Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom

Ray Lewis
Laws and institutions must go hand in hand with the progress of the human mind. As that becomes more developed, more enlightened, as new discoveries are made... and opinions change with the change of circumstances, institutions must advance also, and keep pace with the times. We might as well require a man to wear still the coat which fitted him when a boy.

—Thomas Jefferson

I. INTRODUCTION

One hundred and seventeen years ago, Samuel D. Warren and Louis D. Brandeis published an article titled The Right to Privacy, introducing the idea that “existing law affords a principle which may be invoked to protect the privacy of the individual from invasion.” The two contended that protection of the individual “is a principle as old as the common law” but “[p]olitical, social, and economic changes entail the recognition of new rights, and the common law... grows to meet the demands of society.” The “growth” perceived by Warren and Brandeis was mankind’s right to an “inviolate personality,” a right “to be let alone,” a right to privacy.

Allegedly, the stimulus for the article was Warren’s recent marriage into a wealthy “blue blood” Bostonian family. Warren found that his marriage was accompanied by detailed reports of his family life in Boston’s Saturday Evening Gazette. This naturally annoyed Warren, who conferred with Brandeis, resulting in The Right to Privacy. Beyond the personal experience of Warren, the two scholars identified urgent threats to privacy that had a broader effect on society as a whole:
Recent inventions and business methods call attention to the next step which must be taken for the protection of the person . . . . Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of the private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops." 8

Ironically, Warren and Brandeis's nineteenth century apprehension for "recent inventions" and "business methods" is even more pertinent in the twenty-first century. In 1890, the two were concerned that photographic technology and yellow journalism would diminish "each individual[']s right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." 9 Today, individual autonomy is matched against new opponents: e-mail and electronic surveillance. In 1985, the Congressional Office of Technology Assessment reported that the "primary purpose of electronic surveillance is to monitor the behavior of individuals, including individual movements, actions, communications, [and] emotions . . . ." 10 This new "business method" of electronic monitoring is capable of completely erasing an individual's right to privacy in his e-mails, thereby diminishing his ability to determine what aspects of his life remain private or public.

Computer technology and the Internet have reshaped and revolutionized the private-sector workplace unlike any technological advance since perhaps the Industrial Revolution. Unfortunately, this new technology developed into a double-edged sword. Although the Internet allows for faster communications and greater access to information, it poses an unparalleled threat to privacy rights. The Internet has spawned countless privacy issues; this comment focuses upon the lack of e-mail privacy afforded to an employee within corporate America. 11 Given that "e-mail remains the most prevalent online activity, with 87.8 percent of

9. Id. at 198.
11. This comment focuses upon the private-sector workplace. Public-sector privacy claims rely upon the Fourth Amendment because the employer is a government entity. The themes and ideology surrounding privacy permeate the controversy at both levels; however, analysis of the two sides is substantially different given that private-sector employees have no direct constitutional claim.
Internet users sending and receiving e-mail,"\textsuperscript{12} preserving the individual's right to control the extent to which these personal communications are disclosed is critical. Advances in technology and deficiencies within the law have created a work environment in which an employer can read, monitor, and store employee e-mails without ever being detected,\textsuperscript{13} without ever breaking the law, and with no regard to employee privacy. Frustrated commentators have labeled the current legal situation as creating "electronic sweatshops,"\textsuperscript{14} being "haystack[s] in a hurricane,"\textsuperscript{15} and as a legal "sleeping giant."\textsuperscript{16}

Thomas Jefferson believed that the law should respond to the progression of the human mind.\textsuperscript{17} Regrettably, in the arena of electronic privacy, lawmakers in the United States have ignored his philosophy. The legal framework in the United States is antiquated and cannot adapt or adjust to the changes in society and

\begin{itemize}
  \item \textsuperscript{12} United States Department of Commerce, Economics and Statistics Administration & National Telecommunications and Information Administration, A Nation Online: Entering the Broadband Age 9 (2004), available at http://www.ntia.doc.gov/reports/anol/NationOnlineBroadband04.htm. The report found that 54.6 percent of U.S. households have access to the Internet and that between 2001 and 2003, "the number of households with Internet connections grew by 6.9 million." Id. at 5.
  \item \textsuperscript{13} See 1985 OTA Surveillance Report, supra note 10, at 11:
    New surveillance tools are technically more difficult to detect, of higher reliability and sensitivity, speedier in processing time, less costly, more flexible and adaptable, and easier to conceal . . . . Current R&D will produce devices with increased surveillance capabilities . . . .
  \item \textsuperscript{14} Catherine Collins, Bill Would Require Notices When Bosses Snoop on Employees, L.A. TIMES, Nov. 3, 1991, at D2 ("[U]nrestrained surveillance of workers has turned many modern offices into electronic sweatshops" (quoting Senator Paul Simon)).
  \item \textsuperscript{15} Bloustein, supra note 6, at 962 (quoting Ettore v. Philco Television Broad. Co., 229 F.2d 481, 485 (3d Cir. 1956)).
  \item \textsuperscript{17} THE JEFFERSONIAN CYCLOPEDIA, supra note 1, at 726.
\end{itemize}
technology. The primary avenues through which an employee would hope to find e-mail privacy protections are tort law, federal law, or state law. Unfortunately, at every turn, the employee finds the road blocked because the law heavily favors the interests of the employer over the privacy rights of the employee.\(^{18}\) Common law remedies have an “expectation of privacy” requirement that insulates employers from liability.\(^{19}\) Applicable federal legislation, the Electronic Communications Privacy Act (“ECPA”), fails to protect the employee because it is confusing, poorly drafted, and riddled with holes and exceptions.\(^{20}\) State constitutional protections rarely apply to private employers, and state statutes either parallel the flawed ECPA or are inapplicable to private employers.\(^{21}\) In essence, the privacy rights of employees vanish the moment they come in contact with their workplace or employer.

The condition of employee e-mail privacy protection in the United States is a gross injustice. When Warren and Brandeis perceived a problem in 1890, they called for and took the “next step” in protecting the individual. Presently, there is a problem in our electronic privacy law, and again it is necessary for the law to catch up to technology and to the needs of the people. Numerous scholars have approached this issue by engaging in comparative analysis between U.S. law and European versions, but comparative studies fall short of providing a solution to the problem. This comment proposes a solution by calling for the abandonment of the ECPA and the adoption of legislation that mirrors the provisions, ideas, and foundations of the electronic privacy law of the United Kingdom—the Data Protection Act (“DPA”).

Part II of this comment explicates and analyzes the three paths an employee might utilize when attempting to redress an invasion of privacy, ultimately showing that the employee’s right to privacy is unprotected at each level. Part III discusses the emergence of electronic monitoring in the workplace and the threat it poses to privacy. More importantly, Part III explores the U.S.’s conception of privacy that justifies a legal framework that sacrifices the privacy rights of the employee.

