Journal of Technology Law & Policy

Volume 4 | Issue 1 Article 2

January 1999

With Nowhere to Hide: Workers Are Scrambling for Privacy in the Digital Age

Rod Dixon

Journal of Technology Law & Policy
Volume 4 Spring 1999 Issue 1
Published by Students at the University of Florida College of Law

Return to Table of Contents | Comment on this Article

With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age

by Rod Dixon [*]

Cite as: Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4J. TECH. L. & POL'Y 1 <http://journal.law.ufl.edu/~techlaw/4/Dixon.html> (1998-1999).

TABLE OF CONTENTS

SUMMARY

{1} Recent innovations in digital technology [1] have resulted in the proliferation of workplace surveillance devices, which allow bugging, telephone monitoring, visual surveillance during night or day, communications interceptions on computer networks and the creation of digitally controlled human recognition and tracking devices. Not surprisingly, the expanding presence of digital technology in the American workplace has guaranteed that complex issues of personal and workplace privacy have

become far more pervasive than ever before.

{2} The modern workplace uses digital technology -- in the form of desktop computers, powerful database servers, facsimile transmissions, electronic mail, electronic networks, and interconnected information systems -- to routinely process, store, and transmit data for most important transactions. [2] As a result, employers have significant concerns regarding the best methods to protect their computer networks and the valuable information or data stored and transmitted on those computer networks from theft or damage. In this respect, employers are showing greater concern today for managing the conduct of employees when workers are accessing or using the employer's interconnected computer systems; namely, employers are managing employee conduct by monitoring workers' activities through the use of advanced technologies. [3] As the spread and use of digital technologies in the workplace have encompassed the surveillance [4] and monitoring activities [5] of employees, the failure of current privacy law doctrine [6] to protect the interests of workers has become more apparent. [7]

{3} The law of privacy, like other legal doctrines, developed in response to society's needs. In the past, the law of workplace privacy generally evolved in the context of societal notions about the degree of personal autonomy and informational confidentiality an individual should have when he or she is in the workplace using the technologies of the time. Not surprisingly, current privacy law doctrine evolved slowly and was largely developed for a time when telegraphs, typewriters, and mimeographs were the commonly used office technologies and when employers conducted business with paper documents transmitted by postal mail. Unlike a few other employment law doctrines that have recently created legal uncertainty after they were repealed or drastically revised, the legal protections that exist as a result of privacy law doctrine are being overpowered by technological force, not legislative or judicial intervention. In other words, the prevalence of digital technology in the workplace implicitly constructs a new objective reality regarding expectations of privacy. Paradoxically, privacy protections have been significantly weakened, notwithstanding the apparent vitality of current privacy law. In the digital age, however, workplace technologies are so advanced and sophisticated that societal notions about the degrees of intrusiveness that a particular technology may pose are often based on unfounded or mistaken assumptions about the possible uses of digital technologies. [8] The failure of courts, in particular, to grasp the fundamental nature of digital technologies is especially troublesome regarding workplace privacy issues since many employers use digital technologies to surreptitiously monitor employees' activities. [9] When workers do not know they are being monitored, the right of privacy is presumptively eroded. To thwart the de facto erosion of workplace privacy, privacy law must be expanded to encompass the present-day realities and future possibilities of high technology and its impact upon employer monitoring practices. In attempting to resolve the legal and moral questions that arise when employers engage in monitoring activities, a new balance must be struck between employees' right of privacy and an employer's need to manage its workforce.

{4} Surreptitious and sweeping surveillance of the workplace through the use of digital technologies should be presumptively unwarranted under the law of privacy. [10] As such, employers could only use such technology when particularized suspicion of harmful or unlawful conduct of an employee could be articulated or when the presumption could be rebutted by evidence of exigent circumstances. And, in no case, should an entire workplace be subject to widespread surreptitious surveillance. Surreptitious workplace surveillance, when such use is warranted, should be limited to the area of the workplace for which particularized suspicion has been articulated.

{5} At first glance, this proposed enhancement of privacy doctrine may seem extraordinarily disadvantageous to employers. Yet, it is not. Instead, this proposal tips the balance more evenly between employee and employer. Noteworthily, relevant case law has permitted the termination of employees by employers who have determined that an employee surreptitiously used surveillance technology against his employer. [11]

{6} In particular, employers are relying on technology to make their operations more efficient by using high-performance computers linked together as private networks, which are then connected to a vast collection of networks called the Internet. As part of their information infrastructure, employers utilize a combination of mainframes, desktop computers, routers, servers, database software, program applications, and connections to external computer systems. This information infrastructure is both expensive and highly valuable to the employer. [12] Not only are employees able to work more efficiently, but employers can reap significant competitive benefits by investing in and developing the right kind of information infrastructure. In this respect, an employer's interest in securing their information infrastructure from damage or sabotage is magnified by the vulnerability of the infrastructure when it is interconnected to other computer systems - - like the Internet - - and when access to the information infrastructure is granted to most employees. [13]

{7} Undoubtedly, one of the most difficult problems arising out of the everyday use of interconnected computer systems facing employers is whether, and if so, in what manner, to use modern surveillance technology [14] to monitor employees' use of the computer network. [15] In the workplace, this issue involves two competing values: security and privacy. Employers want secure computer networks. Employees want protection from impermissible intrusions into their personal privacy. [16] Although the protection and security of an employer's information systems is not a trivial matter, neither are the concerns of employee right of privacy. As the technological surveillance capabilities of employers increase, similarly, an employee's right of privacy protections must grow in response. Digital technology provides employers with an arsenal of extraordinarily intrusive methods of workplace surveillance. These technologies enable employers to record unsuspecting employees engaging in very personal and private behavior. [17]

{8} Although hackers have been exploiting security weaknesses of computer systems and have been viewed as external threats to networks connected to the Internet for years, the increasing number of employers who have connected to the Internet has brought to the forefront a more serious threat: employee sabotage from inside the organization. [18] The threat of employee sabotage coupled with the rapid growth and reliance on interconnected computers, have turned Cyberspace and some work spaces into a veritable electronic frontier. Undoubtedly, the need to secure information from those who might damage expensive computer systems or conduct economic espionage or perform some other havoc has never been greater. The concomitant risk that employers may implement digital surveillance and monitoring systems that require employees to surrender substantial privacy interests is also greater than ever before. In most cases, a prudent approach to this problem involves a simply stated, but notably difficult solution; namely, selecting an appropriate level of monitoring or protection of the employer's network, while ensuring that the security measures adopted do not breach the fundamental privacy interests' of employees.

INTRODUCTION

{9} There are no laws prohibiting employers from using digital surveillance [19] to monitor employees in the modern American workplace. [20] In this respect, the Orwellian nightmare of the Thought Police and Big Brother appears to reflect reality and has several disturbing similarities to the current widespread use of surveillance technology in American workplaces. [21] Employers now have an unprecedented ability to monitor virtually every aspect of an employee's activities throughout the day using video surveillance, electronic eavesdropping, [22] and a wide variety of computer monitoring techniques. [23] The presence of surveillance technology [24] has become so ubiquitous that it appears as if the right of privacy for employees is facing inevitable extinction. [25]

{10} The growing presence of surveillance technology [26] may be directly related to the nature and prevalence of computer technology; particularly the expanding use of computer networks. As employers

expand their reliance on automated and interconnected information systems, they face an increasing challenge to protect the integrity, confidentiality, and availability of the data they maintain. Along with this challenge comes the need to implement methods that enable employers to maintain a watchful eye on the use of their computer and information systems by their employees. Although employers have relied on computers for years, employers throughout the world are experiencing an explosion in the growth of electronic data and networked computer systems, [27] and in the way that organizations collect, process, store, and disseminate information. [28] The presence of digital technology [29] in the workplace has become widespread and far-reaching as a result of the use of desktop computers and the Internet. [30] The Internet, in particular, has revolutionized the information [31] of the nation's businesses and governments by linking a vast number of business and organizations to each other. This interlinkage enables the efficient electronic transfer of funds, the distribution of electrical power, and varying forms of digital communications. Harnessing the power of desktop computers wired together has already proven essential for many businesses to compete effectively in the information age.

{11} Yet, our dependence on the new information infrastructure has created new vulnerabilities for employers who are connected to the Internet. Employers are relying on an unprecedented use of digital surveillance technology, ostensibly, in order to protect the integrity of the employer's information systems connected to the Internet. On October 20, 1997, the President's Commission on Critical Infrastructure Protection [32] (the Commission) issued a report identifying the nation's dependence on computers and telecommunications as posing unprecedented risks that an organization's computer network connected to the Internet may be harmed by an insider or someone legitimately authorized access to a system or network. In addition, another report issued by the Federal government found that government agencies were severely lacking in implementing systems to safeguard information technology from malicious attack. [33] In other words, the vast number of employers who have connected their computer systems to the Internet have also rendered these systems vulnerable to malicious attack by disgruntled workers. The potential risks include the danger that sensitive and critical information could be inappropriately modified, disclosed, or destroyed, and possibly result in significant monetary losses for an employer or, if a government employee sabotages his employer's computer system, such could result in a loss of confidence in the government's ability to protect confidential data concerning individuals. [34]

{12} These potential risks are increasing because automated systems and records are fast replacing manual procedures and paper documents, which in many cases are no longer available as backup, if automated systems should fail. [35] As such, the vulnerabilities of an employer's information infrastructure are exacerbated because, when systems are interconnected to form networks - like the Internet -- they are not only much more vulnerable to anonymous intrusions from remote locations, but workers from inside the company can potentially sabotage an employer's computer system much more easily than before, and the effect of an attack one computer system interconnected to others could easily multiply the damage exponentially. [36] So grave does the Federal government view this problem that the Commission recommended several policy and legislative changes to thwart the threat of a so-called Cyberspace meltdown. [37]

{13} Interestingly, the Commission found that employees and other insiders provide the most frequent avenue of attack to an organization's information infrastructure. Quite remarkably, the Commission concluded that the Federal government, as an employer, has been better able than the private sector to protect against employee sabotage as a result of having the legal authority to conduct background investigations of employees and applicants. [38] To assist other employers, the Commission recommended changes in certain fair employment and privacy right restrictions that currently preclude private sector employers and others from lawfully adopting practices that could allegedly assure employers that the company's computer systems and information infrastructure were adequately protected from sabotage by disgruntled or rogue employees. [39]

{14} The Commission recommended, inter alia, that the Attorney General impanel a group of professionals from law, state and Federal governments, labor and management organizations, and the privacy community to explore existing laws and recommend measures to safeguard employer networks that do not fully compromise employee right of privacy. The Commission's report is notable because it directed the nation's employers to seriously consider whether the ubiquitous presence of interconnected computer systems sufficiently justified the need to consider how these computer systems and the information and data they maintain could be compromised by unhappy or malicious employees. Although the critical importance of an employer's information infrastructure warrants sufficient considerations of how to protect and safeguard information technology, the Commission's view of the American workplace is uncompromisingly cynical. [40]

{15} Indeed, another view of the impact of information technology on the workplace reveals that the unmistakably intrusive nature of digital technology and its many uses for workplace surveillance warrant an examination of whether an employee's privacy interests are sufficiently protected by current law. [41] Not surprisingly, the formulation of the question may have a pivotal impact on the nature of the answer. In this respect, questions concerning the right of privacy often entail ready-made assumptions about the importance of privacy; unfortunately, these assumptions limit or confine the privacy interest at the start of the analysis. [42] To thwart the reliance on false or improper assumptions about an individual's interest in privacy in this case - the employee, once a privacy right is detected, privacy analysis should begin by setting forth the countervailing interests, which will be weighed against the interests of privacy, to establish the real impact of the countervailing interests. In framing the analysis in this manner, the outcome will not be limited to the rather predictably interdependent conclusion that the privacy interest should or should not be further restricted, but, instead, could include the determination that the privacy interest should be expanded.

{16} Under this framework, the questions concerning whether or how the status quo-workplace should be altered in view of the ubiquitous presence of digital technology would be vastly different than the questions the Commission posed. What follows is an analysis of whether the presence of the Internet and other digital technologies in the workplace, which can be used for unprecedented workplace surveillance, warrant a reevaluation of whether current laws adequately protect employee right of privacy and, if so, what is the outcome of that evaluation?

Internet History

{17} Today the Internet is composed of a global network of over 4 million host computers linking approximately 35 million people in 140 countries. [43] According to some online observers, the number of people who join the Internet community expands by nearly a half million per month. [44] During the 1980s, the National Science Foundation (NSF) built the high-speed, long-distance data lines that carry Internet traffic and that form the Internet's so-called backbone or basic network infrastructure. [45] Internet traffic moves over almost any physical channel - telephone lines, cable-TV setups, satellite links, wireless phones, or high-speed fiber-optic trunks. Through a collaborative effort among universities, national labs, large corporations, and national governments funding and technical support was provided for operating the global network. [46] In 1991, the NSF ended restrictions on commercial usage of the Internet, which ultimately opened the floodgates to the general public. [47] As its design suggests, decentralization is one of the Internet's salient features. In keeping with its goal to withstand the impact of a nuclear blast, there is no central authority that controls the content or functioning of the global network. Highlighting the absence of central control on the Internet is the reality that there isn't even a master switch or magic fuse that can shut the Internet down in case of emergency. [48] At its inception, therefore, the Internet embraces a concomitant degree of vulnerability and invincibility: presumably the entire network cannot be shut down by the acts of one individual or group, but the Internet also opens doors to the private networks interconnected to it that cannot be shut or entirely

controlled once a TCP/IP connection is made. [49]

{18} The Internet is a network of computers that are linked together, allowing computer users to share information and data. [50] Each computer that is linked to the Internet contains a numeric address called an Internet protocol address, or IP address. [51] The numeric IP address has four parts, each separated by a decimal point. However, since it is easier to use, each computer is given an alphanumeric address, called a domain name, which corresponds to the IP address. [52] When an Internet user types in the domain name, the user's computer reads the name as the numeric IP address and contacts the appropriate computer. An example of such a domain name is "redlaw.com". Domain names are the alphanumeric monikers that ease the use of the Internet. Computers are linked on the Internet by "IP addresses," which are each composed of a long string of numbers. Each computer or user has a unique number, so that information can be directed to a specific destination, by using the IP address. [53]

{19} The domain name is a more accessible, more memorable, occasionally catchy, title that can be attached to an IP address. However, domain names must be unique, to avoid confusion in delivery. To send electronic mail ("e-mail"), the user addresses the message to the domain name of the recipient's e-mail provider. America Online, for instance, is an e-mail provider, whose domain name is "aol.com". Each user of the America Online service is given a user name to use with the domain name (e.g., "harrysmith"). Therefore, if a person wants to contact Harry Smith, an America Online subscriber, the user would send an e-mail message to "harrysmith@aol.com". The computer would read "aol.com", translate this into the corresponding numeric IP address, and deliver the message to the America Online computer, which would then deliver the message to Harry Smith.

