.

[238] The main thrust of this policy is not to decide when and how to monitor employees, but on how to secure an employee's property in his or her electronic documents.

[239] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 15.

[240] *Id.* See *supra* Part II.A for a further discussion of surveillance technologies used. Under the ECPA an employer is permitted to utilize these methods.

[241] *See* ECPA, Pub. L. No. 99-508 (1986), 100 Stat. 1848 (codified as amended in scattered sections of 18. U.S.C.). The ECPA only applies when active interception takes place. Documents stored in a passive state, like Shmueli's contact list, are not protected from copying or taking under this statute. *See* NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142.

[242] NATIONAL WORKRIGHTS INSTITUTE, *supra* note 142, at 15.

a solid basis for how, where, and why surveillance should take place; however, these laws insufficiently protect an employee's property right over his or her electronic documents. Under these statutory frameworks, when an employee assents to the monitoring and in the course of the surveillance, an employee's document is copied—the employee will never be able to assert property interest over the documents because the notice negated any and all property rights. Any statutory solution must include provisions that protect an employee's property interest. A statutory solution must secure employees' property rights over their documents so rigidly that it can never be signed away through an AUP or negated through notification standards. Thus, if an employee were to write the next great American novel on a computer at work, it would never be owned by his or her employer.

The proposed PCWA of 1990 appears to be the best springboard to form a sound national policy. Under the PCWA, employers would have to inform all employees, even prospective ones, of all the monitoring that takes place in the workplace. Furthermore, the PCWA would guarantee an employee's rights over their First Amendment expressions, for instance the Great American novel written during a non-paid lunch hour. However, the PCWA does nothing to protect documents that are taken without an employee's knowledge.[243] In order "to protect employees' privacy rights, uniform standards must be set to govern monitoring of employees' communications . . . [in light of] current technological capabilities."[244] Therefore, the uniform statutory standard must include notice, audit, and remedies.

Notice will involve a two-part standard. The Delaware Notice of Monitoring Act is a good starting point for analysis.[245] First,

---

[243] Justice Cahn states that an owner does not forfeit his ownership for failure to take good care of intangible personal property any more than he forfeits it for failure to take good care of his watch. Shmueli v. Corcoran Group, 802 N.Y.S.2d 871, 874 (Sup. Ct. 2005). Therefore, an employee should be afforded the same protections when his belongings are taken without his knowledge. In essence, how can a man call the police to report a stolen watch, when he didn't know it was gone in the first place?

[244] Green, *supra* note 231, at 457.

[245] 19 DEL. C. § 705 (2005). See *supra* Part III.A for a further discussion.

employees must be informed of how, when, and why monitoring will take place. It must be recognized that employees are at work to work for their employer, not to toil on their own personal ventures, such as web-surfing, e-mailing, or even writing the next great American novel. If an employee is able to create personal work incidental to required tasks, the employer must concede that the personal work is the property of the employee. Second, if continuous active monitoring takes place as described, pop-up notification, similar to the one at issue in *Haynes*,[246] must be displayed every time users login into their computers informing them that active monitoring is taking place.

The data and information collected as a result of monitoring must be subject to audit and review. This facet has not been addressed by any other previous legislative attempts. Employers must be allowed to access the data collected upon the showing of an appropriate and reasonable request. Furthermore, just as employers are required to report tax and benefit summaries to employees, they must also include summaries of what information or personal documents have been collected.

If employees should discover that their electronic documents have been taken without their knowledge, appropriate remedies must be available. First, the inherent property right that employees have over their documents must be recognized. Without an acknowledgement of the inherent property right that employees maintain in documents, employees would not have the benefit of suing for conversion. In addition, employees must be able to seek appropriate compensatory damages as suggested by the proposed Notice of Electronic Monitoring Act of 2000.[247] Under NEMA, employees could sue for actual and punitive damages, and other fees, up to $500,000.[248]

---

[246] Haynes v. Attorney General of Kansas, 2005 WL 2704956 (D. Kan. Aug. 26, 2005). See *supra* note 205-208 for a further discussion of other types of pop-up notifications.

[247] H.R. 4908, 106th Cong. (2nd Sess. 2000). See *supra* Part III.B.3 for a further discussion.

[248] *Id.*

B. Private Solution

Despite the lack of statutory guidance concerning electronic documents in the workplace, business must continue to function. In light of the *Shmueli*[249] decision, and in the absence of a national statutory framework that recognizes an employee's property right, employers must continue to provide employees with AUPs. Current industry standards detailing how employees assent to an AUP must continue to be followed.[250] Under current federal law, employers are not required to provide their employees with an AUP[251]—those that do, do so to satisfy state requirements[252] or out of their own initiative.[253]

Until a national policy is in place, companies should continue to provide their employees with AUPs, understanding that employees maintain an inherent property right over their personal electronic documents. Any unified policy should and will recognize an organization's need to monitor to protect company assets and ensure employee productivity. However, current AUPs do nothing to help determine ownership over an electronic document.[254] Rather, current AUPs only make blanket statements stating that company assets such as computers should be used solely for business purposes.[255] Nevertheless, studies have proven that employees are using their work computers for personal purposes.[256] Therefore, if employees maintain an inherent property right over their personal electronic documents and employees are indeed creating these documents at work, AUPs must address this issue.

Under current law, as in *Shmueli*'s holding alone, employees are able to sue for conversion.[257] At the very least, AUPs must

---

[249] Shmueli v. Corcoran Group, 802 N.Y.S.2d 871 (Sup. Ct. 2005).

[250] *See supra* Part II.C.

[251] *See supra* Part III.B.

[252] *See supra* Part III.A.

[253] *See* U.S. GEN. ACCT. OFF., *supra* note 92.

[254] *See supra* Part III.C.

[255] *See* Porter, *supra* note 95.

[256] *See supra* Part II.A.

[257] *See* Shmueli v. Corcoran Group, 802 N.Y.S.2d 871 (Sup. Ct. 2005).

address this problem or companies risk litigation exposure. Ultimately, an AUP should include the same suggestions as discussed previously under a suggested statutory solution, such as notice and audit. Crucially, AUPs should protect the company, while providing adequate notice to the employee of when and why electronic monitoring is taking place, while recognizing an employee's property right over their electronic documents.

Employees should not be given a blanket right to do what they wish while at work—employees should still be subject to disciplinary actions if they are found to violate fundamental precepts of their work agreement or the AUP.[258] Employers, however, must recognize that if an employee is able to write the great American novel utilizing work resources, while still satisfying work requirements, in order to protect the company from suit exposure and other increased expenses, an AUP must recognize the employee's property right over those documents.

CONCLUSION

As computer use in the workplace continues to grow, checks must be put into place which balance a company's need to monitor their employees and control their trade secret and other proprietary information against an employee's inherent property right over their personal electronic documents. Current federal and state statutes insufficiently secure this right. Although privately drafted AUPs protect the corporation, they do little to protect employees. *Shmueli* illustrates the first official step toward recognizing an employee's property right over their documents that is grounded in the overlap between privacy and the security of electronic communications. A national policy must recognize this right, but until then, employers must protect themselves by creating adequate AUPs to guard the interests of all parties. Employees must satisfy their work requirements—that is what they are paid to do—not write the great American novel. However, if an employee is able to do both, policy, either statutory or privately driven, must reflect the employee's property interest.

---

[258] *See* Porter, *supra* note 95.