\(^{18}\) See generally Kesan, supra note 13, at 292; Steven B. Winters, Do Not Fold, Spindle or Mutilate: An Examination of Workplace Privacy in Electronic Mail, 1 S. CAL. INTERDISC. L.J. 85, 94–97 (1992); Peter Schnaitman, Comment, Building A Community Through Workplace E-mail: The New Privacy Frontier, 5 MICH. TELECOMM. & TECH. L. REV. 177, 183 (1999).

\(^{19}\) See discussion infra Part II.A.

\(^{20}\) See discussion infra Part II.B.

\(^{21}\) See discussion infra Part II.C.
Part IV presents the creation, safeguards, and provisions of the Data Protection Act. This section first charts the development of the DPA, focusing on the influence of the European Union’s (“EU”) Charter of Fundamental Human Rights and the EU Directive 95/46/EC, then outlines the DPA and its effects. Part IV also explains why adopting the DPA is the best road to take. In comparing the two bodies of law, the ECPA and the DPA, it is clear that at each level the protections provided under the UK law are more comprehensive than under applicable U.S. law.

II. THE LAW: A THIN VEIL AT BEST

Since Warren and Brandeis successfully presented their concept of a right to privacy, numerous legal methods of protecting this right have developed. For an employee seeking to remedy what he feels is an invasion of e-mail privacy in the workplace, there are generally three avenues of recovery. The first is found within common law tort principles. The second is the vastly more complex federal anti-wiretapping statute. Lastly, the individual states have statutory versions of the federal anti-wiretapping statute; for the most part these state statutes possess minor variations of federal guidelines and protections.

A. The Common Law

Publication of Warren and Brandeis’s article in 1890 was the advent of privacy tort law. The next step in the tort’s evolution was William Prosser’s 1964 article Privacy. Prosser concluded that privacy was “not one tort, but a complex of four,” described as follows: (1) intrusion upon the seclusion or solitude of another; (2) public disclosure of embarrassing facts; (3) placing another in a “false light” in the public eye; and (4) appropriation of another’s name or likeness. Each distinct tort attempts to recognize and protect a “substantial zone of freedom” where an individual has

---

22. See generally Bloustein, supra note 6, at 963; Kesan, supra note 13, at 302–04; William L. Prosser, Privacy, 48 CALIF. L. REV. 383 (1960); Warren & Brandeis, supra note 2, at 206.

23. Prosser, supra note 22, at 383.

24. Id. at 389. See also W. Page Keeton et al., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 849–69 (5th ed. 1984); RESTATEMENT (SECOND) OF TORTS § 652A (1977).

25. Gantt, supra note 13, at 374 (citing Young v. Jackson, 572 So. 2d 378, 381 (Miss. 1990)).
the "right to be let alone." A majority of employee claims against an employer for e-mail monitoring involve the privacy tort of "unreasonable intrusion upon the seclusion of another." Therefore, the primary focus remains upon this version of the common law remedy.

An employee's prima facie claim of intrusion has three elements: "(1) an intentional intrusion; (2) that is highly offensive; and (3) the employee had a reasonable expectation of privacy." An "intrusion" is easily accomplished because it need not be physical in nature nor does it require disclosure. In most cases, courts will find that electronic monitoring or surveillance is sufficient to establish the first element. Over the years, analysis of the second element has merged into the third; the result being that a privacy claim rests upon the employee's reasonable expectation of privacy.

The courts have added an additional legal test to this crucial element and require that the "expectation" be both subjectively and objectively reasonable. Fundamentally, the courts have placed the elements for a Fourth Amendment constitutional claim into the common law tort of privacy, even though there is no enumerated right to privacy found in the Constitution. Judicial application of this subjective/objective test is to "first define the scope of an employee's reasonable expectation of privacy" to determine its subjective nature "and then balance the employer's business interest[s] against the employee's individual rights" to determine its objective nature.

In most cases, an employer can easily defeat any expectation of privacy asserted by an employee. Any subjective expectation held by the employee is generally unwarranted because at work the employer defines the expectation of privacy by establishing an

30. Id. at § 652B cmt. a.
31. Gantt, supra note 13, at 375.
32. Id.
33. Establishing a Fourth Amendment violation requires the claimant to demonstrate a subjective expectation of privacy and an objective expectation that society would consider reasonable. Katz v. United States, 389 U.S. 347, 361 (1967). See also Gantt, supra note 13, at 375; Winters, supra note 18, at 94–97.
office policy regarding electronic monitoring. Additionally, many courts find that any objective expectation of privacy is outweighed by the "operational realities of the workplace." The net result is that "employees maintain few privacy interests that cannot be overridden by strong employer interests or... intrusive business practices."

Judicial interpretation of the "expectation" standard has resulted in a convoluted entanglement that operates to protect the employer and bar employee claims. The lack of recourse under tort law is the first in a string of examples where the employee's right to privacy is ignored in favor of the interests of the employer. In the search for a remedy for an invasion of e-mail privacy, the next avenue an employee may attempt is the federal anti-wiretapping statute.


In response to the 1968 holdings in *Katz v. United States* and *Berger v. New York*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act. This legislation regulated the use of telephone wiretaps and hidden microphones to record or intercept communications through a common carrier, the

35. *Id.* See also Bourke v. Nissan Motor Corp., No. BO68705 (Cal. Ct. App. July 26, 1993) (finding that plaintiffs had no expectation of privacy because they were informed of company policy that restricted their privacy rights); Hall Adams III, et al., *E-mail Monitoring in the Workplace: The Good, the Bad, and the Ugly*, 67 DEF. COUNS. J. 32, 44 (2000) (stating that the simplest course of conduct is for employers to have a policy regarding e-mail); Kesan, *supra* note 13, at 303 ("[B]y communicating an electronic monitoring policy, the employer can establish the level of privacy that employees may reasonably expect.").


39. 389 U.S. 347 (1967). The Supreme Court set the threshold for Fourth Amendment protections at whether a reasonable expectation of privacy existed in the area searched by officials. See generally id.

40. 388 U.S. 41 (1967) (extending the ruling in *Katz* to electronic eavesdropping on oral communications).

underlying purpose being the protection of individual privacy rights. Two decades later, congressional reports indicated that the existing law under Title III was "hopelessly out of date." By 1985, Congress was well aware of the need to amend the 1968 version of Title III. Congress directed the Office of Technology Assessment ("OTA") to study the effects that electronic surveillance had upon civil liberties. The subsequent report found that "innovations in electronic surveillance technology [had] outstripped constitutional and statutory protections." The primary area of concern was surveillance of electronic mail or e-mail. The OTA found that "interception of e-mail . . . involves a high level of intrusiveness and a significant threat to civil liberties." In regard to this concern, the report repeatedly noted that the law lagged behind the technology and that e-mail was afforded weak or nonexistent privacy protections.

The report also considered the differing protections afforded to postal mail and electronic mail. It troubled the OTA that a letter delivered by the U.S. Postal Service is granted extensive legal protections while that same letter via e-mail is almost totally insecure. The report found that:

A letter sent by first class mail is afforded a high level of protection against unauthorized opening by a combination of constitutional provisions, case-law, and U.S. Postal Service statutes and regulations . . . . But there are no comparable Federal statutory provisions to protect the privacy and security of communications transmitted by . . . new forms of telecommunications and computer technology.