{20} The domain name may also function as a "World Wide Web" address, if preceded by the letters www (e.g., www.redlaw.com). Web sites are pages of electronic information that a company, organization, or person wants to advertise to Internet users. Entities and people such as Sports Illustrated, Duke University, the National Basketball Association, and certain individual politicians have web sites that allow Internet users to look up information. [54] Once connected to the Internet, users are able to access and transmit data across Cyberspace in many different ways, including using electronic mail (e-mail) and downloading home pages from the World-Wide Web (the Web). [55] E-mail allows users to easily send primarily text-based messages between computers. The Web employs a point-and-click technology, which allows users to easily access information on other computers as well as establish Web sites that incorporate graphics and other multimedia features. [56] Much of the Web's usefulness is derived from its use of links. [57] A user interested in accessing the referenced document selects the link, causing the document to be displayed automatically, along with a new set of links that the user may follow.

{21} While the linked structure of the Web is well-suited to allow users to browse among many sites, following whatever links happen to draw their interest, it is poorly suited for users who want to find a single Web site directly. Users searching for a specific Web site have two options. First, if users know or can deduce the address of a Web site, they can type the address into a browser and connect directly to the Web site as if dialing a telephone number. [58] More often, users do not know the exact address and must rely on search engines available on the Web to search for key words and phrases associated with the desired Web site. Because of the quantity of information on the Web, searches often yield thousands of possible Web sites. Such a cumbersome process often leads to what is now commonly known as web surfing. Web surfing consists of a user going from one web page to another in a rather haphazard fashion in an attempt to locate a website of interest. Web surfing is particularly alarming for employers because it inevitably leads to a significant amount of inefficient computer use. More important, website surfing may lead to a user unexpectedly coming upon an obscene web page or encountering malicious programs. [59] The Web is filled with malicious code that either disable an employer's computers or, perhaps worse, enable theft of trade secrets or other important data stored on an employer's private

network. [60]

{22} Undoubtedly, the Internet has revolutionized the information infrastructure [61] of many employers by linking many organizations to one another. This interlinkage enables the speed and efficient electronic transfer of funds, the distribution of vast amounts of information as well as varying dimensions of digital communications. [62] This form of networking has already proven essential for many businesses to compete effectively in the information age. Yet, dependence on the new information infrastructure has created new vulnerabilities for employers who are connected to the Internet.

Areas Where Employers Are Subject to Liability

{23} In this digital age, employees may be exposing their employers to unprecedented liability risk [63] now that many desktop computers in the workplace are interconnected to the Internet. [64] For instance, pornography may enter the workplace as a result of an employee downloading graphic images from the Internet. Once these images are downloaded, they may be viewed on a computer screen or transmitted to other employees via e-mail. Under these circumstances, an employer may be exposed to a sexual harassment lawsuit or the employee, himself, may be engaged in criminal conduct.

{24} In December 1997, a lawyer at the law firm Dickstein Shapiro Morin & Oshinsky was discovered using the Internet to access pornographic materials from his desktop computer. The lawyer was not dismissed. Instead, the firm suspended his Internet privileges for a few weeks and fined him an undisclosed sum for acting in contravention of firm policy. [65] Although this employer apparently escaped economic harm, the firm was exposed to embarrassing publicity from news accounts of the event.

{25} Despite the fact that Interconnected computer systems are now a fact-of-life for most modern office employers, some employers are just beginning to develop policies on the proper uses of technology in the workplace while others have still not done so. Indeed, a wide swath of employers are confronting this issue. The problem of stemming the tide of inappropriate e-mail messages and graphic digital pictures at work has come to the forefront lately because of the casual attitude many workers display when using their employer's computer equipment.

{26} One, largely unanticipated, problem with granting workers wide access to the Internet is the reality that when an employee visits a web site they leave a trail usually identifying the employer who owns the computer. [66] And, there's more than just personal embarrassment at stake. In February 1995, Chevron Corp. settled a suit brought by four female workers who were distressed by descriptive, sexual e-mail sent around the office. The settlement cost the company $2.2 million; to wit, employers have a significant basis to presume that monitoring employee Internet activity is justified to prevent an employer from being held liable for the website viewing habits of employees.

{27} Indeed, that's exactly what happened at Dickstein, Shapiro, the law firm mentioned supra. The unnamed lawyer's actions came to light only after he allegedly printed an indecent image from his computer screen. He sent the document to a printer, where a staffer saw it and later complained to management.

{28} Additionally, sexual harassment claims may have serious consequences for an employer. Statistics have shown that many employees spend a "disturbing" amount of time surfing pornographic Websites during working hours. Employees at I.B.M., Apple Computer, and NASA logged on to the Penthouse website thousands of times per month during 1996. [67] Of course, employers are not without remedial measures to significantly decrease unwanted Internet abuses, short of denying workers access to

Interconnected systems like the Internet. Indeed, employers are using monitoring devices as technological solutions to this problem. One technological solution involves the use of a proxy server for access to web sites. A proxy server acts as a giant cache for the employer's network. Instead of requests for Web pages going directly out to the Internet, they're passed through a proxy server. If the proxy server already has the requested page stored locally, it delivers it to the employee's Web browser, or Internet software, without going out to the Internet.

{29} The advantage of using a proxy server from an employer's standpoint is that, because all Web requests pass through the proxy server, it can track all those requests. By checking the proxy server's records, an employer can find out every site visited by every employee on its network. [68] Employers also have access to software that can monitor Internet access and keep a log of all activity. For example, Cyber Snoop, is a software application that runs on an employer's network and provides Internet blocking and monitoring capability with features that could enable an employer to monitor employees' Internet use, including Web activity, FTP downloads, chat discussions, e-mail messages and Usenet news group posting activity. [69]

{30} In the digital age, it has become common practice for sexual harassment plaintiff's lawyers to seek copies of an employer's network e-mail logs during discovery. This practice could be critical to an explosive case even if only a few, out of several thousand, offensive e-mail messages are discovered. The consequences for technology-related harassment suits in the private sector have become an employee's grist in supporting a wide variety of employment discrimination cases against employers like Morgan Stanley, Citibank and R.R. Donnelly. [70]

{31} In a recent case involving Oracle Corporation chief executive Larry Ellison, Ellison's former girlfriend, Adelyn Lee, was convicted of sending him a falsified e-mail. [71] That very e-mail, in which Ellison was purported to have been told by Lee's supervisor that "I have terminated Adelyn per your request," was the key piece of evidence that originally led Oracle to settle with Lee for $100,000 in her wrongful termination suit. [72] But cellular phone records showed that Lee's boss, Oracle vice president Craig Ramsey, was in his car at the time of the e-mail transmission, and could not have been the sender. [73] What the Oracle case illustrates is that e-mail is as much a type of evidence in employment cases as traditional documents or oral evidence has been. [74]

{32} Generally, employers consistently articulate three considerations that drive the need for monitoring Internet usage by employees: [1] employee productivity; [2] cost of network bandwidth and technology resources; and, perhaps most importantly, [3] the potential negative publicity and legal liabilities resulting from inappropriate use of the Internet.

{33} Employers are typically concerned about the impact of non-business related Internet surfing on employee productivity. It is often assumed that excessive Internet usage results in measurable organizational costs -- e.g., upgrading network resources like leased lines, routers, disk storage, and printers to handle the increased load -- and wasted time caused by slow network response, the deployment of anti-virus programs, and an increase in unreliable connections. [75]

{34} Undoubtedly, as a result of the use of interconnected computer systems, employers can be held liable for the acts of their employees in a variety of ways, including defamation (from inflammatory e-mail messages or harmful electronic bulletin board postings), copyright infringement (from installing or downloading pirated copies of software onto employer owned computers), sexual harassment (from offensive or hostile e-mail messages), obscenity (from downloading or distributing obscene graphic images or use of offensive material that is distributed by means of the workplace e-mail system), and discrimination. [76] For example, in one case, still pending, two African-American employees sued their employer, Morgan Stanley, under Title VII claiming that a white employee authored and sent e-mail

messages containing racist or offensive jokes and that Morgan Stanley tolerated a racially hostile environment to exist by permitting the jokes to be passed around through the corporate e-mail system. [77]

{35} In addition, employers may be subject to liability for the conduct of their employees in other ways. Employees who download unlicensed copies software programs from the Internet or install pirated copies of applications on their desktop computers leave their employers liable to legal challenges on copyright infringement. Software piracy is a common area of liability exposure on the Internet. If an employee uses company equipment to download software, and then wrongfully distributes the software or unlawfully makes changes to it, the company could be held liable for piracy -- which is, in effect, copyright infringement.

{36} Finally, e-mail can be a very dangerous means of intentionally leaking corporate trade secrets. Employers want to minimize the legal risks associated with the Internet since providing access to the Internet is akin to giving employees access to a ubiquitous, powerful, communications tool that allows instantaneous communication to others throughout the world. This is particularly true with regard to the protection of trade secrets. [78] Trade secrets are, obviously, one of the most confidential types of information owned by an employer to which an employee may have lawful access. Although courts decide on the individual circumstances of the case what is or is not a trade secret, the most important factors in making this determination are the nature of the information and to what extent the employer treated it as confidential within its organization. Examples of trade secrets include: special manufacturing processes, chemical formulae, designs, a board's corporate strategy, or highly sensitive financial information. [79] Loss associated with stolen trade secrets can be substantial. In some cases, the loss associated with the public revelation of a trade secret is more a matter of reputation than pecuniary interests. While Borland Corporation was surreptitiously using electronic surveillance to monitor its employees' e-mail messages, it discovered that one of its high level software executives, who had announced an imminent departure from the company, was sending e-mail messages that contained corporate trade secrets to his future boss, Gordon Banks, the president of Symantec Corporation. Borland reported its discovery to law enforcement officials who charged the employee, Eugene Wang, and Banks with theft of trade secrets under California state law. [80]

Areas Where Employers Are Subject to Employee Sabotage

{37} In the Federal employment sector and in accordance with the Paperwork Reduction Act of 1980 (Public Law 96-511), OMB is responsible for developing information security policies and overseeing Federal agency practices. In this regard, OMB published its guidelines on Federal sector information security in what is commonly referred to as OMB Circular A-130. [81] In addition, responsibility for developing Federal agency technical standards and providing related guidance for sensitive data belongs primarily to the National Institute of Standards and Technology (NIST), [82] in accordance with the Computer Security Act. [83] In the Federal government, primarily, information security risks are most troublesome when unauthorized persons gain access to highly sensitive information in the Defense Department's (the Pentagon) computer systems. Surprisingly, the Pentagon's computer systems are compromised frequently and more than a few of the attacks are considered malicious insider attacks. [84] Although the exact number of attacks [85] cannot be determined precisely, the Pentagon believes that it may have experienced as many as 250,000 attacks in 1995. These attacks are often successful! The number of attacks have doubled each year during the 1990s as Internet use as also increased. At a minimum, these attacks amount to a multimillion dollar nuisance to the Pentagon. At worst, they frequently pose a serious threat to national security.

{38} In one well publicized information security breach, in 1990, the computer network at the Air Force's Rome Laboratory in Rome, New York (Rome Laboratory) was sabotaged. Rome Laboratory is

considered the Air Force's premier command and control research facility -- it works on very sensitive research projects such as artificial intelligence and radar guidance. In March and April 1994, Rome Laboratory's computer systems were attacked by hackers and other unknown individuals over 150 times. The attack, which is thought to have involved insiders as well as hackers, ultimately succeeded in shutting down thirty three government network systems for several days. [86] During the attacks, the intruders stole sensitive air tasking order research data. [87] Air Force Information Warfare Center staff estimated that the attacks on Rome Laboratory cost the government over half a million dollars. [88] If the research project had been damaged beyond repair, it would have cost about $4 million and 3 years to reconstruct it. [89]

{39} Additionally, an employer's vulnerability to insider or employee infrastructure sabotage is not limited to the public sector. Private sector computer systems have been attacked and damaged by disgruntled workers with increasing frequency. In a case that is believed to be one of the most expensive computer sabotages in history, Timothy Lloyd, 30, of Wilmington, Delaware, was charged with intentionally damaging Omega Engineering Corporation's (Omega) computer system by activating a software-bomb that permanently deleted all of the company's software and system files. Lloyd's former employer manufactured high-tech measurement and control instruments used by NASA and the Navy. As a result of the damages caused by the software-bomb, [90] the company had to forego millions of dollars in sales and contracts with the Federal government. Lloyd, who was a chief computer network program designer at Omega, allegedly became exceptionally frustrated after Omega decided to dismiss him for poor performance. Lloyd is now facing possible conviction and a prison sentence of 15 years. [91]

Electronic Surveillance Techniques Used By Employers

{40} Employers may use electronic surveillance techniques to monitor employee performance. In the name of assessing productivity, telephone company supervisors eavesdrop on their operators and used software to count and record the number of keystrokes per minute entered by the data entry workers. White-collar-knowledge-workers are also becoming just as vulnerable to electronic surveillance. [92] In the settlement of a class action lawsuit brought by the Communications Workers of America (CWA), Northern Telecommunication Corporation (Northern Telecom) agreed to compensate workers whom the union alleged were subjected to secret electronic surveillance over a 13-year period at the company's Nashville, Tennessee location. In addition, as part of the settlement, the company announced a new policy banning all forms of undisclosed employee monitoring. The new policy affects more than 22,000 workers at Northern Telecom. Apparently, Northern Telecom used hidden bugging devices and telephone wiretaps at several locations in the Nashville plant between 1976 and 1989 to identify and weed out CWA supporters and thus thwart unionization drives. [93] Although an employer has many reasons to conduct surveillance on its employees: to detect theft or tardiness, to monitor quality control or poor job performance, to examine the workplace for the presence of drugs and alcohol, [94] oftentimes, what an employer would like to do, and what an employer is legally allowed to do are two very different things.

{41} Some Federal agencies often use the same monitoring techniques they use to monitor employee Internet use as they use to monitor the public's computer users are visiting their websites. For example, the Department of Labor uses sniffer [95] programs to record the IP [96] addresses of users who visit the agency's web pages. [97] These same programs are installed on the agency's network computers to monitor the websites visited by the agency's employees. [98]

{42} Undoubtedly, the digital age has brought about both unprecedented resources that employees may rely on to increase productivity and efficiency and unprecedented possibilities for employees to use the resources provided to them to the intentional or unintentional detriment of the employer. Consequently,

it would be obnoxious to common sense and plain logic to deny that employers, whose information infrastructure includes the use of technologies like the Internet, have legitimate interests in protecting and securing their computer networks through some use of monitoring technologies. The issue remains, however, to what extent should surveillance technology be put to use?