The OTA further criticized the situation as a "gap" in the protection of privacy that resulted in irresponsible "legal uncertainty." Guided by the OTA's report and various committee hearings, Congress's remedy for the "legal uncertainty" was an amendment.

---

44. 1985 OTA Surveillance Report, supra note 10, at 12.
45. Id. at 45.
46. Id. at 3-4, 12, 45.
47. Id. at 45.
49. Id.
to Title III called the Electronic Communications Privacy Act of 1986. Theoretically, the amended legislation "update[d] and clarif[ied] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies" in order to resolve the legal inadequacies of Title III.\textsuperscript{50} Since its passage in 1985, the ECPA has undergone no changes and, at present, is the primary federal law applicable to the issue of workplace e-mail monitoring.

1. Electronic Communications Privacy Act Provisions

Originally, Title III applied only to communications categorized as containing the human voice;\textsuperscript{51} therefore, the goal of the ECPA was to expand protection into "non-voice portion[s] of a wire communication."\textsuperscript{52} To achieve this goal via an amendment, Congress incorporated into the legislation a comprehensive set of definitions, the most significant being § 2510(12), a broad definition of "electronic communication."\textsuperscript{53} Once Congress defined the term, it was simply inserted into the statute wherever Title III had previously referenced wire and oral communications.

The next significant hurdle Congress had to overcome was that electronic communications are more complex than the telephones and "bugs" Title III regulated. The OTA report emphasized the

\begin{enumerate}
\item \textsuperscript{50} Id. at 3555.
\item \textsuperscript{51} Id. at 3568.
\item \textsuperscript{52} Id. at 3567.
\item \textsuperscript{53} 18 U.S.C. § 2510(12) (2000) states, in pertinent part, that:
\begin{itemize}
\item "[E]lectronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
\begin{itemize}
\item (A) any wire or oral communication;
\item (B) any communication made through a tone-only paging device;
\item (C) any communication from a tracking device (as defined in section 3117 of this title); or
\item (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds . . . .
\end{itemize}
\end{itemize}
\end{enumerate}
complicated nature of electronic communications, namely, the vulnerability to interception and surveillance at every stage of their existence.\textsuperscript{55} From transmission to receipt to storage, electronic communications were almost totally unprotected by Title III. Congress’s solution was to divide the ECPA into two components, Title I and Title II, which would protect the communications during transmission or storage.\textsuperscript{56} Notwithstanding this split in coverage, the definitions found in Title I’s § 2510 apply to Title II as well, and the price for violating either part’s provisions includes both civil and criminal penalties.\textsuperscript{57}

Title I, otherwise known as the Wiretap Act, prohibits any person\textsuperscript{58} from intentionally intercepting any wire, oral, or electronic communication.\textsuperscript{59} It also prohibits the use and disclosure of any contents of intercepted communications.\textsuperscript{60} Title I expands Title III’s definition of “intercept” to include both “aural or other acquisition” and requires that the interception take place through some kind of “electronic, mechanical, or other device.”\textsuperscript{61} Title II, designated the Stored Communications Act, prohibits anyone from intentionally accessing wire or electronic communications held in “electronic storage.”\textsuperscript{62}

\textsuperscript{56} Compare 18 U.S.C. §§ 2510-22 (2000) (Title I of the ECPA), with Id. §§ 2701-11 (Title II of the ECPA).
\textsuperscript{57} See 18 U.S.C. § 2520 for civil remedy and § 2511(4)(a) for criminal penalties under Title I. Id. §§ 2520, 2511(4)(a). See also 18 U.S.C. § 2707(a) for civil remedy and §2701(b) for criminal penalties under Title II. Id. §§ 2707(a), 2701(b).
\textsuperscript{58} 18 U.S.C. § 2510(6) defines a person as “any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation.” Id. § 2510(6).
\textsuperscript{59} Id. § 2511(1)(a).
\textsuperscript{60} Id. § 2511(1)(b)-(d).
\textsuperscript{62} 18 U.S.C. § 2701(a) (2000). “Access” was used in the 1968 version of § 2701, but neither that act nor the ECPA ever defines the term. “Electronic storage” is: (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any
However, the two-pronged construction is the source of major judicial confusion, which diminishes the ECPA’s effectiveness. Courts are cynical over the intersection of Title I and Title II, one court labeling it as “famous (if not infamous) for its lack of clarity.”63 In 2005, the U.S. First Circuit Court of Appeals referred to the intersection of Title I and Title II as “complex, often convoluted.”64 E-mail makes the situation more complex because, at various stages in transmission, the e-mail is temporarily stored before moving on to its final destination.65 When applying the ECPA to e-mail cases, the courts are divided over whether Title II applies to momentary storage occurring during an e-mail’s transmission or whether Title II applies strictly to post-transmission storage.66 The net result of the various interpretations among the federal circuits is that the ECPA fails to have a coherent standard of operation. Instead, the scope and extent of ECPA protections largely depend upon which circuit has jurisdiction over the plaintiff’s claim rather than application of the statutory language. Consequently, the structure Congress drafted into the ECPA has made the law functionally confusing, problematic, and inconsistent.

Legal scholars also criticize the ECPA’s effectiveness in protecting privacy by arguing that it focuses on “third party” interception and fails to protect any privacy rights an employee may have in his e-mail.67 Another troubling aspect of the ECPA legislation is that it never refers to nor mentions privacy rights. One would suppose that Congress’s focus upon privacy in the Act’s development would be reflected in the Act itself, but that is not the case. Another flaw is that the twenty-year-old legislation attempts to regulate technologies that constantly advance.

While the bifurcated structure, lack of clarity, and ambiguous history of the ECPA has garnered a large amount of disapproval, it storage of such communication by an electronic communication service for purposes of backup protection of such communication. Id. at § 2510(17).

63. Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 462 (5th Cir. 1994). See also United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998); Moriarty, 962 F. Supp. at 221; Forsyth v. Barr, 19 F.3d 1527, 1543 (5th Cir. 1994) (all citing Steve Jackson Games or independently pointing out the lack of clarity in the sections).

64. Councilman, 418 F.3d at 80 (quoting Smith, 155 F.3d at 1055).

65. See source cited infra notes 108–09.


67. See, e.g., Gantt, supra note 13, at 352, noted in Winters, supra note 18, at 119 (1992).
pales in comparison to the criticism the body of law has experienced as a result of the statute’s exceptions.

2. Statutory Exceptions Under the ECPA

In a workplace context, the ECPA theoretically protects the privacy of the individual by prohibiting or limiting the extent to which the employer could intercept or access an employee’s communications. Yet, the ECPA includes three general exceptions to its provisions that are in direct conflict with that ambition. The consent exception, the service provider exception, and the business use exception work in conjunction to negate any liability an employer might incur under the ECPA. If an employer shows that its monitoring activity fits under any one of these exceptions, an employee’s claim will fail.

a. Consent Exception

The consent exception is the least broad of the three exceptions and is present in both Title I and Title II. This exception bypasses ECPA protections if a party to the communication gives prior consent. While judicial interpretation of the consent exception under Title II’s provisions has yet to occur, the courts have established that consent under Title I may be express or implied but “not . . . casually inferred.” An employer may easily escape the ECPA provisions by simply establishing an office policy of monitoring and making the acceptance of its policies a requirement for employment. Therefore, oftentimes, an individual must either give up a chance at employment or forfeit his right to privacy.