The Scope of an Employee's Right of Privacy

{43} Generally, and under the right circumstances, employers can use private security guards, supervisors or managers or technological devices, such as video cameras, to monitor employee activities without running afoul of an employee's right of privacy. [99] Under the law of communication privacy, whether the circumstances of a communication justify a belief that it is not subject to interception is analyzed in the same manner as the question of whether an investigative activity amounts to a search: that is, whether there is a justifiable expectation of privacy at the time and place of the communication. [100] Privacy law [101] is confusing because its sources stem from tort law, constitutional law, criminal procedure, civil procedure, family law, and contracts. [102] Nonetheless, in the context of the workplace, the fundamental concern raised under the tutelage of the right of privacy actually may boil down to the complex task of defining the proper contours of when it is appropriate for countervailing interests - - be they the interests of the government or the employer - - to justify an employee's loss of individual power and personal autonomy. [103] The Federal Constitution protects an individual's privacy in many spheres of privacy [104] including the interest in preventing the disclosure of certain types of personal information [105] without consent. [106] Of course, the Constitution's protections are not absolute. [107]

{44} In Griswold v. Connecticut, [108] the United States Supreme Court enhanced the jurisprudence of privacy by declaring that a Connecticut law forbidding the distribution of contraceptives violated the right of "marital privacy." The Court defined the right of privacy as being imputed from the "zones of privacy" [109] or "penumbras" emanating from general constitutional protections of liberty. [110] Interestingly enough, the Griswold case is a provocative precursor to contemporary privacy issues brought about by the present-day increasing use of digital technology in the workplace. The expansive right of privacy protected by Griswold resulted, in part, from technological advancements in birth control. [111]

{45} Another fundamental privacy case is Roe v. Wade. [112] This case established that the constitutional right of privacy [113] protects a woman's decision to have an abortion. [114] Although Roe appears to have been altered by Planned Parenthood of Southeastern Pennsylvania v. Casey, [115] the case remains good law, but it too may be eventually affected by technological advancements. [116]

{46} In the workplace setting, common law, statutory, and constitutional tests used to determine whether a reasonable expectation of privacy exists, in turn, require an initial determination whether there is an actual (or subjective) expectation of privacy. [117] The latter, objective determination [118] is tested against the customs, values, and common understandings that confer a sense of privacy upon many of our basic activities. [119] Thus, whether there is a legitimate expectation of privacy in a particular case depends necessarily on the facts and circumstances, with the actual expectation manifested by a party being a question for the fact-finder and the objective reasonableness [120] of the expectation being determined for the particular circumstances as a matter of law. [121]

{47} It is generally accepted that there is a legitimate expectation of freedom from visual electronic surveillance by police [122] in private rest rooms or private areas of public rest rooms. [123] This expectation of privacy is objectively reasonable both because of the setting, [124] compare People v. Triggs, supra (reasonable expectation of privacy in restroom) with United States v. Hitchcock, [125] and because individuals can shield themselves from view. Notably, it is legitimate to expect that a particular

conversation will not be electronically intercepted by the police. [126] Moreover, there can be a legitimate expectation of freedom from clandestine electronic interception of a conversation by police despite the fact that the police or others might hear a conversation unaided. And, simply because a person allows one conversation to be overheard by nearby individuals does not mean that the expectation of freedom from electronic reception by police is objectively unreasonable. [127] This is because the legitimacy of an expectation of privacy depends, in part, on the ability of persons to control their circumstances. [128] And, without a warrant, police may not negate an otherwise reasonable expectation of privacy by surreptitiously eliminating such control. [129] Thus, while a listening device may be properly used to reveal information otherwise available by personal observation were a police agent actually present, [130] it may not be used without a warrant when its value is in hearing what a visible observer could not overhear. [131]

{48} Although conflicts over workplace privacy are increasing, legal analysis of the issue remains fragmented. A number of federal and state statutes regulate aspects of employee privacy, but each addresses only a particular, narrowly defined invasion. For example, separate federal statutes regulate the use of polygraph testing, credit reports, and medical examinations by employers. Similarly, over half the states have statutes regulating the use of polygraphs in employment; at least fourteen limit employer drug testing plans; and nearly two dozen forbid adverse employment actions based on off-duty tobacco use. No statute, however, deals with the issue of employee privacy in any comprehensive way. [132]

{49} The federal wiretapping law, Title III of the Omnibus Crime Control and Safe Street Act of 1968, 18 U.S.C. 2510-2525, as amended by the Electronic Communications Privacy Act of 1986, 18 U.S.C. 2510-3126, prohibits any person from intentionally intercepting, using, or disclosing any wire, oral, or electronic communication. [133] In the employment context, this frequently arises in the context of an employer taping telephone calls made to and from the business phone. There are two exceptions to Title III's coverage relevant to employers: [1] the prior consent exception, [134] and [2] the business extension exception. [135] Generally, an employer may be able to monitor sales or marketing calls for training or other legitimate purposes. The exception, however, will not extend to the monitoring of personal calls made by the employees on the same telephone lines. [136] The type of surveillance used seems to be a key factor affecting whether the employer's use of such equipment will be upheld in court. [137] For example, video cameras that also record sound are covered by the federal Wiretap Act as described above. However, video cameras that merely record activity, particularly when visibly placed in public work areas, have not been found to be a violation of employee privacy under the Act. [138]

{50} Five current or former workers at a Sheraton hotel in Boston are suing the company for secretly videotaping them and other workers in the male employees' locker room over a seven-week period in 1991. The workers say they were humiliated after discovering that some of them were captured on videotape in their underwear. Such videotaping may be viewed as an attempt by employers to control every aspect of workers' lives while they're on the job, and that includes when they're changing their clothes or taking breaks. [139]

{51} ITT Sheraton Corporation defended its actions by arguing that the videotaping was intended to investigate suspicions of drug dealing. A previous survey, a poll of 301 businesses by Mac-world magazine in 1993, found that 22% had engaged in searches of voice or electronic mail or computer files. [140] Electronic surveillance is most prevalent in larger organizations where employees perform routine jobs at a computer or on the telephone. [141] Apparently, the majority of employees being electronically monitored are women in low paying clerical positions. [142]

{52} In Watkins v. L.M. Berry & Co., [143] the employer intercepted a personal phone call. The court found that the employee did not give consent to this action and therefore the employer violated the Wiretap Act. [144] The interception of a personal call was also the alleged harm in Epps v. St. Mary's

Hospital of Athens, Inc. [145] In that case, the employer was found to be in compliance with the Wiretap Act because its actions fell within the business-extension exception. [146] As noted, in one of the most extensive cases of covert monitoring to date, Northern Telecom agreed to settle a suit filed by the Communications Workers of America. [147]

{53} Of course, not every violation of privacy norms warrants legal intervention. Some intrusions are so trivial that they will be experienced by most people as mere annoyances or rudeness. The intensity of social life inevitably results in frequent minor personal offenses. These breaches of social norms are easily repaired through ritual interchanges--a simple apology is the most obvious example--which are designed to affirm the norm violated and to vindicate the victim's claim to basic forms of respect.

{54} The law, however, should be concerned with serious violations of personal autonomy and human dignity, those which threaten an individual's self-regard and honor. From its first articulation by Warren and Brandeis, the right of privacy has been linked to the principle of an inviolate personality. [148] As such, the values underlying the right of privacy rests on a conception of privacy that is concerned with maintaining basic forms of respect for the individual. [149] Since the observance of fundamental social norms by others is a crucial constituent of individual personality, violation of these norms is itself harmful, independent of other considerations because privacy can be understood as redressing human dignitary harm. [150]

{55} In addition to an intrusion, a violation of privacy involves an element of loss of control over one's personal human dignity. [151] The degree of this loss of control affects the significance of a given intrusion. For example, the passerby who lingers by a bedroom window in order to overhear private conversations can be easily shut out by closing the window, while the surreptitious use of a listening device to acquire the same information leaves the victim feeling a sense of loss when the intrusion is discovered and the victim recognizes that he could do nothing to prevent the intrusion since the invasion of privacy was furtive and secret. [152] Indeed, the worst since of loss of human dignity may occur when an individual is systematically deprived of privacy through the exercise of power by another - such as in the employment context. In such cases, power is used to intrude directly, or to force another to expose aspects of himself to the boss. [153] Even in these contexts, however, there may be a kind of quid-pro-quo relationship wherein the employee knowingly relinquishes a degree of personal autonomy in exchange for the opportunity to earn a living. [154] Nonetheless, covert surveillance would still exceed the bounds of this relationship. The employee cannot be assumed to have consented to or agreed upon the presence of surveillance simply because of its possibility. With little doubt, a fair agreement would require the employee to be put on notice that surveillance is taking place. In this respect, the sense of loss of human dignity or personal autonomy may not be as injurious since the knowledge and awareness of surveillance empowers the employee with the ability to control the degree to which he exposes aspects of self to the employer. [155]

{56} At first blush, this may not appear to serve the employer's needs well. But, even under the current doctrine of privacy law, the employer is never justified in insisting on unlimited access to employees. [156] This is particularly true of certain forms of invasive electronic monitoring. As noted, supra, in the case of e-mail: an interesting condition of e-mail is that e-mail seems to promote a certain type of candor in its users. In this respect, e-mail messages tend to be more revealing of a person's inner feelings than a traditional paper document. As such, an employer's monitoring of e-mail messages surreptitiously obtains unauthorized access to an employee's personal self. [157]

{57} In this digital age, employers must be permitted to undertake reasonable precautions to protect and secure their information infrastructure. It can hardly be doubted that employers face unprecedented vulnerabilities to their computer systems and private networks when those technologies are interconnected to the Internet. In this regard, employers have legitimate interests in surveillance

technologies and other devices that assist employers in securing their vital information infrastructure. Yet, the employers' interests are not without their limits.

{58} Contemporary interpretations of privacy law doctrine has left employers with an arsenal of powerful technologies to use in the workplace to surreptitiously monitor the activities of employees. This framework may have been sufficient when the critical issues of workplace privacy involved considerations of whether a manager could open a sealed envelope delivered to the employer, but addressed to an employee. [158] Although a great deal of the mail still is delivered in an envelope, billions of messages travel across employer networks in the form of electronic mail. Employers have the technological capability not only to read each message addressed to an employee, but to so undetected and unknown. In this respect, privacy law doctrine could impose clear limits on an employer's ability to lawfully undertake secret surveillance activities. Employment is not an all-encompassing relationship. Employers and employees enter into the employment relationship for a specific, limited purpose. The law of privacy is fundamentally concerned with serious violations of personal autonomy and human dignity; namely, those which threaten an individual's self-regard and deep sense of honor. When those core areas of privacy are threatened by an employer's interests in protecting and securing its information infrastructure, such intrusions should not be permitted. [159]

CONCLUSION

{59} As employers expand their use of information technology, they face an increasing challenge to protect the integrity, confidentiality, and availability of information that is vital to their business. The conclusion that employees do not lose all ordinary expectations of privacy merely because they enter into an employment relationship has been confirmed in a number of legal contexts. [160] Courts have often held that an employee does not somehow abandon his right to privacy at the doorstep of the employer's premises. [161] Merely by signing on to an employment relationship, an individual does not automatically open his entire private life to the scrutiny of the employer. Digital technology provides employers with an arsenal of extraordinarily intrusive methods of workplace surveillance. [162] These technologies enable employers to record an unsuspecting employee engaging in very personal and private behavior. [163] The increasing number of employers who have connected to the Internet has brought to the forefront a serious threat that employers could have their entire information infrastructure significantly damaged through employee sabotage. Moreover, employers face an unprecedented degree of risk of liability for the acts of their employees when those employees have access to the Internet.

{60} Undoubtedly, the need to secure information from those who might damage expensive computer systems or conduct economic espionage or perform some other such havoc has never been greater. The concomitant risk that employers may implement digital surveillance and monitoring systems that require employees to surrender substantial privacy interests is also greater than ever before. In most cases, a prudent approach to this problem involves a simply stated, but notably difficult solution; namely, selecting an appropriate level of monitoring or protection of the employer's network and also ensuring that the security measures that are adopted do not breach the fundamental privacy interests of employees. Unfortunately, most employers that engage in digital surveillance monitoring, do so surreptitiously. When workers do not know they are being monitored, the right of privacy is presumptively eroded. [164] To thwart the de facto erosion of workplace privacy, privacy law must be enhanced to encompass the present-day realities and future possibilities of technology and its potential impact upon employer monitoring practices. Surreptitious and sweeping surveillance of the workplace through the use of digital technologies should be presumptively unwarranted under the law of privacy. [165] As such, employers could only use such technology when particularized suspicion could be articulated or when the presumption could be rebutted by evidence of exigent circumstances. And, in no case, should an entire workplace be subject to widespread surreptitious surveillance. Surreptitious workplace surveillance, when such use is warranted, should be limited to the area of the workplace for

which particularized suspicion has been articulated. All surveillance technologies, operations and practices should be subject to procedures to ensure accountability. Explicit criteria should be agreed for deciding who should be targeted for surveillance and who should not, how such data is stored, processed and shared. In this manner, the values underlying the right of privacy, which rest on a conception of privacy that is concerned with maintaining basic forms of respect for the individual, will be legitimately supported by the legal doctrine.

ENDNOTES

[*] Rod Dixon is an attorney at the U.S. Department of Education, and is currently completing work toward an LL.M. degree in Labor Law at Georgetown University Law Center. (J.D. 1992 George Washington Law Center; M.A. 1986, University of Pittsburg; University of Pittsburgh in 1984).

[1] Digital technology can be used to efficiently express vastly different forms of information - such as factual databases, audio recordings, or electronic mail messages - on a desktop computer or across the Internet using bits of data in the form of computer 0s and 1s. Bits (or binary digits) are essentially the smallest and most fundamental units of digital technology data; each bit has a value of 0 or 1. The bits 0 and 1 represent off and on switches, which measure the presence or absence of electrical voltage in any given memory register of the computer. Since binary digits enable fairly easy digital expression and digital technology significantly expands the amount of data that can be processed on a single silicon chip, digital format has become the format of choice in electronics. *See* Rod Dixon, *Profits in Cyberspace: Should Newspaper and Magazine Publishers Pay Freelance Writers for Digital Content? - - Tasini v. New York Times*, 4 MICH. TEL. & TECH. L. REV. 5 (1998).

[2] So common is the use of digital technologies in the workplace, that this technology is now simply referred to as *information infrastructure*. This term of art is presumed to reflect the critical value of the underlying technologies that are used to maintain an organizations's personnel records, trade secrets, business plans, corportate strategy, customer lists - - information - - any information of value maintained in digital form. Notably, the White House and the Department of Commerce have begun to refer to the Internet as the National Information Infrastructure or the NII.