---

69. Id. § 2511(2)(a)(i) (interceptions); id. § 2701(c)(1) (stored communications).
70. Id. § 2510(5)(a) (interceptions only).
71. See id. §§ 2511(2)(d), 2701(c), 2702(b)(3).
b. Service Provider Exception

The service provider exception shields Internet and e-mail system providers from ECPA prohibitions under both Title I and Title II. Again, Congress’s statutory construction and unclear language have made this exception vague and led to confusion within the law.

Under Title I, the exception permits a service provider whose facilities are used in the transmission of the communication, “to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity that is a necessary incident to the rendition of his service.” Title I’s provider exception, then, confusingly amends itself and prohibits a public provider of wire communications from carrying out random monitoring. This ban on random monitoring only extends to wire communications, leaving e-mail devoid of any protection and vulnerable to random interception by a service provider.

Title II’s provider exception has two parts. First, the ECPA prohibition on accessing stored communications does not apply to conduct authorized by the “service provider” of the electronic communications system. Second, a “public service provider” is allowed to disclose the contents of a stored communication if disclosure is a necessary incident to the rendition of the service or protects the rights or property of the service provider.

Confusion exists because Congress failed to distinguish a “public service provider” from a “service provider”; nor did Congress define or limit the language “normal course of employment” or “necessarily incident to rendition of services.” With so little direction available and the broad scope of the exception’s language, commentators argue that the service provider exception grants employers “unfettered discretion” in monitoring their employees’ e-mails.

---

75. Id. § 2511(2)(a)(i).
76. Id.
77. Greenberg, supra note 54, at 237.
79. Id. § 2702(b)(5).
c. Business Use Exception

The final and most unnerving exception to ECPA liability is a carryover provision from pre-ECPA law, known as the business use exception under Title I. Congress amended the definition of "intercept" under Title I in order to extend protections to electronic communications but added the requirement that an "electronic, mechanical or other device"81 be used in the interception of the communication. Congress then retained a pre-ECPA restriction and exempted certain types of devices or equipment from the statute’s prohibitions. Basically, this exception insulates employers from liability if they use certain devices to monitor their employees.82

The courts have adopted two general approaches in applying the business use exception: the context and the content approach.83 The context approach focuses on the circumstances surrounding the interception, such as the extent, knowledge, notification, and existence of a legitimate business purpose.84 In practice, the courts allow employers to escape liability if they “satisfy a checklist of objective considerations.”85 This “checklist” inserts into the ECPA the common law reliance upon “expectations of privacy,” even though the federal legislation should protect communications regardless of these expectations.86 The content approach stresses the nature of the intercepted communication and whether or not it is personal or business related. Precedent permits employers to intercept a communication that is “likely to further any legitimate business interest” or is “reasonably related to a business purpose.”87 In the context of phone communications, an employer may only monitor calls to the extent necessary to determine their nature, and if the employer discovers that the call is personal they must terminate the monitoring.88

Judicial application of the business use exception to e-mail monitoring has not yet occurred. Some scholars argue that this

82. Id. § 2510(5)(a).
83. Gantt, supra note 13, at 365.
85. Gantt, supra note 13, at 365 (citing Martha W. Barnett & Scott D. Makar, "In the Ordinary Course of Business": The Legal Limits of Workplace Wiretapping, 10 HASTINGS COMM. & ENT. L.J. 715, 728 (1988)).
86. Id.
exception has no application to e-mails. However, others believe that when claims involving this exception and e-mail appear before the courts, the precedent under the context and consent approaches will permit unrestricted interception of employee e-mails. The context approach converts the federal legislation into the common law tort of privacy, which, as previously shown, affords no protection to employees. The content approach to e-mail is unsound because an e-mail's business or personal nature can only be discovered through looking at its contents. Using the content of an employee’s e-mail to justify the employer’s intrusion is illogical because the employer should have adequate justification before it invades the employee’s privacy.

Once any of the aforementioned exceptions are successfully asserted, the ECPA fails to place any restrictions on the form and extent of such exempted monitoring. It is unclear why Congress elected to provide protections with one hand and then remove them with the other. Nevertheless, the overall effect of the exceptions is to completely offset the protections afforded under the ECPA. Scholars have commented that, in light of the scope of the exceptions, the ECPA is “ineffective in regulating the employer/employee relationship.” In 1986, Congress set out to “update and clarify Federal privacy protections” in an effort to remove the “legal uncertainty” existing at that time. Disappointingly, somewhere in the ECPA’s conception, Congress lost sight of its goals and enacted a body of law that affords limited privacy protections and, ironically, has proven to be infused with legal uncertainties. The only certainty connected to the ECPA is that it fails across the board to protect the privacy rights an individual, especially an employee, may have in his e-mails.

---

89. McIntosh, supra note 13, at 553.
90. Gantt, supra note 13, at 369–70.
91. See discussion supra Part II.B.2.
94. Greenberg, supra note 54, at 235.
95. Kesan, supra note 13, at 299. See generally Greenberg, supra note 54, at 234–35; McIntosh, supra note 13, at 549–58; Schnaitman, supra note 18, at 187–91.
3. Congressional Recognition of the Problem

Congress, despite its lack of action, has demonstrated that it is aware of the problems and contradictions that permeate the ECPA. In 1991, 1992, and again in 1993, the Privacy for Consumer and Workers Act ("PCWA") was introduced to Congress in the hopes of addressing the issues created by electronic workplace monitoring. The five major reforms proposed under the PCWA were: (1) employers would be required to generally notify prospective and current employees of how and when monitoring may take place; (2) employers would be required to give specific prior notification to an employee who would be monitored; (3) there would be a prohibition of random or periodic monitoring for employees employed for at least five years; (4) there would be additional time limits set as to the length of monitoring; and (5) employers would be prohibited from taking action against an employee based upon any personal data obtained in violation of the PCWA.

Initially, this new legislation appeared to increase e-mail privacy protections, but, again, Congress included exceptions that bypassed such protections. If an employer had a reasonable suspicion that an employee was engaging in conduct that was criminal, constituted gross misconduct, was likely to cause economic loss or injury, or the employer had an "immediate business need for specific data," then the employer could monitor without regard to the prohibitions.

Although the PCWA was approved by a subcommittee of the House Committee on Education and Labor in 1994, the bill died there. Despite the exceptions, the PCWA was at least a step in the right direction toward better protecting the privacy rights of the individual. Perhaps it best serves as a signal that lawmakers are cognizant of the problem.