[3] Michael F. Rosenblum, *Security vs. Privacy: An Emerging Employment Dilemma,* 17 EMPLOYEE REL. L.J. 81, 86 (1991). Undoubtedly, employers have a strong interest in searching for new methods to make their employees more productive and for making the workplace safe. In this respect, some employers may justify the use of surveillance technology to improve employee performance, increase productivity, or increase worker safety practices; notwithstanding that such uses are usually challenged as pretextual excuses for monitoring employees, these uses are not the direct focus of this paper.

[4] Here, "surveillance" means employer controlled observation of employees to ascertain employee performance, behavior, characteristics, and other information by mechanical device or electronic means. This form of surveillance is automatic and unremitting. For example, monitoring devices that use computer technology can provide a means for an employer to view an employee's computer screen without the employee's knowledge. *See* Andrew M. Kramer & Laurie F. Calder, *The Emergence of Employees' Privacy Rights: Smoking and the Workplace*, 8 LAB. LAW. 313, 321 (1992) (citing Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898, 1903 (1991)) (noting technology that enables employers to count employees' keystroke and computer screen activity); Oscar H. Gandy, Jr., *The Surveillance Society: Information Technology and Bureaucratic Social Control,* 39 J. COMM. 61, 63 (1989) (noting that in addition to standard surveillance techniques, employers also use hidden microphones, video cameras, polygraph examinations, and computer programs designed to monitor productivity).

[5] Generally, although not consistently, courts weigh four factors to determine whether an employer's surveillance violates an employee's right of privacy: (1) the means that an employer used to acquire the information, (2) the employer's interest in obtaining the information, (3) the information's relevance to the employer's interest, and (4) the place of surveillance. Jeff Kray & Pamela Robertson, Comment, *Enhanced Monitoring of White Collar Employees: Should Employers Be Required to Disclose?,* 15 U. PUGET SOUND L. REV. 131, 144 (1991). In this respect, surveillance may not be actionable, if conducted in a reasonable, non-obtrusive manner with proper notice given to the employee. *Pemberton v. Bethlehem Steel Corp.*, 502 A.2d 1101, 1117 (Md. Ct. Spec. App. 1985) (citing *McLain v. Boise Cascade Corp.*, 533 P.2d 343, 346 (Or. Ct. App. 1975) and *Forster v. Manchester*, 189 A.2d 147, 151 (Pa. 1963) and *Ellenberg v. Pinkerton's, Inc.*, 202 S.E.2d 701, 703-04 (Ga. Ct. App. 1973)), *cert. denied,* 508 A.2d 488 (Md.), and *cert. denied,* 479 U.S. 984 (1986).

[6] The "privacy law doctrine" is fully developed, *infra.* Essentially, the concept is a short-hand way of referring to the basic principles underlying most privacy laws - - whether the law emanates from constitutional sources, common law tort or statutory right.

[7] Most instances of digital surveillance are not well documented, but many have become well known as a result of wide-spread publicity. Alana Shoars, a former systems administrator at Epson America Inc., was discharged for insubordination when she complained that company supervisors were secretly monitoring the electronic mail messages of employees. Alyeska Pipeline Service Company, the employer of Charles Hamel, secretly recorded Hamel's telephone conversations at work and at home through the use of electronic listening devices unauthorized by AT & T when Hamel became an outspoken critic of the company. Micheal Barriere, formerly employed by Delco Systems Operations in Santa, Barbara, California, was dismissed by his employer when he reported that he had discovered that Delco was furtively wiretapping and intercepting voice mail and e-mail communications of employees. Rebecca Huls, the electronic surveillance monitor for USAA Insurance Corporation, was discharged by USAA when she began monitoring management telephone conversations as well as employee calls. *See,* Robert Ellis Smith, WAR STORIES, vol. 1, 1993.

[8] Perhaps the most evident examples of mistaken societal assumptions about the uses of digital technologies are contained in lower court findings involving intellectual property issues and the Internet. There are an unusually large number of recent court decisions that have been criticized by commentators who reveal how those decisions were based on inaccurate assessments or entirely unfounded assumptions about the technology at issue. For similar reasons, Congress removed jurisdiction over patent cases from the various Federal circuit courts and created an ostensibly specialized court, the Federal Circuit Court of Appeals, to review appeals in patent cases. This is not to say that employment cases involving technological issues should be adjudicated by specialized courts. Rather, the point is simply to illustrate how the development of the law may be hindered or even corrupted when courts, or society, in general, hold mistaken assumptions about the uses of technology.

[9] Telephone monitoring is a standard method of employer monitoring. Supervisors may listen in on employee telephone calls or record conversations for later, more deliberate review. An employer may also electronically ascertain the party called and the number and duration of calls made by an employee or rely on advanced electronic monitoring devices by employing hidden, high-powered microphones and voice-activated tape recorders to record office conversations between and among employees. In addition, the technique referred to as computerized work measurement refers to the practice of monitoring an employee's computer screen as he works and collecting data about the employee's work performance for later review. *See* Gene Bylinsky, *How Companies Spy on Employees,* FORTUNE, Nov. 4, 1991, at 131.

[10] At bottom, the law of privacy should inform and remind us that the invasive nature of high

technology supports the notion that vigilant protection of the right of privacy must encompass the basic principle that personal autonomy and individual dignity do not become less important simply because the individual has entered a workspace. *See,* Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications*, 2 VA. J. L. & TECH. 4 (1997).

[11] For example, a Federal court in Maryland determined that terminating an employee for surreptitiously tape-recording conversations with his supervisors constituted a legitimate, non-discriminatory reason for discharge. In *Bodoy v. North Arundel Hospital,* 945 F. Supp. 890 (D. Md. 1996) the plaintiff, Angelo L. Bodoy, contended that his former employer, North Arundel Hospital (the Hospital), discriminated against him on the basis of his race and national origin in violation of Title VII of the Civil Rights Act of 1964 (Title VII), 42 U.S.C. 2000e (1994) and 42 U.S.C. 1981 (Section 1981). The Hospital moved for summary judgment on the retaliatory discharge claim, arguing, *inter alia,* that it terminated Bodoy for a legitimate, non-discriminatory reason -- the fact Bodoy surreptitiously tape recorded conversations between himself and his supervisors in violation of Maryland's Wiretap and Electronic Surveillance law, MD. CODE ANN., CTS. & JUD. PROC. 10-401 to 10-414 (Michie 1995). The court granted summary judgment, agreeing with the Hospital. Employers also have successfully pursued state statutory claims against employees who record conversations at work without the consent of all parties.

[12] Citicorp's massive private computer network spans 90 countries and is used by its employees to process over $3 trillion a day in transactions. *AT&T Wins Contract to Run Citicorp's Global Data Network*, WALL ST. J., March 10, 1998 at B8.

[13] Another troubling aspect concerning the use of digital technology in the workplace involves the growing use of digital technologies by employees that enhance employee performance, but are devices owned by the employee. While employers may favor the use of electronic devices such as Personal Digital Assistants (PDAs) and other handheld devices that enable employees to maintain organized schedules and increase their accessibility when they are on travel assignments, most workers who use their own electronic devices maintain personal as well as business related information on these devices. The curious problem this poses is whether an employer may permissibly "sneek-a-peek" at the data on these devices when they are connected to the employer's computer network? *See, e.g.*, Michael Schrage, *IS Troubles: of graying hair...and grayer areas,* COMPUTERWORLD, March 23, 1998 at 37 (arguing that electronic devices like the PalmPilot, which is popular among techno-oriented employees, require periodic connections to a PC and, thereby, may give the employer an unfair opportunity to read personal employee data).

[14] "Surveillance Technology" covers a vast range of products and devices but the overall trend is towards miniaturization, more precise resolution through the adoption of digital technology and increasing automation so that the technology can be more effectively targeted. Today, it is possible to quickly build up a comprehensive picture of virtually anyone by gaining electronic access to their records. For instance, automatic fingerprint readers are now common place in many companies. There is also a plethora of devices, many pre-packaged to fit into phones, look like cigarette packets or light fittings and some, like the ever popular PK 805 and PK 250, that can be tuned into from a suitable radio. For example, the multi-room monitoring system of Lorraine Electronics called DIAL (Direct Intelligent Access Listening) allows an operator to monitor several rooms from anywhere in the world without effecting an illegal entry. Up to four concealed microphones are connected to the subscribers line and these can be remotely activated by simply making a coded telephone call to the target building. Neural network bugs go one step further. Built like a small cockroach, as soon as the lights go out they can crawl to the best location for surveillance. In fact, Japanese researchers have taken this idea one step further, controlling and manipulating real cockroaches by implanting microprocessors and electrodes in

their bodies. The insects can be fitted with micro cameras and sensors to reach the places other bugs cannot reach. Millimeter Wave Imaging developed by the US Millitech corporation can scan people from up to 12 feet away and see through clothing to detect concealed items such as weapons, packages or other items. Variations of this through-clothing human screening (used by companies such as the US Raytheon Co.), include systems which illuminate an individual with a low-intensity electromagnetic pulse. A three side very-low X ray system for human useage, in fixed sites such as prisons, is being developed by Nicolet Imaging Systems of San Diego. Electronic monitoring of offenders or 'tagging', where the subject wears an electronic bracelet which can detect if they have relocated from their home after Satellite tracking is now facilitated by the once military Global-Positioning System(GPS), which is now available for commercial uses. *See,* STATEWATCH, October, 1996, pp. 6-7.

[15] In *Coulter v. Bank of American National Trust & Savings Ass'n,* 33 Cal. Rptr. 2d 766 (Cal. Ct. App. 1994), a California appellate court held that an employee violated California law by secretly taping meetings with the employer without the employer's consent, when the employer "expected the conversations to be private." *Id.* at 771. In so ruling, the court affirmed an award of over $130,000 against the employee. Although the employers in these two cases seem to have relied upon state laws as a basis for worker discharge and discipline, the existence of a relevant state law is not necessarily critical in a jurisdiction that follows an at-will employment doctrine. In an at-will jurisdiction, assuming no other cause-of-action was relevant, employees could be discharged for the same conduct complained of by the employers in the California and Maryland cases, despite the absence of similar laws. *See,e.g.*, Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications, supra,* (in an at-will jurisdiction, the employment relationship exists at the will of both parties, and either is free to terminate the relationship at any time).

[16] As developed more fully *infra*, there is no doubt that employer monitoring can constitute tortious invasion of privacy; especially where the employer does not notify employees of the monitoring activity or obtain their prior consent. If the monitoring activity is also aimed at the employees' personal or private affairs, then the likelihood increases that the monitoring will be tortious.

[17] *See, e.g.,* note 31, *infra.*

[18] The modern workplace may have all sorts of "insiders." Employers now frequently hire freelancers, contingent employees, consultants, part-timers, and independent contractors in addition to full-time hourly and salaried employees. *See, e.g.,* COMPUTERWORLD, MARCH 23, 1998 at 37.

[19] Digital surveillance technology can be defined as devices or systems which can monitor, track and assess the movements of individuals, their property and other assets through the use of a microprocessor or computer chip. Up until the recent dominance of computers for surveillance uses, most surveillance was actually very low-tech and expensive. The trend toward the use of digital technology for surveillance efforts was fueled in the 1990's by accelerated Federal government funding, at the end of the cold war, of intelligence agencies and the sharing of electronic surveillance technology between these agencies and the private sector. To counteract reductions in military contracts which began in the 1980's, computer and electronics companies expanded into new markets - in the U.S. and abroad - with equipment originally developed for the military. Companies such as E Systems, Electronic Data Systems (founded by Ross Perot) and Texas Instruments started selling advanced computer systems and surveillance equipment to private sector employers. A huge range of surveillance technologies has evolved, including microphones to detect conversations over a mile away; laser versions marketed by the German company PK Electronic, can pick up any conversation from a closed window in line of sight; the Danish Jai stroboscopic camera which can take hundreds of pictures in a matter of seconds and individually photograph all the participants in a crowd; and the automatic vehicle recognition systems, which, after identifying a car license plate number, can track the car for miles using a computerized

geographic information system from one work station. The GUARDIAN, May 3, 1995 at 10-11.

[20] In *O'Connor v. Ortega*, 480 U.S. 709, 722-24 (1987), the United States Supreme Court agreed with the government that employers may have legitimate, work-related reasons to intrude upon a public sector employee's right of privacy. The Court seemed convinced that in some exigent circumstances employers must be given wide latitude when the invasion is work-related or pursuant to an investigation of work-related employee misconduct or possible criminal behavior. *Id.* at 723-24.

[21] George Orwell, 1984, (Signet Classic ed., Penguin Books 1992) (1949) (Big Brother, Orwell warned us, is an entity, not unlike the modern employer, that in return for services may surreptitiously maintain watch over its subjects in order to control them. Was Orwell clairvoyant? It may be too early to determine. What seems obvious, however, is that the powerful technologies of digital surveillance are destined to be on the job right along with the American worker.)

[22] *See, e.g.,* Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications*, 2 VA. J. L. & TECH 4 (1997) (describing electronic monitoring by employers as generally referring to the practice of employer recording, reading, or listening to telephone or computer communications sent to employees by others.) In a few specific contexts, the law governing electronic communications establishes a narrow technical definition of electronic monitoring. *Id.*

[23] Pamela Burdman, *Employee Privacy in Peril in the High-Tech '90s,* SAN. FRANCISCO. CHRONICLE., Aug. 11, 1992, at B1; Veronica Fowler, Is the Boss Watching You While You Work?, GANNETT NEWS SERV., Nov. 12, 1992; Carol Kleiman, Worker Privacy Right Puts Businesses to Test, CHICAGO TRIBUNE., July 23, 1989, Jobs section at 1; Ronald Rosenberg, Most Workers in Survey Think Employers Use Electronic Means to Spy on Them, BOSTON GLOBE, Mar. 9, 1989, at 10; Jeffrey Rothfelder et al., Is Your Boss Spying on You? High-Tech Snooping in 'the Electronic Sweatshop,' BUSINESS WEEK, Jan. 15, 1990, at 74.

[24] Employees may be far beyond future shock. The presence of some forms of surveillance in the worklace has become so common or expected that there seems to be a contemporary lack of outrage on the part of many workers when they actually discover the existence of monitoring devices; this is particularly true of video monitors (*future shock* is an obvious reference to the title of Alvin Toffler's 1970 book, Future Shock, a phrase Toffler used to describe how people were becoming overwhelmed by the future. This concept seems particularly appropriate as a notion to describe the state of mind of an individual who has been so overwhelmed by the presence of technology that he slowly, but paradoxically, becomes underwhelmed or beyond future shock).