100. Id. at § 4(b).
101. Id. at § 5(b)(3).
102. Id. at § 5(b)(2).
103. Id. at § 8(a).
104. Id. at § 5(c).
105. Id. at § 9(a).
C. State Law

The remaining legal remedy open to employees is either state constitutional law or statutory law. In addition to incorporating language that parallels the Fourth Amendment, a number of state constitutions additionally extend to their citizens a right to privacy. However, those protections apply only against state governmental entities; therefore, constitutional claims against private employers will predominantly fail.

California, under Hill v. National Collegiate Athletic Association, is the only state to judicially extend its constitutional right to privacy to the private sector. The California Supreme Court found that the constitutional right to privacy extended to nongovernmental entities but divided the right to privacy into two categories: invasions "fundamental to personal autonomy" and invasions of "less central" privacy concerns. Using this distinction, the court then established a balancing test of "competing or countervailing privacy and non-privacy interests" that, consequently, works exactly like the expectation of privacy requirement found in tort law. Applying the balancing test, the court found that the National Collegiate Athletic Association did not violate constitutional rights because the athletes' privacy interests were reduced by their voluntary participation in NCAA athletics. This countervailing interest analysis curtails individual rights and diminishes the likelihood that an employee would be able to recover under this constitutional scheme. Additionally, this scenario will only play out in California, leaving this type of constitutional privacy issue inapplicable in the other forty-nine states.

Beyond constitutional protections, forty-eight states have legislation that parallels the provisions of the federal ECPA. A

---

107. 865 P.2d 633 (Cal. 1994) (involving a privacy challenge against the NCAA's drug testing program).
108. Id. at 653.
109. Id. at 655.
110. Id. at 657–59.
111. The only states that do not have such statutory protections are South Carolina and Vermont. See Lawrence E. Rothstein, Privacy or Dignity?: Electronic Monitoring in the Workplace, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 404 (2000). In situations where a state has enacted legislation, the courts consistently hold that the ECPA only preempts similar state laws if it is found that the state laws are less protective of the rights of the individual. See also
number of the states mirror the ECPA, including the consent, business use, and provider exceptions. Twenty-two states restrict the provider exception to common carriers of communications and/or have no business use exception. In thirteen states, prior consent must be obtained by all parties connected to the communication. The difficulty in administering these conflicting jurisdictional laws is compounded by the statutory interpretations of the state courts. For example, Illinois courts have ruled that the all-party consent rule in reality means the consent of at least one party.

In principal, relying on state statutes to protect employee e-mail privacy is unwise. The protections, scope, and application have no structure and, as one scholar noted, are "ill-suited for regulating a technology which erases state and national borders." The nature of the Internet, e-mail, and the right to privacy call for a cohesive solution best provided by federal regulation.

112. Adams, supra note 35, at 41.
113. Rothstein, supra note 111, at 404. Those states are Alabama, Delaware, District of Columbia, Georgia, Idaho, Indiana, Iowa, Kentucky, Louisiana, Maine, Minnesota, Mississippi, Missouri, New Hampshire, New Jersey, New Mexico, North Dakota, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, and Texas.
114. California, Connecticut, Delaware, Florida, Georgia, Illinois, Maryland, Massachusetts, Michigan, New Hampshire, Pennsylvania, and Washington all require both parties' consent to the monitoring. See CAL. PENAL CODE §§ 631(a), 632(a) (West 2006); CONN. GEN. STAT. § 52-570d (2005); DEL. CODE ANN. tit. 11, § 2402(c)(4) (West 2001); FLA. STAT. 934.03(3)(d) (2001); GA. CODE ANN. § 16-11-66(a) (2003); 720 ILL. COMP. ANN. STAT. § 5/14-2(a)(1) (West 2002); MD. CODE ANN., CTS. & JUD. PROC. § 10-402(c)(3) (West 2002); MASS. GEN. LAWS ANN. ch. 272 § 99(B)(4) (West 1992); MICH. COMP. LAWS ANN. § 750.539c (West 2004); N.H. REV. STAT. ANN. § 570-A:2 (2001); 18 PA. CONS. STAT. ANN. § 5704 (West 2000); WASH. REV. CODE ANN. § 9.73.030(1)(b) (West 2003).
116. Kesan, supra note 13, at 301.
III. E-MAIL, THE WORKPLACE, AND "OUR" PRIVACY

If you've got a boss who is monitoring e-mail to see if people are calling him a jerk—he probably is . . . .

The invention of the Internet drastically changed the face of American society. The world is literally constantly at our fingertips, so much so that this era is often called the Information Age. A major part of this so-called "Age" is the use of e-mail as a means of communication. E-mail may seem complicated, but when stripped of its technical terminology, it is actually a simple process. Basically, the contents of the e-mail are broken down into small packets and forwarded from one computer or network to another until all the packets reach their destination, where they are re-combined to form the original message. Amazingly, all of this takes fractions of a second. The technology behind e-mail has made it infinitely faster and far more efficient than postal mail; therefore, its popularity and use have exploded.

Naturally, corporate America has been quick to take advantage of the benefits e-mail offers its day-to-day operations—one "benefit" being the ability to electronically monitor its employees' use of e-mail. The U.S. General Accounting Office reported that in 1998, eighteen percent of employees were using e-mail at work, and by 2001, that number increased to forty-two percent, an increase of twenty-four percentage points in just three years.

In response to increased e-mail use in the workplace, employers have gone to great lengths to maintain a watchful eye upon their employees. A 2005 American Management Association survey found that seventy-six percent of employers are engaging in some form of electronic surveillance at the workplace. Thirty-six percent of employers track the content and keystrokes on their employees' computers and fifty-five percent retain and review employee e-mail messages. It was also reported that twenty-six percent of companies had terminated someone's employment.

118. See United States v. Councilman, 418 F.3d 67, 69 (1st Cir. 2005).
121. Id.
based upon e-mail use.\textsuperscript{122} Other reports place the percentage of employers monitoring e-mail at seventy percent and expect electronic monitoring software sales to climb from $139 million in 2001 to $662 million in 2006.\textsuperscript{123} It appears that the situation will worsen with time, and, if left in its current state, the law will only become more inept.

The privacy concerns set off by employer monitoring are intensified by statistical indications that e-mail is becoming a dominant form of personal communication. In 2004, the U.S. Department of Commerce reported that fifty-four percent of U.S. households possessed Internet connections, a twelve point increase from 2001.\textsuperscript{124} The report also found that one-third of the United States has access to the Internet on a daily basis.\textsuperscript{125} Furthermore, the most prevalent online activity is by far personal communications, with eighty-seven percent of Internet users sending and receiving e-mail.\textsuperscript{126} These numbers reflect that American society has adopted e-mail as a means of transmitting personal communications, many of which likely contain the very thoughts, sentiments, and emotions ideally protected by Warren and Brandeis’s right to privacy.

The statistics demonstrate that employer monitoring has become a part of the corporate atmosphere. Statistics also show that e-mail is gradually developing into a mainstream medium for personal communications. Just as it did in 1890, it seems that the turn of this century has once again thrown “recent inventions,” “business methods,” and privacy into direct conflict.