[25] *See ACLU Study Estimates More than 20 Million Workers Have E-Mail, Computer Files Searched by Bosses,* West Legal News, Sept. 12, 1996 (1996 WL 513566); see also Jerry Mahoney, Watchful Workplace; Employee Monitoring Has New Dimensions and Old Concerns, Austin American.-Statesman, Sept. 8, 1996, at H1 (estimating that 25 million employees -- nearly one quarter of the entire workforce -- are subject to electronic monitoring).

[26] Planting illegal bugs to intercept cellular telephone conversations is yesterday's technology. Modern snoopers can use desktop or laptop computers running the appropriate software and simply tune in to all the mobile cellular phones active in the area by dragging a cursor down the computer screen and highlighting a particular number. Some communications systems even lend themselves to a dual role as a communications tool and an interceptions network. For example the message switching system used on digital exchanges that support an Integrated Services Digital Network (ISDN) Protocol. ISDN allows

digital devices to share the system with existing lines. Many employers use ISDN lines to connect to the Internet because the digital connection provided by ISDN is faster and more efficient than typical analog telephone line connections. Built in to the ISDN protocol is the ability to take phones 'off hook' and listen into conversations occurring near the phone, without the user being aware that it is happening. This effectively means that a national dial up telephone tapping capacity is built into these systems from the start. Interestingly enough, cellular phone technology has a similar disadvantage. The technology required to pinpoint mobile cellular telephone users for incoming calls, means that cellular mobile telephones are essentially mini-tracking devices, giving their owners/users whereabouts at any time and stored in the cellular telephone service company's computer - - which employers may have access to if the cellular telephone is used for business reasons - - for up to two years. *See, Coupled With System X Technology, This Is A Custom Built Mobile Track, Tail And Tap System Par Excellence,* SUNDAY TELEGRAPH, February 2, 1997 at 1.

[27] For example, the nation's largest public sector employer, the Federal government, has a vast information infrastructure that includes 2.1 million computers, 10,000 local networks, and 100 long-distance networks. In addition, the Federal government uses the Internet to exchange electronic mail, log on to remote computer sites, and obtain files from remote locations. Like the nation as a whole, the Federal government is becoming increasingly dependent on widely interconnected computer systems and the electronic data they maintain. These systems have become essential to carry out critical operations, such as tax collections; asset protection, such as military equipment and accounts receivable; and delivery of basic services, such as social security payments and other benefits.

[28] Of course, the Internet, itself, creates significant privacy concerns unrelated to the protection of employer information infrastructure. These concerns are significant and garner substantial media attention, but are outside the scope of this paper. *See, e.g., Exposed: Computer technology, managed health care, and genetic science are all undermining the American tradition of medical privacy,* WASHINGTON POST, February 8, 1998, (http://www.washingtonpost.com/wp-Sunday/longterm/exposed/exposed1.htm/) (noting that Internet sites offering information about certain diseases have solicited data from cyber-visitors and then sold that information to companies marketing drugs or therapies).

[29] Digital technology can be used to efficiently express vastly different forms of information - such as factual databases, audio recordings, or electronic mail messages - on a desktop computer or across the Internet using bits of data in the form of computer 0s and 1s. Bits (or binary digits) are essentially the smallest and most fundamental units of digital technology data; each bit has a value of 0 or 1. The bits 0 and 1 represent off and on switches, which measure the presence or absence of electrical voltage in any given memory register of the computer. Since binary digits enable fairly easy digital expression and digital technology significantly expands the amount of data that can be processed on a single silicon chip, digital format has become the format of choice in electronics. *See,* Rod Dixon, *Profits in Cyberspace: Should Newspaper and Magazine Publishers Pay Freelance Writers for Digital Content? - - Tasini v. New York Times,* 4 MICH. TEL. & TECH. L. REV. 2 (1998).

[30] Richard Lacayo, *Nowhere to Hide: Using Computers, High-Tech Gadgets and Mountains of Data, an Army of Snoops Is Assaulting Our Privacy,* TIME, Nov. 11, 1991, at 34.

[31] This term broadly refers to an employer's computer systems, computer network, and most importantly, the Intellectual property and trade secrets of an employer.

[32] THE REPORT OF THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *Critical Foundations: Protecting America's Infrastructures,* (October 1997) (the Commission submitted its report to the President on October 20, 1997 pursuant to Exec. Order 13,010,

62 FED. REG. 37,347).

[33] GENERAL ACCOUNTING OFFICE, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (Chapter Report, 09/24/96, GAO/AIMD-96-110). The GAO study found that weak information security is a serious government-wide problem, with serious weaknesses reported for over two-thirds of the agencies reviewed. Commonly reported weaknesses included information access control problems and inadequate disaster planning. At half of the agencies reviewed, information security problems remained uncorrected for 5 years or more.

[34] To be sure, some computer systems connected to the Internet are highly subject to malicious attacks by outsiders, such as the much maligned hacker groups, which meet at malls or other public spaces to plan future website attacks. Estimates by the Department of Defense indicate that attacks on unclassified computer systems and networks are a serious and growing threat to our national security, including the Defense Department's ability to execute military operations and protect sensitive information. Defense Department data indicate that the agency may have experienced as many as 250,000 attacks in 1995 and that the number of attacks doubles each year. Successful attacks have shut down systems and corrupted sensitive data. Similarly, annual audits of the Internal Revenue Service (IRS) since 1993 have found that due to poor computer controls, the IRS cannot ensure that the confidentiality and accuracy of taxpayer data are protected and that the data are not manipulated for purposes of individual gain. Specifically, controls have not prevented users from unauthorized access to sensitive programs and data files. GAO REPORT at 47-50.

[35] Of course, information maintained on computer systems by employers is not limited to trade secrets or strategic business plans, but could include employee and customer information such as taxpayer data; purchasing records, commercial transactions; payroll data, personnel records, and health records.

[36] Indeed, as powerful as digital technology may be, it is often difficult to determine which technologies are best suited for monitoring the activities of people as well as machines. Employers frequently face a difficult task when it comes to monitoring their computer network simply for technological bugs and viruses. The Internet is frequently flooded with information about computer viruses, for example. This information can be found on obscure web sites or from postings on USENET newsgroups, but more often this kind of information spreads throughout the Internet in e-mail messages. Interspersed among genuine e-mail computer virus notices are computer virus hoaxes. These hoaxes report on viruses that do not infect information systems, but because users connected to the Internet do not have equal knowledge about technology, many hoaxes are not recognized as such, and have been very costly as unsophisticated employers try to quickly deploy anti-virus software on their computer networks to battle a virus that does not exist, while also taking resources away from detecting and destroying real computer viruses. This problem is often compounded by the fact that many employees often spread the false virus warning by forwarding the hoax e-mail message to several of their closest co-workers. In some instances, television and print news reports have unwittingly added authority to the hoax by mistakenly reporting it as a genuine computer virus scare.

One virus warning, called the "good times" virus warning, spread through out employer networks in April 1995 because employees had mistakenly taken the warning as serious and forwarded the virus warning to others by e-mail. Since many employer networks are connected to the Internet, this virus hoax was spread rapidly by unwitting employees through universities, government agencies, private sector companies, and was reported on network television news shows. Many computer users were apparently completely unaware that the e-mail message described a computer virus that could not exist. The message contained the following warning:

The FCC released a warning last Wednesday concerning a matter ofmajor importance to any regular

user of the InterNet. Apparently, a new computer virus has been engineered by a user of America Online that is unparalleled in its destructive capability. Other, more well-known viruses such as Stoned, Airwolf, and Michaelangelo pale in comparison to the prospects of this newest creation by a warped mentality.

What makes this virus so terrifying, said the FCC, is the fact that no program needs to be exchanged for a new computer to be infected. It can be spread through the existing e-mail systems of the InterNet. Once a computer is infected, one of several things can happen. If the computer contains a hard drive, that will most likely be destroyed. If the program is not stopped, the computer's processor will be placed in an nth-complexity infinite binary loop- which can severely damage the processor if left running that way too long. Unfortunately, most novice computer users will not realize what is happening until it is far too late.

Indeed, the problems that this virus hoax caused did occur because many computer users, including those that should have known better, did not realize the virus message warned of a virus that could not exist. Notably, some of the difficulty in managing computer networks in a manner that they are less vulnerable to harm or sabotage involves the rather simple need to clearly understand the obvious limitations of computer technologies so that unwarranted fears do not become the basis for organizational information technology policy. As comical as the Goodtimes hoax may seem to be, it represents a single example of the difficult task employers face when monitoring their computer networks.

[37] "Cyberspace," although once a concept of fiction, is now the fairly common term used to describe the location of activities that occur on computers linked to each other through networks using the Transmission Control Protocol and the Internet Protocol (TCP/IP) or, more simply stated, computers connected to the Internet. *See,* Rod Dixon, *Profits in Cyberspace: Should Newspaper and Magazine Publishers Pay Freelance Writers for Digital Content? - - Tasini v. New York Times, supra.* The most popular location of Cyberspace currently is the World-Wide-Web (the Web), which contains web sites (or home pages) that have information that may be viewed on a computer monitor by any computer properly connected to the Internet. *Id.*

[38] All major Federal agencies rely on computer systems to provide critical support for their operations, and even greater reliance is planned for the future. In addition, Federal agencies are increasing their use of interconnected systems and electronically transmitted data in order to streamline operations, make data more accessible, and reduce paperwork. For example, the Department of Defense has a vast information infrastructure that includes 2.1 million computers, 10,000 local networks, and 100 long-distance networks. The Defense Department also uses the Internet. The Customs Service relies on automated systems to process port-of-entry declarations, which totaled over 39 million in fiscal year 1994. GAO REPORT at 11-12.

[39] Other than to suggest that the Federal government uses polygraphs, background investigations, criminal histories, and financial records, the Commission did not elaborate extensively on what methods should be adopted to ensure that an employer's computer systems remain safe from employee sabotage. Nor did the Commission directly refer to technological uses of surveillance technology. These omissions, however, do not mean that the Commission would view the use of such as outside of the scope of its recommendations. To the contrary, the Commission's report contains a great deal of anecdotal evidence suggesting that employers adopt broad measures sufficiently secure to preclude harm to an organization's information infrastructure, and that the need to protect information infrastructure from employee sabotage should balance favorably against an employee's privacy interests. *See id.*

[40] *Cf. Schowengerdt v. United States*, 944 F.2d 483, 488 (9th Cir. 1991), *cert. denied,* 112 S. Ct. 1514

(1992) (stating that the "operational realities" of the employee's job precluded any objectively reasonable expectation of privacy and that the nature of employment justified the employer's constant surveillance of his activities); *Johnson v. Corporate Special Servs., Inc.*, 602 So. 2d 385, 388 (Ala. 1992) (filing a workers compensation claim eliminated any reasonable expectation of privacy and permitted investigation into the employee's physical condition).

[41] Although most instances of digital surveillance are not well documented - - since employers use surveillance technology surreptitiously - - there are many instances that have become well known. Alana Shoars, a former systems administrator at Epson America Inc., was discharged for insubordination when she complained that company supervisors were secretly monitoring the electronic mail messages of employees. Alyeska Pipeline Service Company, the employer of Charles Hamel, secretly recorded Hamel's telephone conversations at work and at home through the use of electronic listening devices unauthorized by AT & T when Hamel became an outspoken critic of the company. Micheal Barriere, formerly employed by Delco Systems Operations in Santa, Barbara, California, was dismissed by his employer when he reported that he had discovered that Delco was furtively wiretapping and intercepting voice mail and e-mail communications of employees. Rebecca Huls, the electronic surveillance monitor for USAA Insurance Corporation, was discharged by USAA when she began monitoring management telephone conversations as well as employee calls. *See* Robert Ellis Smith, WAR STORIES, vol. 1, 1993.

[42] *See, e.g.,* Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications, supra. (*demonstrating that the district court in Smyth v. Pillsbury, which held that private sector employees in Pennsylvania have no reasonable expectation of privacy in the content of their e-mail messages, relied upon a flawed analysis of privacy by assuming that the scope of the right of privacy is limited by notions of solitude). Although the Smyth holding was sweeping, it is doubtful that its application will be. Smyth so egregiously departed from current doctrine on the law of privacy that the decision may be validly distinguished and limited to its peculiar findings. *Id.*

[43] John W. Verity, *The Internet: How It Will Change the Way You Do Business,* BUSINESS WEEK, Nov. 14, 1994, at 82; *ACLU v. Reno*, 929 F.Supp. 824 (E.D. Pa..1996).

[44] *ACLU V. Reno,* 929 F.Supp. at 831. Interestingly, the genesis of the Internet can be traced back to a design made in 1964 by Paul Baran, a Rand Corporation researcher. This design consisted of a computer-communications network that had no hub, no central switching station, no governing authority, and that assumed that the links connecting any city to any other were totally unreliable. Building on Paul Baran's conceptual scheme, the ARPAnet was unveiled in 1969 by the United States Defense Department as a computerized communications system that was capable of surviving a nuclear attack. The ARPAnet, named after the Federal government's Advanced Research Projects Agency, helped scientists and researchers share limited computing resources. *See,* James T. Madore, *Internet Connects Small Businesses with the World,* BUFFALO NEWS, Oct. 24, 1994, at A13; John W. Verity, *The Internet: How It Will Change the Way You Do Business,* BUSINESS WEEK, Nov. 14, 1994, at 80, 82.

[45] *See generally, ACLU v. Reno*, 929 F.Supp. 824 (E.D. Pa. 1996) (findings of fact paragraphs 12 & 46).

[46] *Id.*

[47] *Id.*

[48] *Id.*

[49] The Internet is an open system. Once an employer connects its private computer network to the Internet, the TCP/IP protocols enable computer users anywhere in Cyberspace to obtain access to some parts of the private network since every node of a TCP/IP network becomes a door into or out of the employer's system. *See, The Firewall Diemma: Too Few locks, Too Many Doors, BYTE,* August 1996 at 72. In other words, the Internet is a window into a private network; that, in itself, may not be severely compromising of information security. However, there are more than enough computer users, who are not satisfied with just looking through the network window, they want to force the window open and crawl inside without authorization.

[50] *See generally, Intermatic Inc. v. Toeppen*, 947 F. Supp. 1227, 1230-32 (N.D. Ill. 1996).

[51] An example of such an address would be 123.456.101.1.

[52] At first blush, it may seem as if Internet users should assume they can be easily identified by their numeric IP address, and that this realization should lead to less bad faith, not more. However, most Internet users are unaware of the nature of the technology that enables them to access Cyberspace so the nature of the technology has little direct impact upon the behavior of most computer users. More to the point, those that do understand the technology are aware that most IP addresses are dynamic, not static. Each time most computer users log on to the Internet they are assigned a random IP address for that session until their computer disconnects from the Internet Access Provider. Consequently, the use of pseudonymous user names that may be changed frequently and easily along with the random assignment of numeric IP addresses would more likely increase an individual's inclination to act in bad faith rather than the contrary.