In the workplace, this recurring conflict is framed by two competing interests: the right of the employer to control its business and the employee’s right to privacy.\textsuperscript{127}

Employers assert that it is necessary in the furtherance of their business that they reserve broad discretion to monitor their employees’ workplace communications. The need to protect themselves from employee theft, security breaches, computer viruses, and losses in productivity demand that they maintain a watchful eye on their employees’ Internet conduct.\textsuperscript{128} Far more
terrifying to management is the possibility of incurring legal liability for the content of e-mails sent or received by their employees, for example, racial, obscene, or sexist material. Employers embrace these concerns by asserting one general theory: their interests should be favored because their networks, offices, and equipment are used to facilitate the communications.

It is evident from the current state of the law that legislators and government entities agree that the employer’s interests outweigh the employee’s right to privacy. Lawmakers rationalize this devaluation of privacy rights based on the U.S.’s concept that the right to privacy is not an absolute right but rather an aspect of personal property. Gail Lasprogata, an assistant professor at Seattle University, contends that the overall result of this conceptual framework has turned “privacy [into] a commodity [that] may be bargained away in exchange for employment.” Under this scheme, the right to privacy is converted into a contractual term or bargaining chip. Unfortunately, it is a bargaining chip that, no matter when played, the employee loses. If the employee wishes to maintain his right to privacy, he forfeits employment; or, if he accepts employment, he forfeits his right to privacy. Ordinarily, a person understands the effects of not having a paycheck but might not comprehend the consequences of giving up aspects of his privacy. In effect, privacy loses any real resemblance of a “right” and becomes a perk that might accompany employment.

Therefore, the first step in changing the law must be to change the manner in which privacy is viewed and understood. Primarily, the goal should be to completely erase the current property-based concept of privacy. Warren and Brandeis initially focused upon the individual when they defined the right to privacy as an individual’s right to control “to what extent his thoughts, sentiments, and emotions shall be communicated to others.”

The origin of the “property-based” concept of privacy extends from the influence of Prosser’s classification of privacy as four distinct torts.

129. Id.
130. Schnaitman, supra note 18, at 183.
132. Lasprogata et al., supra note 131, at 28.
133. Warren & Brandeis, supra note 2, at 198.
By converting the foundations of privacy into torts, Prosser stripped the right of its inherently human nature. In 1964, Edward J. Bloustein published an article criticizing Prosser's theories, which remains pertinent in contesting the "property-based" approach. Bloustein asserts that Prosser changed privacy from a spiritual value to a material one, ultimately concluding that Prosser's approach to privacy is backwards. Prosser views the "wrong" in invading privacy as the infliction of mental distress or infringement upon the value of one's name and reputation. But, Bloustein argues that invasions of privacy are "wrong" because they violate man's mentality, individuality, and personal dignity.

Even Warren and Brandeis expressed that "it is difficult to regard the right as one of property" but rather a "right to one's personality." Expressions of opinions, ideas, love, anger, or animosity between individuals are not things that should be measured in property values. Society can measure the effects of privacy invasions in monetary increments, but that is as far as it should go. The right to privacy is not pecuniary but connected to an individual's dignity, personality, and control over his own life. Privacy rights are not bargaining chips; therefore, lawmakers need to redefine their understanding of privacy and adjust the laws to protect privacy, not as property, but as a right to dignity.

IV. PROPOSAL: LEGAL ADVICE FROM ACROSS THE POND, THE DATA PROTECTION ACT IN FAVOR OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

It is to secure our rights that we resort to government at all.
—Thomas Jefferson

The United States needs to reconstruct the law that currently regulates privacy in electronic communications. This redrafting of the law will be a difficult task and will have monumental effects both nationally and internationally. However, the task can be simplified if lawmakers use international bodies of law as prototypes. While the U.S.'s attitude towards this issue has been legally stagnant for the last twenty years, the nations of the

134. Bloustein, supra note 6, at 971.
135. Id. at 965.
136. Id. at 971, 973.
137. Warren & Brandeis, supra note 2, at 200.
138. Id. at 207.
European Union\textsuperscript{140} have confronted electronic communication privacy and developed clear and comprehensive protections.

This comment proposes that the United States examine the steps that the United Kingdom has taken in this area and adopt legislation that mirrors its laws. The UK’s Data Protection Act has provisions that are best tailored to respond to corporate/privacy conflicts—the law is modern, unambiguous, concise, and it is grounded in the correct notions of privacy.

\textbf{A. Foundations of the Data Protection Act}

The European Union addressed the conflict between the Internet and individual privacy and devised a solution that is the polar opposite of the U.S. approach—the major difference being that the EU’s primary emphasis is upon the individual. The Preamble of the EU’s Charter of Fundamental Rights states that the “Union is founded on the indivisible, universal values of human dignity... [and that] it places the individual at the heart of its activities.”\textsuperscript{141}

This Charter of Fundamental Rights outlines the rights and freedoms that the individual member states must respect in order to retain their membership in the European Union.\textsuperscript{142} Each member state controls the drafting and enforcement of its laws limited only in that they must comply with the recognized fundamental rights. Of the fifty-four major rights and freedoms outlined by the Charter of Fundamental Rights, four are integral in developing the EU’s legal scheme for protecting electronic communications: (1) Article

\begin{itemize}
  \item \textsuperscript{140} “The European Union (EU) is a family of democratic European countries that work together to promote peace and prosperity. It is not a State intended to replace the existing European States, but is more than an organization for international cooperation. The EU is, in fact, unique. Its member states have established common institutions and delegate portions of their sovereignty to those institutions so that matters of joint interest can be resolved at a European level.” Europa, Panorama of the European Union, http://europa.eu.int/abc/panorama/index_en.htm (last visited Feb. 14, 2007). The EU fosters cooperation among the peoples of Europe, promotes unity, and protects shared values of democracy, freedom, and social justice. \textit{Id.}
  \item \textsuperscript{141} Charter of Fundamental Rights of the European Union, 2000/C 364/01, 364/8 (Dec. 18, 2000).
  \item \textsuperscript{142} \textit{Id.}
\end{itemize}
1 firmly states that "human dignity is inviolable";\textsuperscript{143} (2) Article 3 grants individuals a right to their physical and mental integrity;\textsuperscript{144} (3) Article 7 grants individuals privacy rights in their life, home and communications;\textsuperscript{145} and (4) Article 8 grants individuals a right to the protection of personal data, which must be processed fairly, with consent of the person concerned and for some legitimate basis.\textsuperscript{146}

Guided by the individual-based rights above, the European Parliament\textsuperscript{147} issued Directive 95/46/EC\textsuperscript{148} outlining the EU’s position on the protection of the individual concerning the processing of personal data and the movement of that data.\textsuperscript{149} EU directives are designed to establish specific objectives that the laws of the member states must facilitate. Member states satisfy the directives by designing laws that ensure the objectives are reached within their borders.\textsuperscript{150} The objective of Directive 95/46/EC is to strengthen the protections to a person’s "fundamental rights and freedoms, notably the right to privacy," in regard to the processing of personal data.\textsuperscript{151}

B. The Data Protection Act\textsuperscript{152}

The Data Protection Act of 1998\textsuperscript{153} gives EU Directive 95/46/EC legal effect inside the United Kingdom. Abiding by the

\begin{itemize}
\item \textsuperscript{143} Id. at 364/9.
\item \textsuperscript{144} Id.
\item \textsuperscript{145} Id. at 364/10.
\item \textsuperscript{146} Id.
\item \textsuperscript{147} The European Parliament is elected every five years by the people of Europe to represent their interests and is made up of 785 members from all twenty-seven EU countries. The European Parliament’s main function is to pass European laws, a role it shares with the Council of the European Union and the European Commission. Parliament also shares joint responsibility for approving the EU’s annual budget. The Parliament elects the European Ombudsman, who investigates citizens’ complaints regarding maladministration by the EU institutions. See Europa, Panorama of the European Union, http://europa.eu.int/abc/panorama/index_en.htm (last visited Feb. 14, 2007) for more information on the organization and institutions of the European Union, including the European Parliament.
\item \textsuperscript{149} Directive 95/46/EC can be found at http://www.cdt.org/privacy/eudirective/EU_Directive_.html (last visited Oct. 15, 2005).
\item \textsuperscript{152} Data Protection Act 1998, c. 29 (Eng.).
\item Id.
\end{itemize}
Charter of Fundamental Rights and the EU Directive, the UK law focuses upon the rights of the individual rather than the interests of another party. The DPA accomplishes this by way of eight Data Protection Principles. These eight principles work as guidelines that regulate the type, extent, and form of data processing, as well as the uses of the processed data. They are as follows:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless—
   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

The DPA refers to those whose data is being processed or monitored as “data subjects” and labels those controlling the data processing as “data controllers.” For the purposes of the DPA, the term “data” is applicable to a broad range of situations. In its broadest sense, it means information processed by automatic

154. Id. at Schedule 1.
155. Id. at Schedule 1, Part I.
156. Id. at Part I.1.
equipment or recorded as part of a relevant filing system.\textsuperscript{157} The relevant filing system refers to a set of information that specifically relates to an individual or his criteria.\textsuperscript{158} A more specific form of "data" under the DPA is personal data. Personal data is data relating to an individual who can be identified from that data.\textsuperscript{159} The definition of the term also includes any expression of opinion about the individual and any indication of the intentions of the data controller.\textsuperscript{160} A more specific and the most protected form of data under the DPA is sensitive personal data.\textsuperscript{161} This form of data is defined as data that pertains to racial origins, political opinions, religious beliefs, membership in a trade union, sexual life, physical or mental health, and allegation or commission of a crime.\textsuperscript{162}

In order to comply with the DPA, a data controller must take the necessary steps to ensure that processing does not violate any one of the eight Data Protection Principles. Each individual principle builds upon the protections afforded under its predecessors, resulting in an inter-reliant protective framework.

The first principle regulates exactly when electronic processing can take place. This principle on the whole requires that "data shall be processed fairly and lawfully."\textsuperscript{163} Additional DPA provisions clarify that "fairly" means that the data subject is supplied with the identity of the data controller, the purpose for the processing, and any other information that is relevant to the specific circumstances of the processing.\textsuperscript{164} The DPA also requires that, in determining fairness, the method of processing must also be considered.\textsuperscript{165}

In addition to the obligatory degree of fairness, the first principle provides two sets of "conditions" that must be present in order for processing to take place. The first set of "conditions" permits processing when any one of the following is present: (1) the data subject consents; (2) processing is necessary in performance of a contract; (3) processing is necessary to comply with a legal obligation; or (4) processing is necessary to protect the vital interests of the data subject.\textsuperscript{166} The second set of "conditions" that permit processing only arise when the data being processed is

\begin{itemize}
\item \textsuperscript{157} Id.
\item \textsuperscript{158} Id.
\item \textsuperscript{159} Id.
\item \textsuperscript{160} Id.
\item \textsuperscript{161} Id.
\item \textsuperscript{162} Id.
\item \textsuperscript{163} Id. at Schedule 1, Part I.1.
\item \textsuperscript{164} Id. at Schedule 1, Part II.2(3).
\item \textsuperscript{165} Id. at Schedule 1, Part II.1(1).
\item \textsuperscript{166} Id. at Schedule 2.1–5.
\end{itemize}
When processing sensitive personal data, the first principle requires that a condition from part (a) be accompanied by the data subject’s explicit consent and that the processing be necessary for the protection of the data subject or others. When processing sensitive personal data, the first principle requires that a condition from part (a) be accompanied by the data subject’s explicit consent and that the processing be necessary for the protection of the data subject or others. The DPA also permits processing when a government entity or an employer obtains a judicial order compelling processing. Processing is also allowed if the data controller can demonstrate that there is an urgent legitimate issue. While this appears to operate in the same way as the ECPA’s legitimate business purpose exception, it is not the same. Application of this condition is preempted if any unwarranted prejudice to the data subject’s rights or freedoms occurs.

The second principle limits the range and scope of processing by allowing processing only for specified purposes that are communicated to the data subject. This works to prevent data controllers from engaging in continuous or random monitoring. Principles three through five regulate the quality, duration, and security of the data legally obtained by the data controller, primarily ensuring that the data remains accurate and relevant.

The sixth principle, illustrating the DPA’s emphasis on the individual, demands that processing be in accordance with the “rights of the data subject.” DPA protections grant the individual a broad range of rights, most importantly, entitlement to notification from the data controller when data processing is going to take place and for what purposes. The data subject also has the right to demand that the data controller prevent or stop processing that is likely to cause substantial damage or distress to the data subject or another. A data subject may also prevent a data controller from making a decision based solely upon the processed data if that decision significantly affects the data subject. However, this right to contest a data controller’s

167. Id. at Schedule 1, Part I.1. See source cited supra note 152 for a description of sensitive personal data.
168. Id. at Schedule 3.1–10.
169. Id. at Schedule 2.6.
170. Id.
171. Id. at Schedule 1, Part I.2 and Schedule 1, Part I.5.
172. Id. at Schedule 1, Part I.3–5.
173. Id. at Schedule 1, Part I.6.
174. Id. at Part II.7.
175. Id. at Part II.10.
176. Id. at Part II.12(1).
decision might be exempted if the decision is related to a contractual obligation.\footnote{Id. at Part II.12(6), (7).}

The seventh principle requires precautionary measures that will prevent unauthorized processing and damage to the personal data of any individual.\footnote{Id. at Schedule 1, Part I.7.} The final principle prevents transmission of data into countries whose laws afford fewer protections than those required by the EU Directive.\footnote{Id. at Schedule 1, Part I.8.} In its current state, the U.S. law is classified as a country with fewer protections, meaning that personal data within the United Kingdom should be prohibited from being transmitted to the United States.\footnote{See EU and U.S. “Safe Harbor” Plan, http://www.export.gov/safeharbor/.html, for more information on the prohibition of data transfers from the European Union to the United States. This subject is complicated and its scope extends beyond the focus of this comment.}

C. The Battle of the Acronyms: The DPA v. the ECPA

Juxtaposed against the Electronic Communications Privacy Act, the Data Protection Act proves to be a better body of law in every aspect. The terminology, framework, and provisions are easily applicable to any setting where data processing creates conflicts between the rights of the individual and a larger entity—whether that be the government, a third party, or an employer. In a workplace context, the DPA is better suited to protecting the privacy interests of the employee while ensuring that the employer is not stripped of the ability to protect his interests.