[53] Edward Cavazos and Gavino Morin, CYBERSPACE AND THE LAW: YOUR RIGHTS AND DUTIES IN THE ON-LINE WORLD, 2-11 (1994).

[54] Daniel P. Dern. THE INTERNET GUIDE FOR NEW USERS 16 (1994).

[55] Web pages are stored on web servers, which are computers that are set up to run Internet software. Web servers log every access. As such, each web page downloaded by an employee is logged on the remote server that contains the web site visited as well as the employer's proxy server, if the employer uses a firewall to protect its private network from unauthorized users on the Internet. In this respect, everything a computer user reads on the Internet is logged and stored while being read in at least one location and possibly several. Only those actively concealing their identity are ostensibly protected from Cyberspace's automated tracking schemes. Most of this tracking and recording happens automatically without the active intervention of humans since the very nature of the Internet's technologies creates records of all computer users activities.

[56] Daniel P. Dern, THE INTERNET GUIDE FOR NEW USERS 16 (1994).

[57] A link is an image or a short section of text referring to another document on the Web.

[58] *Panavision Int'l, L.P. v. Toeppen,* 945 F. Supp. 1296, 1299 (C.D. Cal. 1996).

[59] *Id.*

[60]http://www.cs.ucsb.edu/~andre/attack.html. Despite a few claims to the contrary, the software often

used to surf the Web, Web Browsers like Netscape Navigator, are notoriously insecure and bug-riddled. This is especially true when unsavvy computer users are given access to the Internet without prior training in safety techniques that could inform users how to spot suspicious websites or detect the presence of malicious code. *See,* e.g., A.L. Dos Santos et al., *Secure Browsers?*, Computer Science Department, University of California, .

[61] As noted *supra,* this term broadly refers to an employer's computer systems, computer network, and most importantly, the Intellectual property and trade secrets of an employer.

[62] *See* Daniel P. Dern, THE INTERNET GUIDE FOR NEW USERS 16 (1994).

[63] *See* Janet Zimmerman, *Exasperated Employees Belt Boss on Web Site*, THE DENVER POST, January 20, 1998, at p. G-01.

[64] What are employees doing online? One web site that is frequently visited during the work day is Claude Carter created the Web site and claims 100,000 people per week tap in to his page anonymously to share stories about their victimization by supervisors. There are anecdotes - like the guy who sold 68 cellular phones in two months for his company in hopes of winning an all-expenses-paid trip to a Mexican resort. His boss, who sold two phones, took the trip. *Id.* at G-02. With the power available through the Internet, a disgruntled employee could easily send his company's client list, personnel roster, or other sensitive data to a competitor in a matter of seconds. Even employers who do not connect desktop computers directly to the Internet, have substantial security concerns about their information infrastructure since with the simple use of a modem and telephone an employee can expose an entire private network to the risks of the Internet. *See id.* at G-02.

[65] *See* C. Johnson, *Firms Fight Out-Of-Line Online Use*, THE RECORDER, January 28, 1998, at 1.

[66] *See id.* at 2. Surprisingly, one law firm, Wilson, Sonsini, Goodrich & Rosati has gone on record as opting to forgo instituting a policy governing its workers' online behavior. According to Phillip Hoare, the firm's vice president, the firm discussed creating such a policy, but so far has declined to do so. Hoare stated that the firm has never faced a situation where such a policy was necessary and recalled that an outright ban on accessing questionable sites might have impaired the firm's ability to handle a recent case involving a sexually explicit Web site. In that instance, monitoring lawyers' activity might have turned up research mistaken for personal use according to Hoare. At any rate, in Hoare's view, absent an Internet policy, he doesn't know if the firm even has the right to watch over its employees' shoulders. *Id.*

[67] *See* Trip Gabriel, *New Issue at Work: On-line Sex Sites,* N.Y. TIMES, June 27, 1997 at C1.

[68] Compaq Computer dismissed twenty employees for logging more than 1,000 visits each on sexually explicit websites in contravention of company policy. *See,* Sally Greenberg, *Threats, Harassment, and Hate On-line: Recent Developments,* B.U. PUB. INT. L.J. 673, 677 (1997).

[69]http://www.pearlsw.com *See,* Pearl Software Website (visited March 1, 1998) .

[70] *See id.* at 4. There are several technological solutions - - in the form of software applications - - to lessen the difficulty of patrolling inappropriate use of the Internet by employees. However, no technological solution, not itself involving surveillance, has proven sufficient to alleviate the reliance on electronic surveillance. For example, "CYBER-sitter" is a software application designed to operate or run on the ubiquitous Windows 95 operating system. This software allows employers to block access to

adult and sexually oriented material on the Internet and other on-line services. Yet, for employers, the software's most useful feature appears to be the additional ability to monitor files, programs and directories on the employee's own computer hard disk. Working secretly in the background, the software is constantly watching all computer activity, including recording Web sites, news groups, chat lines, and FTP sites visited as well as monitoring all incoming and outgoing e-mail and file downloads. PR Newswire September 28, 1995 at 2.

[71] *See A former Girlfriend of Oracle's Ellison Convicted of Perjury*, WALL ST. J., Jan. 29, 1997, at B3.

[72] *See id.*

[73] In the end, Lee was sentenced to a year in jail and forced to pay back the $100,000. Telecom-worldwide, May 15, 1997, 1997 WL 10960890.

[74] *See, e.g.,* Anthony J. Dreyer, Note, *When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence,* 64 FORDHAM L. REV. 2285, 2288 (1996). Another interesting condition of e-mail is that e-mail seems to promote a certain type of candor or unguardedness. In this respect, e-mail messages might be more revealing of a person's inner feelings than a traditional paper document. As noted more fully below, an employer's monitoring of e-mail messages surreptitiously necessarily raises very serious questions regarding the invasion of employee privacy.

[75] In one notably case, Compaq Computer Corporation fired 20 employees at one time for allegedly distributing pornographic images downloaded from the Internet on the employer's computers. *See Employee Internet Use: Big Brother Gets Involved*, NEW YORK L. J., March 17, 1997.

[76] *See id.*

[77] *Owens v. Morgan Stanley,* 1997 WL 49354 (S.D.N.Y. 1997); *see also, Curtis v. Citibank,* No. 97-1064 (S.D.N.Y. 1997) (a pending class action case wherein the plaintiffs raise allegations that are substantially similar to those alleged in the Owen case.)

[78] American employers lost $250 billion to thefts of trade secrets in 1997. *See* Frances A. *McMorris Corporate Spy Case Rebounds on Bristol,* WALL STR. J., February 2, 1998 at B5.

[79] *See Id.*

[80] *See,* Marc S. Friedman and Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway,* CLA BULLETIN, Jan. 15, 1998 at 13.

[81] Appendix III, *Security of Federal Automated Information Resources.* Since 1985, this circular has directed agencies to implement an adequate level of security for all automated information systems that ensures (1) effective and accurate operations and (2) continuity of operations for systems that support critical agency functions. The circular establishes a minimum set of controls to be included in federal agency information system security programs and requires agencies to review system security at least every three years. (GAO/AIMD-96-84, May 22, 1996). Forty two federal organizations estimated that they provided Internet and e-mail access to about 1.7 million, or about 50 percent, of their civilian and military employees and Web access to about 1 million, or about 31 percent, of their employees. In the Federal sector, the Internet has become a valuable and widely used means of communicating and sharing

information. There are thousands of Federal government websites. Perhaps quite startling, there is no government-wide policy or regulation that specifically govern employee use of the Internet.

[82] The Computer System Security and Privacy Advisory Board was established by the Computer Security Act to identify emerging issues related to computer system security and privacy; to advise NIST on these issues; and to report its findings to OMB, the National Security Agency, the Secretary of Commerce, and appropriate committees of the Congress. It is composed of both federal and private sector representatives. *Id.*

[83] OMB, NIST, and agency responsibilities regarding information security were recently reemphasized in the Information Technology Management Reform Act of 1996. (GAO/AIMD-96-84, May 22, 1996).

[84] *Id.*

[85] An "attack" is an attempt to gain unauthorized access to a computer system with malicious intent. Most attacks of computer systems from those on the outside involve brute-force attempts to compromise a private network's security by overwhelming the computer system in a manner that could lead to a system failure. Some brute-force attacks are aided by the assistance of an employee on the inside who may not have authorized access to the computers that are the focus of attack, but may provide the unauthorized intruders with information about the private network that could enable the intruders wage an assault on the other computers on the private network.

[86] Steven M. Bellovin. *Using the Domain Name System for System Break-ins.* Proceedings of Fifth Usenix UNIX Security Symposium, June 1995.

[87] Air tasking orders are the messages military commanders send during wartime to pilots; the orders provide information on air battle tactics, such as where the enemy is located and what targets are to be attacked. The intruders also launched other attacks from the lab's computer systems, gaining access to systems at NASA's Goddard Space Flight Center, Wright-Patterson Air Force Base, and Defense contractors around the country. (GAO/T-IMTEC-92-5, November 20, 1991).

[88] Computer Security: Hackers Penetrate DOD Computer Systems (GAO/T-IMTEC-92-5, November 20, 1991).

[89] Indeed, countries today do not have to be military superpowers with large standing armies, fleets of battleships, or squadrons of fighters to gain a competitive edge. Instead, and, perhaps most troubling of all, is that all they really need to steal sensitive data or shut down military computers is a $2,000 computer and modem and a connection to the Internet.

[90] As noted *infra,* malicious programming code is often referred to as software bombs, trojan horses, and computer viruses. Whatever its nomenclature, malicious code is inserted on a computer network to surreptitiously wreak bothersome or, oftentimes, serious harm to the computer network it travels on.

[91] *See id.*

[92] There are many instances of electronic surveillance that have recently become well known. Alyeska Pipeline Service Company, the employer of Charles Hamel, secretly recorded Hamel's telephone conversations at work and at home through the use of electronic listening devices unauthorized by AT & T when Hamel became an outspoken critic of the company. Micheal Barriere, formerly employed by

Delco Systems Operations in Santa, Barbara, California, was dismissed by his employer when he reported that he had discovered that Delco was furtively wiretapping and intercepting voice mail and e-mail communications of employees. Alana Shoars, a former systems administrator at Epson America Inc., was discharged for insubordination when she complained that company supervisors were secretly monitoring the electronic mail messages of employees. Rebecca Huls, the electronic surveillance monitor for USAA Insurance Corporation, was discharged by USAA when she began monitoring management telephone conversations as well as employee calls. *See,* Robert Ellis Smith, WAR STORIES, vol. 1, 1993.

[93] U.S. NEWSWIRE, CWA, *Northern Telecom Settle Suit on Secret Electronic Surveillance,* February 27, 1992 at 2-3. The concept of privacy as a legal interest deserving an independent remedy was actually first enunciated in an article co-authored by Samuel Warren and Louis Brandeis in 1890, *supra,* which describes privacy as "the right to be let alone."

[94] While Borland Corporation was surreptitiously using electronic surveillance to monitor its employees' e-mail messages it discovered that one of its high level software executives, who had announced an imminent departure from the company, was sending e-mail messages that contained corporate trade secrets to his future boss, Gordon Banks, the president of Symantec Corporation. Borland reported its discovery to law enforcement officials who charged the employee, Eugene Wang, and Banks with theft of trade secrets under California state law. *See,* Marc S. Friedman and Kristin Bissinger, *Infojacking: Crimes on the Information Superhighway,* CLA BULLETIN, Jan. 15, 1998 at 13.

[95] A sniffer program is a software communications application that runs on a network and records or steals IP addresses from digital data packets that are transmitted throughout the Internet when computers send messages back-and-forth to web servers, which are the powerful computers that store webpages. Not surprisingly, as the Labor Department's use of sniffer programs illustrate, these programs can be used for legitimate and illegitimate purposes.

[96] Every computer that accesses the Internet must use the Internet Protocol (IP) to do so. Internet Protocol is a communications language computers use to "talk" to each other. When connecting to the Internet, the Internet Protocol uses an IP address (or identifying number) assigned to the computer requesting access. This number may be dynamic or static upon each new connection to the Internet, but regardless of whether the number changes or remains the same, for each connection the IP number can be used to determine which computer is connected to the Internet. Not only does every computer leave a trail of its IP address everywhere it goes on the Internet, but sniffer programs, savvy computer users, untrustworthy computer hackers, website owners, and just about any employer can, with little difficulty, surreptitiously grab a computer's IP address; surprisingly, most Internet users are unaware of this. Oftentimes, if a computer is assigned a static IP address - - most large organizations use static IP addresses whereas most consumers are assigned dynamic IP - - the identity of the computer user can be determined by anyone with access to the Internet and to the protocol called Finger, which is an obscure, but powerful, database that identifies millions of computer users by IP address, e-mail address and occasionally workplace and phone number. You can Finger someone by simply entering a name, e-mail address or IP address when running the Finger protocol. *See generally,* MDA COMPUTING GLOSSARY, (visited February 18, 1998) ,http://www.mediawest.com/ver2/def/mwstdf23.html; *Internet Address-Rerouting Incident Raises Concern over Control of System,* Wall Str. J., Feb. 5, 1998 at B6 (noting that the ultimate authority on the Internet addressing system currently is held by the Internet Assigned Numbers Authority (IANA) at the University of California under contract from the Department of Defense).

[97] This data is gathered in log files to detect which computer users are repeatedly requesting access to the secure parts of the website. This enables the agency to trace visitors who attempt to attack the

website. *See* GOVERNMENT COMPUTER NEWS, February 9, 1998, at 12.

[98] According to more than just a few media sources, computer users access the Internet under the illusion of privacy because they do not consider their computers virtual peepholes in Cyberspace. Indeed, many computer users are often stunned to discover the type of information and the quantity of information that many website owners record from Internet users without their permission. *See Don't Expect Your Secrets to get Kept on the Internet,* WALL ST J., Feb. 6, 1998 at B5.

[99] *Hector Vega-Rodriguez v. Puerto Rico Telephone Co.,* 110 F.3d 174 (1st Cir. 1997). A few cases have even improperly stated in dicta that employees have no right of privacy. *See, e.g., Delury v. Kretchover,* 66 Misc. 2d 897, 322 N.Y.S. 2d 517 (Sup. Ct. N.Y. Co. 1971); FMC Corp., 46 Lab. Arb. 335 (1966) (closed circuit cameras); *Rogers v. McKoy,* 1997 U.S. Dist. Lexis 132 (S.D.N.Y., January 6, 1997) (papers in wastebasket).

[100] *People v. Palmer,* 888 P.2d 348 (Colo. App. 1994); Colo. Const. art. II, § 7; *see also Katz v. United States,* 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967); Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510, et seq. (1988).

[101] To be sure, there is no such thing as a systematic conception of law called "privacy law." The doctrinal basis to the law of privacy is amorphous and unyielding to simple analysis. Nonetheless, the right of privacy emanates from a cohesive framework requiring courts to balance similar equities regardless of whether the cause-of-action is based on tort, contract, or constitutional principles; even statutory privacy protections often are developed in reference to the established framework undergirding the right of privacy.

[102] Although the right of privacy is usually viewed as an exception to the doctrine of at-will employment for private sector employees seeking protection under tort, the fact that courts have had difficulty in applying the right of privacy to appropriate cases may demonstrate the existence of two well-established common law doctrines coming into conflict. The right of privacy protects employees from unreasonable intrusions on their privacy while in the workplace. The doctrine of at-will employment authorizes an employer to discharge its employees at his will, unless a clear agreement exists to the contrary. *Cf. Jennings v. Minco Tech. Labs, Inc.,* 765 S.W.2d 497, 499-502 (Tex. Ct. App. 1989) (rejecting plaintiff's claim of wrongful discharge based on invasion of common law right of privacy) with *Twigg v. Hercules Corp.*, 406 S.E.2d 52, 55 (W. Va. 1991) (recognizing right of privacy as public-policy limitation on at-will rule) and *Luedtke v. Nabors Ala. Drilling, Inc.*, 768 P.2d 1123, 1130 (Alaska 1989) (concluding that violation of public policy protecting employee privacy may breach covenant of good faith and fair dealing implied in at-will employment contract).*Cf. Luck v. Southern Pac. Transp. Co.,* 267 Cal. Rptr. 618, 634-35 (Cal. Ct. App. 1990) (California constitutional right to privacy is not public-policy exception to at-will rule).

[103] A number of Federal statutes have presumptively taken employers out of the at-will employment relationship by forbidding the discharge of employees for certain enumerated reasons. Title VII of the Civil Rights Act of 1964, 42 U.S.C. sections 2000e to 2000e17 (1994), forbids discharge because of an employee's race, color, religion, sex, or national origin, and the Age Discrimination in Employment Act (ADEA), 29 U.S.C. sections 621-634 (1994), and the Americans with Disabilities Act, 42 U.S.C. sections 12101-12213 (1994), similarly limit discriminatory discharges based on age or disability. Other federal laws prohibit employers from dismissing employees for asserting certain statutory rights. *See, e.g.,* National Labor Relations Act, 29 U.S.C. section 158 (1994) (stating that discrimination against or discharge of employee for exercising rights under the NLRA is an "unfair labor practice"); Fair Labor Standards Act, 29 U.S.C. section 215(a)(3) (1994) (stating that it is unlawful to discharge an employee for filing a complaint under the FLSA); Occupational Safety and Health Act, 29 U.S.C. section 660(c)

(1994) (forbidding the discharge of employee for filing complaint pursuant to OSHA); Employee Retirement Income Security Act, 29 U.S.C. section 1140 (1994) (forbidding the discharge of an employee for exercising ERISA rights); and Family and Medical Leave Act, 29 U.S.C. section 2615(a) (1994) (prohibiting discharge of any individual for opposing any practice made unlawful by FMLA).

[104] There are also many state and local laws limiting an employer's right to terminate an employee at-will. Indeed, in light of the extensive statutory protections (on both the Federal and state level) and common law protections now available to private sector employees, it would not be foolish to challenge the notion that the at-will employment relationship has retained its vitality and remains the predominate employment relationship. Undoubtedly, the majority of American workers may find that, at the very least, they are protected from unlawful age discrimination - should the worker remain in the workforce until the age of 40. *See, e.g.,* 29 U.S.C. § 621 (ostensibly, ADEA protects workers 40 years old and older).

[105] The Privacy Act of 1974 provides legal protection for and safeguards on the use of personally identifiable information maintained in federal government record systems. The purpose of the Privacy Act of 1974 is to protect the personal privacy of individuals through the regulation of the government's use, exchange, and dissemination of records concerning the individuals on which it maintains records. In general, the records cannot be released unless the individual on which the record is maintained requests or consents to the disclosure of the information. Although the Privacy Act limits the government's use of an individual's records, it does nothing to discourage the use of the same information by private entities. Once the information departs government control, it cannot be protected by the Privacy Act. Privacy Act of 1974, Pub. L. No. 74-579, 88 Stat. 1896 (1974), (5 U.S.C. § 552a(b) (1988)). In a different context in *United States v. Miller,* the Court rejected the claim that an individual had a Fourth Amendment reasonable expectation of privacy in the records kept by banks because checks are merely copies of personal records that were made available to banks for a limited purpose. The *Miller* court ruled that checks are not confidential communications but negotiable instruments to be used in commercial transactions. In response to the wide hole in informational privacy left bare by *Miller*, Congress enacted the Financial Privacy Act of 1978 (Public Law 95-630), 12 U.S.C. §§ 3401-3422 (1988 & Supp. II 1990), which had the effect of repudiating *Miller.*

[106] *See Whalen v. Roe*, 429 U.S. 589, 599 n. 23, 51 L. Ed. 2d 64, 97 S. Ct. 869 (1977). "Courts have found that those with personal information in the control of the state retain constitutional protection against its inappropriate disclosure." *Scheetz v. Morning Call, Inc.,* 747 F. Supp. 1515, 1521 (E.D. Pa. 1990) (citations omitted), *aff'd,* 946 F.2d 202 (3d Cir. 1991). The Fourth Amendment is not a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further and often have nothing to do with privacy at all. Other provisions of the constitution protect personal privacy form other forms of government invasion. For example, the Fifth Amendment protection against self-incrimination involves a right to privacy against unreasonable surveillance by the government or compulsory disclosure to the government.

[107] *Fraternal Order of Police, Lodge No. 5 v. City of Philadelphia*, 812 F.2d 105, 110 (3d Cir. 1987).

[108] 381 U.S. 479 (1965).

[109] *See Young v. Jackson,* 572 So. 2d 378, 381 (Miss. 1990) (noting that other people may not invade the privacy zone without the person's consent).

[110] *Id.* at 484-86. A penumbra is a body of rights guaranteed by implication in a civil constitution. Merriam Webster's Collegiate Dictionary 860 (10th ed. 1994). Penumbra is an umbrella term that

encompasses a broad range of rights that are explicit and implicit in the Constitution. Justice Holmes first spoke of penumbras in relation to privacy in *Olmstead v. United States*, 277 U.S. 438, 469 (1928) (Holmes, J., dissenting). But the original use of the term was by Justice Field in *Montgomery v. Bevans,* 17 F. Cas. 628 (C.C.D. Cal. 1871) (No. 9735). For a detailed history of penumbra, see Henry T. Greely, A Footnote to "Penumbra" in *Griswold v. Connecticut*, 6 CONST. COMMENTARY 251 (1989). Before *Griswold*, the protection of privacy was viewed simply as essential to the protection of other more well-established rights. In *Griswold*, the Court struck down a Connecticut statute that prohibited the prescription or use of contraceptives and viewed the case as concerning "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees," that is, the First, Third, Fourth, Fifth and Ninth Amendments, each of which creates "zones" or "penumbras" of privacy. The majority supported the notion of an independent right of privacy inherent in the marriage relationship. *Id.*

[111] *Id.* Following the logic of *Griswold,* the Court, in *Eisenstadt v. Baird*, 405 U.S. 438 (1972), extended the right to privacy beyond the marriage relationship to lodge the right more personally in the individual, according to the court, if the right of the *individual* means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to give birth.

[112] 410 U.S. 113 (1973).

[113] As noted *supra,*, one important area of privacy involves informational privacy, which could include the protection of medical or health records, social security numbers, or records on consumer purchases. George B. Trubow, *Protecting Informational Privacy in the Information Society,* 10 N. Ill. U. L. Rev. 521, 532 (1989). Notably, although some courts often confuse or conflate the distinct aspects of privacy, some forms of informational privacy actually concern matters of confidentiality and, are therefore, analytically distinct from the right of privacy. *See, e.g., Norman-Bloodsaw v. Lawrence Berkeley Laboratory,* 1998 WL 39209 (9th Cir. 1998) (holding that the constitutional right of privacy encompasses the right to avoid disclosing personal medical information in order to protect confidentiality). For example, credit reports are protected by Federal law from being used for inappropriate uses; namely, credit reports are considered confidential and may be kept secret from those who do not have authorized access. Personal autonomy and human dignity are rarely invoked as principles underlying the protection of credit reports. From this perspective, informational privacy is largely the province of secrecy wherein confidentiality is protected through intentional concealment. However, under the general right of privacy, conceptually, human dignity and personal autonomy in decision making is protected through superimposed barriers (e.g., the home) or delineated lines (e.g., abortion decisions) of unwanted access.

[114] *Roe,* 410 U.S. 154.

[115] 505 U.S. 833 (1992).

[116] There is also an aspect of informational privacy wherein human dignity and personal autonomy is protected through confidential privilege. The privilege against self-incrimination is one example; the right to bodily integrity is another (precluding certain drug tests under the Fourth Amendment, for example). The right to conceal one's own thoughts - - even if those thoughts are recorded on paper or electronically on computer - - is, similarly, an aspect of personal autonomy protected through confidential privilege as well as superimposed barriers (encrypted electronic mail messages clearly demonstrate both a subjective and an objective expectation of privacy by superimposing a powerful technological barrier between the author of the electronic message and everyone else...except the intended recipient).

[117] In the context of the workplace, the notion that the scope of an employee's right of privacy, regardless of the source of the right, is limited by the employee's reasonable expectation of privacy is accepted as a threshold principle. *See, e.g.,* Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications, supra.* The Fourth Amendment protects individuals from unreasonable searches conducted by the government, even when the government acts as an employer. *See National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665, 103 L. Ed. 2d 685, 109 S. Ct. 1384 (1989). In order to make out a claim for damages for a Fourth Amendment violation by a government employer, plaintiffs must show as a threshold matter that a governmental "search" has occurred. The watchful eye of a government employer becomes engaged in a search only when the inquiry intrudes upon an area where the employee has a reasonable expectation of privacy. *See O'Connor v. Ortega,* 480 U.S. 709, 715, 94 L. Ed. 2d 714, 107 S. Ct. 1492 (1987); *Coppinger v. Metro-North Commuter R.R.*, 861 F.2d 33, 35 (2d Cir. 1988).

[118] *See, e.g., Young v. Jackson,* 572 So. 2d 378 (Miss. 1990) (employee alleges public disclosure of private facts); *Diamond Shamrock Refining v. Mendez,* 809 S.W.2d 514 (Tex. Ct. App. 1991) (employee alleges false light tort), *aff'd in part, rev'd in part*, 844 S.W.2d 198 (Tex. 1992); *Staruski v. Continental Tel. Co.*, 581 A.2d 266 (Vt. 1990) (employee claim based on appropriation of name and likeness). Because qualified privilege is generally recognized as an affirmative defense to the publicity and false light torts, the employment context may be relevant in evaluating a defendant employer's claim that its communications were privileged.

[119] *People v. Oates*, 698 P.2d 811 (Colo. 1985); *cf. O'Connor v. Ortega*, 480 U.S. 709, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (1987) (reasonable expectation must be addressed on a case-by-case basis weighing the general practical societal expectations of privacy in the workplace against the practical realities of the particular workplace); *Cf. People v. Hillman,* 834 P.2d 1271 (Colo. 1992) (no invasion of privacy in observation of that which is plainly visible to the public) and *United States v. Rose*, 669 F.2d 23 (1st Cir. 1982), *cert. denied*, 459 U.S. 828, 103 S. Ct. 63, 74 L. Ed. 2d 65 (1982) (no reasonable expectation of privacy in communication transmitted by ham radio) with *People v. Sporleder*, 666 P.2d 135 (Colo. 1983) (telephone subscriber has reasonable expectation of privacy in records of telephone numbers dialed).

[120] Traditionally, in the Fourth Amendment context the reasonableness of a search is evaluated with reference to the concept of probable cause and the presumption that a warrant is a prerequisite. *Von Raab*, 489 U.S. at 665; *see generally California v. Acevedo,* 500 U.S. 565, 111 S. Ct. 1982, 1992-94, 114 L. Ed. 2d 619 (1991) (Scalia, J. concurring). However, the reasonableness of a search by the government as employer is not as rigidly circumscribed by probable cause requirements as in the context of law enforcement. *Von Raab*, 489 U.S. at 667-68; O'Connor, 480 U.S. at 722-23. Rather, where the intrusion serves "special governmental needs beyond the normal need for law enforcement," *Von Raab,* 489 U.S. at 665-66, as in the case of governmental work-related intrusions, the reasonableness of the intrusion is determined by balancing the "nature and quality of the intrusion against the importance of the governmental interests alleged to justify the intrusion." *O'Connor,* 480 U.S. at 719.

[121] *See Angel v. Williams*, 12 F.3d 786, 790 (8th Cir. 1993); *see also People v. Juarez,* 770 P.2d 1286, 1289 (Colo. 1989); *United States v. Monie,* 907 F.2d 793 (8th Cir. 1990); *United States v. Carroll*, 337 F. Supp. 1260, 1264 (D. D.C. 1971) (objective reasonableness decided as a matter of law on motion to dismiss).

[122] http://www.aclu.org/library/pbr2.html Only the state of Connecticut has enacted a statutory ban on the use of electronic monitoring devices by employers in areas of the workplace designated for the health or personal comfort of employees. *See Privacy in America: Electronic Monitoring, American Civil Liberties Union*, (visited January 27, 1998) .

[123] *See People v. Triggs*, 8 Cal. 3d 884, 506 P.2d 232, 106 Cal. Rptr. 408 (Cal. 1973) (method of observation rather than physical features of public restroom critical to evaluation of search); *see generally* W. LaFave, 1Search & Seizure § 2.4(c) (3d ed. 1996).

[124] Courts have generally refused to acknowledge a reasonable expectation of privacy for conversations which take place in prisons, even for those who work there. *See Lanza v. New York,* 370 U.S. 139, 143-44 (1962)(conversation between inmate and brother in prison "visitors' room" intercepted by police); *Angel v. Williams,*12 F.3d 786, 790 (8th Cir. 1993) (police officer taped speaking to prisoner in jail); *Commonwealth of Pennsylvania v. Henlen,* 522 Pa. 514, 564 A.2d 905, 907 (Pa. 1989) (investigating police officer taped by suspect during interrogation). These decisions rely in part on the fact that the prison's very nature and purpose give notice to individuals that their privacy is diminished.

[125] 467 F.2d 1107 (9th Cir. 1972), *cert. denied*, 410 U.S. 916 (1973) (no reasonable expectation of privacy in prison).