The principal difference in the two bodies of law results from divergent foundational origins. The ECPA is grounded in the U.S.’s property-based outlook on privacy while the DPA approaches privacy as a component of human dignity. These contrasting tenets create legal schemes that protect completely different entities: the employer under the ECPA and the individual under the DPA. As aforementioned,\footnote{See infra Part II.B for discussion of notions and concepts of privacy.} the U.S.’s property-based approach needs to be replaced by a concept centered upon the individual. What better way to accomplish this than to enact law that is rooted in “plac[ing] the individual at the heart of its activities”\footnote{Charter of Fundamental Rights of the European Union, 2000/C 364/01, 364/8 (Dec. 18, 2000).} and grants the individual legal rights that can be asserted to protect his privacy?\footnote{See generally Data Protection Act 1998, c. 29, Part II, §§ 7–15 (Eng.).}
The principal flaw of the ECPA is a dual construction that provides, at best, piecemeal protection and is largely known by courts as complex and convoluted. Alternatively, the DPA is comprehensive, clear, and easily applied to the circumstances it was designed to regulate. Under the ECPA, a party has to worry about what is or is not an electronic communication, whether it is being transmitted or stored, and then determine if any of the exceptions apply to the situation. Under the DPA, parties only have to determine if "data" is being processed and then apply that processing to the structure of the eight Data Protection Principles. Additionally, the DPA's "data subject" and "data controller" are more efficient and clear characterizations of the possible parties involved.

In regard to protecting the individual, there is almost no comparison. At the most basic level, the ECPA fails to refer to privacy or the rights of the individual, while the DPA constantly mentions and focuses on privacy throughout the body of law. The DPA also requires compliance with eight principles that are collectively geared to protecting the rights and freedoms of the data subject. Given the restrictive effect of the statutory exceptions, the ECPA's protections rarely extend to the individual. In the workplace, the exceptions cause the ECPA to be ineffective in protecting the employee, while the DPA grants rights to the data subject that can be used to combat invasive employer monitoring—the most progressive right being the ability to challenge a data controller's decision made pursuant to the processing. The provision even refers to a data subject's "performance at work" as one of the challengeable "decisions."

The two main benefits under the DPA that are non-existent under the ECPA are: (1) the notice requirement; and (2) increased protections for "sensitive personal data." Expecting notice prior to processing is a small investment that provides a huge return in employee privacy. Notification also fairly balances and represents the interests of employer and employee alike. Notifying the employee removes a substantial portion of the invasive nature of secretive monitoring, which generates the most privacy concerns. Furthermore, notification does not impose a substantial burden on

---


185. Data Protection Act 1998, c. 29, Part II.12(1) (Eng.).

186. Id. at Part I.1.
employers nor does it diminish their ability to protect themselves, their business, and their facilities.

Heightened requisite protections for sensitive personal data are ideal for protecting the privacy of the individual—primarily because this type of information will most likely be the "thoughts, sentiments, and emotions" that Warren and Brandeis endeavored to protect. 187 Additionally, this distinction between types of data further reconciles the privacy interests of the employee with the interests of the employer. Increasing protections for data likely to involve personal privacy concerns of the employee does not rob employers of their ability to protect interests of a more direct business nature.

Another benefit of adopting similar DPA legislation is that the United States will no longer be concerned with the European Union ban on transmitting data into countries whose protection schemes are found to be inadequate. 188 Lagging behind the European Union in this domain erects needless obstacles that interfere with international commerce and relationships. Additionally, it is irresponsible for the United States to continue to allow laws enacted in 1986 to regulate 2007 technology. A body of law drafted only nine years ago is able to respond and adapt to changes in modern technology in ways that a twenty-year-old law could never envision.

The DPA is founded upon the correct notions of privacy and the provisions have a superior structure, are unambiguous, and more conducive to the protection of the rights of the individual. Thomas Jefferson believed that the people revert to government in order to secure their rights, 189 thus, the United States needs to adopt a body of law that adequately protects its citizens' rights. The United States needs to look no further than the European Union and the United Kingdom for a model of what steps to take.

188. Council Directive 95/46, 1995 O.J. (L 281) Ch. 4, art. 25, Principles 1–6 (EU). Article 25(1) states that "Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection." Id. Under the Data Protection Act, this portion of the EU Directive is complied with through the eighth Data Protection Principle: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data." Data Protection Act 1998, c. 29, Schedule 1, Part I (Eng.). See also EU and U.S. "Safe Harbor" Plan, http://www.export.gov/safeharbor/html, for an informal explanation of the ban and its effects upon the United States, including certain steps taken to create methods for data exchange between the European Union and the United States.

189. See source cited supra note 130 and accompanying text.
The Data Protection Act protects the rights and freedoms of the individual, and the United States should enact legislation which emulates that specific body of law.

V. CONCLUSION

The technology of the Internet and e-mail has drastically reshaped the concept of privacy that began over a century ago. Allegedly, the right to privacy was recognized to better protect the rights of the individual in light of social and economic demands. Regrettably, legislators seem to have forgotten this fact when regulating the employee/employer relationship as it relates to e-mail. Workplace privacy, under existing legal privacy protections, is a quintessential misnomer. From tort law to federal law to state law, an employer is permitted to indiscriminately monitor employee e-mail use without regard to employee privacy.

Warren and Brandeis singled out "recent inventions and business methods" as threats to individual autonomy that warranted a specific recognition of the right to privacy. Today, e-mail and workplace monitoring have developed into urgent individual privacy threats, but, to date, have been largely ignored. The law in effect distinctly favors the employer while ignoring the employee's right to privacy; therefore, steps need to be taken in order to keep an individual's right to privacy intact. The best venue for protecting privacy in the electronic workplace is through federal legislation. At present, the twenty-year-old federal legislation is antiquated, inept, and confusing; thus, an ideal setting for development exists.

The "next step" in protecting the rights of the individual is for the United States to abandon the federal Electronic Communications Privacy Act and enact legislation modeled after the UK's Data Protection Act. For the past twenty years, privacy protections within the United States have remained stationary while the European Union and the United Kingdom have transformed and modernized their approaches. Congress must take action; protecting the rights of individuals is a progressive endeavor that must keep pace with the times.

Ray Lewis*

---

190. Warren & Brandeis, supra note 2, at 193.
191. Id. at 195.
192. Id.

* I would like to thank my family for its support and, most importantly, Professor John M. Church for his comments, editing, and guidance during the writing and production of this comment.