[126] *Cf. People v. Hart, supra; Lee v. Florida,* 392 U.S. 378 (1968) (constitutional protections from search and seizure can attach without circumstances justifying perfect privacy); *Sporleder, supra*, n. 118 at 141 ("privacy is not a discrete commodity, possessed absolutely or not at all.").

[127] The inquiry as to the existence of a reasonable expectation of privacy asks whether a person has exhibited an actual expectation of privacy and whether society is prepared to recognize that expectation as legitimate. As previously discussed, the latter is a legal determination, resting solely within the province of the court. *See* W. LaFave, 1 Search & Seizure, § 2.1(d) at 391 (3d ed. 1996) ("The criteria for reasonable expectations must be abstracted from the flow of life, and it is the judge's task to find and articulate those societal standards.").

[128] *See Katz v. United States, supra,* 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[129] *See People v. Oates, supra* (crucial factor that grants a legitimate expectation of privacy is the right to exclude unwanted parties; government constitutionally constrained from adding to natural risks); *United States v. Carroll, supra* (purely objective determination that there was no reasonable expectation is only possible when conversation is overheard unaided and recorded with no contrivance and no augmentation).

[130] "It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence." *See United States v. Karo*, 468 U.S. 705, 712 (1984); *see also Broadway v. City of Montgomery*, 530 F.2d 657, 660 (5th Cir. 1976). If a mere showing that a person's comments were capable of being intercepted was adequate to state a privacy claim in this age of powerful digital surveillance technology, virtually every comment could lead to a complaint. *See Wesley v. WISN Division-Hearst Corp.*, 806 F. Supp. 812, 815 (E.D. Wis. 1992).

[131] Government searches to retrieve work-related materials or to investigate violations of workplace rules -- searches of the sort that are regarded as reasonable and normal in the private-employer context -- do not violate the Fourth Amendment. *O'Connor v. Ortega*, 480 U.S. 709, 732 (1987)(J. Scalia, concurring); *see, e.g., United States v. Taketa*, 923 F.2d 665, 673-74 (9th Cir. 1991); *United States v. Nasser,* 476 F.2d 1111, 1123 (7th Cir. 1973). However, even if the intrusion is work-related, individualized suspicion may be required, depending on the nature and quality of the intrusion. *See*

Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 624, 628, 103 L. Ed. 2d 639, 109 S. Ct. 1402 (1989); *see, e.g., Burka v. New York City Transit Authority*, 739 F. Supp. 814, 827 (S.D.N.Y. 1990).

[132] The Employee Polygraph Protection Act of 1988, 29 U.S.C. sections 2001-2009 (1994), prohibits polygraph testing by private employers except in certain statutorily defined circumstances. The Fair Credit Reporting Act, 15 U.S.C. sections 1681-1681t (1994), permits the use of consumer credit reports in making employment decisions, but imposes certain requirements relating to the disclosure and accuracy of the information. The Americans with Disabilities Act, 42 U.S.C. sections 12101-12213 (1994), regulates employer-mandated medical inquiries and examinations. See 42 U.S.C. section 12112 (d).

[133] In a recent case, a district court noted that the sweep of the ECPA could include instances where the privacy of an individual is violated by use of deceptive practices - - more commonly known as social engineering - wherein an employer obtains personal information by pretending to be someone other than the employer. The steps taken by the Navy in its pursuit of Timothy R. McVeigh were not only authorized under its policy, "Don't Ask, Don't Tell, Don't Pursue," but likely illegal under the Electronic Communications Privacy Act of 1986 ("ECPA"). *See id.* The Court found that it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated. In the words of the court, "in these days of big brother, where through technology and otherwise the privacy interests of individuals from all walks of life are being ignored or marginalized, it is imperative that statutes explicitly protecting these rights be strictly observed." *McVeigh v. Cohen,* 983 F. Supp. 215, 220 (D. D.C. 1998).

[134] The employees' consent to wiretapping or monitoring must be unambiguous and clearly encompass the types of communications subject to the monitoring, although, apparently, it does not need to be explicit or in writing.

[135] This exception covers telephone equipment used for ordinary business purposes by the employer, such as switchboard systems, intercom equipment, as well as numerous phone extensions connected to the same telephone line.

[136] The business-extension exception allows the employer to monitor its employees when the device that intercepts a communication is a telephone or electronic communication system being used in the ordinary course of business. This exception allows for workplace telephone monitoring conducted by employers. Originally, the Wiretap Act only applied when the intercepting device used was a telegraph or telephone equipment. However, with advances in communication technology, an erosion in the effectiveness of the Act occurred because many communication systems failed to use the basic types of technology contemplated by the Act. As a result, Congress amended the Wiretap Act by enacting the Electronic Communications Privacy Act of 1986 (ECPA), which it passed to cover private corporate communication systems. This legislation updated the Wiretap Act to cover new technologies that were developed in the interim. As a result, the Wiretap Act now protects the interception of data transferred by wire, radio, or other electronic means. However, the ECPA does not prevent electronic communication service providers from intercepting, monitoring, and reading electronic mail in certain circumstances. *See* 18 U.S.C. §2511(2)(a)(i).

[137] *See* John R. Aiello, *Computer-Based Work Monitoring: Electronic Surveillance and its Effects,* 23 JOURNAL OF APPLIED SOCIAL PSYCHOLOGY 499 (1993); Julie Gannon Shoop, *Electronic Monitoring: Is Big Brother at the Office?*, 28 TRIAL 1 (1992).

[138] Ottensmeyer, Edward J. and Mark A. Heroux, *Ethics, Public Policy, and Managing Advanced*

Technologies: The Case of Electronic Surveillance. 10 JOURNAL OF BUSINESS ETHICS 519 (1991).

[139] *See id.*

[140] The various types of electronic monitoring currently used include the following: Telephone Call Accounting - employers record such data as how many calls are made from a particular extension, which numbers are called, and the length of the calls. While this method is typically used to establish productivity quotas, employers have also used it to monitor the frequency and duration of personal calls. However, listening to the content of personal calls is illegal under existing legislation. Telephone Service Observation - with this type of surveillance, supervisors listen to their subordinates' business telephone calls. Calls may be recorded for later listening, or supervisors may listen on line. This method is predominately used as a quality assurance check for employees who deal with the public. Computer Monitoring - as alluded to earlier, software exists which allows managers to read their employees' computer screens. More common uses of computer monitoring, however, are counting keystrokes to measure speed of data entry, or monitoring time spent away from the computer. Recent enhancements to computer monitoring may include attempts to transmit subliminal messages that urge employees to work faster. Location monitoring - some organizations even use computer chips placed on employees' badges to track their location. These "electronic leashes" are not yet in widespread use.

[141] *See ASIS Speaks out on Electronic Monitoring,* 36 SECURITY MANAGEMENT, No. 4, April 1992, at 93.

[142] Subcommittee on Labor-Management Relations; U.S. House Committee on Education and Labor; 1991. Hearing on H.R. 1218; The Privacy for Consumers and Workers Act (published proceedings of hearing held June 11, 1992.

[143] 704 F.2d 577 (11th Cir. 1983).

[144] *See id.* at 583.

[145] 802 F.2d 412 (11th Cir. 1986); *see also Deal v. Spears,* 780 F. Supp. 618 (W.D. Ark. 1991); *Simmons v. Southwestern Bell Tel. Co.*, 452 F. Supp. 392 (W.D. Okla. 1978).

[146] *See Epps*, 802 F.2d at 417.

[147] *Parrish v. Northern Telecom, Inc.,* C.A.No. 3:90-0790 (M.D. Tenn. 1990). In a related matter, Northern Telecom later banned secret monitoring. The company stated that it would no longer engage in or permit its employees to conduct undisclosed monitoring of employee voice, video, or data communication. Northern Telecom Bans Secret Monitoring; CWA Agreement Sets Major Privacy Precedent, PR Newswire, Jan. 30, 1992, available in LEXIS, NEXIS Library, PRNEWS File. Northern Telecom Bans Secret Monitoring; CWA Agreement Sets Major Privacy Precedent.

[148] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy,* 4 Harv. L. Rev. 193, 195 (1890).

[149] *See generally,* Robert G. Boehmer, Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop, 41 DePaul L. Rev. 739, 773-95 (1992) (Boehmer analyzes various constitutional and statutory claims that may arise when an employer uses surveillance and monitoring).

[150] The dignitary nature of the right of privacy is no less apparent under Fourth Amendment

jurisprudence; notably, the invasive nature of drawing a person's blood for the purpose of examining the blood for various drugs is per se unlawful if done by a government employer without suspicion and without serving special needs superabounding above the normal or ordinary needs of law enforcement. *See, Walker v. Miller,* 519 U.S. 624 (1997) (holding as unconstitutional a Georgia law requiring candidates for state office to pass a drug test).

[151] *See, e.g., Borse v. Piece Goods Shop, Inc.,* 963 F.2d 611, 620 (3d Cir. 1992) (citing *Vogel v. W.T. Grant Co.*, 327 A.2d 133, 135-36 (Pa. 1974)) (adopting the Restatement (Second) approach in holding that discharge of an employee for refusing to submit to a urinalysis screening may violate employee's privacy); *O'Brien v. Papa Gino's, Inc.*, 780 F.2d 1067, 1071-72 (1st Cir. 1986) (acknowledging that coercing an employee into taking a polygraph examination would be highly offensive to a reasonable person); *Stockett v. Tolin,* 791 F. Supp. 1536, 1555-56 (S.D. Fla. 1992) (stating that unwelcome touching rising to the level of battery constitutes an invasion of solitude); *Neal v. Corning Glass Works Corp.*, 745 F. Supp. 1294, 1299 (S.D. Ohio 1989); *Rogers v. Loews L'Enfant Plaza Hotel,* 526 F. Supp. 523, 528 (D.D.C. 1981) (citing *Pearson v. Dodd,* 410 F.2d 701, 704 (D.C. Cir.) (approving extension of the invasion of privacy tort to intrusions into spheres from which an ordinary plaintiff could reasonably expect defendant to be excluded), *cert. denied,* 395 U.S. 947 (1969)); *Pemberton v. Bethlehem Steel Corp.*, 502 A.2d 1101, 1116-17 (Md. Ct. Spec. App.) (noting that an actionable intrusion requires invasion of a private place or intrusion into the private seclusion of another, but that observation of someone in a public place is not an invasion of privacy since the one observed is not in seclusion), *cert. denied,* 479 U.S. 984 (1986).

[152] Restatement (Second) of Torts section 652A(2) (1977).

[153] *See generally,* David S. Hames, *Are Terminations Precipitated by an Invasion of Privacy Wrongful?*, 42 LAB. L.J. 371, 372 (1991); David S. Hames & Nickie Diersen, *The Common Law Right to Privacy: Another Incursion Into Employer's Rights to Manage Their Employees?,* 42 LAB. L.J. 757, 758 (1991).

[154] *See, e.g., Moffett v. Gene B. Glick Co.,*621 F. Supp. 244, 283 (N.D. Ind. 1985) (holding that the plaintiff, a white apartment manager whose employer and co-workers harassed her with racial and sexually oriented comments when she began dating a black male, had waived her claim to privacy by discussing the relationship in the office thus "making what was formerly private a topic of office conversation"), overruled on other grounds by *Reeder-Baker v. Lincoln Nat'l Corp.*, 644 F. Supp. 983 (N.D. Ind. 1986).

[155] Employees possess a legitimate privacy interest in their persons, offices, desks, and lockers and rightfully expect these areas to be restricted from employer intrusion unless there is good cause and adherence to proper procedures. The legal and moral legitimacy of employment searches depends upon a clear connection between the search and the integrity of business operations or the safety and security of employees, customers, or the public. The employer's policies emerge as a primary ingredient in determining the invasiveness of the search and the reasonableness of an employee's expectation of privacy.

[156] *See, e.g., Johnson v. Corporate Special Servs.,* 602 So. 2d 385, 388 (Ala. 1992) (finding the purpose of a worker's compensation investigation legitimate because the predominant issue in a workman's compensation claim is the extent of the employee's injury); *Catania v. Eastern Airlines, Inc.,* 381 So. 2d 265, 268 (Fla. 3d DCA 1980) (holding that the surveillance of the employee must be shown to have been reasonably limited to a legitimate purpose).

[157] *See, e.g.*, Jeffrey J. Olsen, *A Comprehensive Review of Private Sector Drug Testing,* 8 HOFSTRA LAB. L.J. 223, 269 (1991) (noting that unless off-premises conduct affects the employer's reputation, intrusion is subject to a privacy claim).

[158] *Vernars v. Young*, 539 F.2d 966, 969 (3d Cir. 1976) (holding that individual's have a reasonable expectation that their personal mail will not be read or opened by unauthorized persons); *Cruikshank v. United States,* 467 F. Supp. 539, 543 (D. Haw. 1979) (recognizing that the interception and reading of individual's mail constituted an invasion of privacy).

[159] Surveillance and monitoring at the workplace can negatively affect society as a whole because such practices may violate the right to privacy of its individual members.

[160] *See generally*, Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy, 10* N. ILL. U. L. REV. 479 (1990) (arguing that personal information, including medical records and an employee's financial affair's, implicates the right to privacy).

[161] *See, e.g., Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 626 (3d Cir. 1992); *Kelley v. Schlumberger Tech. Corp.*, 849 F.2d 41, 42 (1st Cir. 1988); *O'Brien v. Papa Gino's of America, Inc.*, 780 F.2d 1067, 1072 (1st Cir. 1986); *Garus v. Rose Acre Farms, Inc.*, 839 F. Supp. 563, 570 (N.D. Ind. 1993); *K-Mart Corp. v. Trotti,* 677 S.W.2d 632, 637 (Tex. Ct. App. 1984); *Cordle v. General Hugh Mercer Corp.*, 325 S.E.2d 111, 117 (W. Va. 1984).

[162] As noted supra, the law of privacy has long recognized the possibility that powerful, sophisticated, modern technology can invade an employee's privacy, tortiously. Unfortunately, courts have been halting and languid in applying this principle of common law tort to actual instances of invasive surveillance.

[163] *See, e.g.*, note 31, *infra.*

[164] Not only is this a questionable practice in a normative sense, but exceptional violations of worker privacy should be considered a bad business practice by scrupulous employers. *See, e.g.,* Dan Gillmor, *Violating Privacy Is Bad Busness*, COMPUTERWORLD, March 23, 1998, at 38.

[165] At bottom, the law of privacy should inform and remind us that the invasive nature of high technology supports the notion that vigilant protection of the right of privacy must encompass the basic principle that personal autonomy and individual dignity does not become less important simply because the individual has entered a workspace. *See,* Rod Dixon, *Windows Nine-To-Five: Smyth v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communications,* 2 VA. J. L. & TECH 4 (1997).
