August 2007

Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity

Laura Evans

Follow this and additional works at: https://scholarship.law.berkeley.edu/californialawreview

Recommended Citation

Link to publisher version (DOI)
https://doi.org/10.15779/Z384D88

This Article is brought to you for free and open access by the California Law Review at Berkeley Law Scholarship Repository. It has been accepted for inclusion in California Law Review by an authorized administrator of Berkeley Law Scholarship Repository. For more information, please contact jcera@law.berkeley.edu.
Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?

Laura Evans†

INTRODUCTION

In an article summarizing privacy law in the American workplace, noted privacy law scholar Matthew Finkin painted a dramatic picture of the surveillance under which many American employees work. For example, he cited a 2001 American Management Association study showing that nearly 80% of the large employers surveyed, who together employ as many as one out of four American workers, listened to employees’ phone conversations and voice mail, and monitored electronic files and email. Finkin quoted the Privacy Foundation’s statistic that 34% of workers are monitored continuously with regard to their email and Internet usage. However, Finkin also pointed
out a study published in 1999, which found that one in three workers surf the internet for personal interests during working hours. Finkin’s article reveals the tension between employers’ interest in controlling the work environment and employees’ interest in privacy. Further, the article exposes the problem of employers using data gathered about employees for one purpose and inappropriately using it for another purpose. This problem could lead, for example, to the creation of employee profiles that employers can use in ways that invade employees’ privacy.

The problem of employee privacy and productivity becomes more significant as the boundaries between formal and informal places of work blur. For example, employers may permit employees to take laptop computers outside of the formal workplace to enable the employee to quickly respond to customer needs, or give such computers to salaried employees with the understanding that they might put them to personal use, as well as use them for work. Such an arrangement could lead to employees’ personal data being stored on employers’ property. The employer could claim a right to all data on the computer and potentially use what was private data, created outside the workplace, for any number of purposes, including as a justification for the employee’s termination. The employer could also use employees’ information to discriminate against employees should the data reveal personal attributes that the employer does not like. Additionally, the employer could create profiles about employees’ spending habits or personal interests, which could be used internally or sold externally for marketing purposes. With sophisticated technology becoming more widely available, the tension between employers and employees’ interests is likely to increase significantly.

Currently, U.S. employment law does not sufficiently regulate employers’ collection and use of private data about employees. This Comment suggests that certain parameters of European Union (EU) law and English law could be integrated into interpretations of enacted state privacy legislation, as well as into future federal legislation. At a minimum, where courts give employers a conditional privilege to monitor employees and use private employee information in the “ordinary course of . . . business” under the Electronic Communications Privacy Act (ECPA), courts could incorporate specific standards in precedent English law to establish employees’ right to know about

4. Id. (citing Surf Watch (June 4, 1999)). The situation facing employers has grown increasingly complex as modern advances in information technology have revolutionized the workplace, introducing a plethora of new opportunities for employee misbehavior. See, e.g., Vivien K. G. Lim, The IT way of Loafing on the Job: Cyberloafing, Neutralizing, and Organizational Justice, 23 J. ORGANIZATIONAL BEHAV. 675 (2002).

data collection, as well as the requirements of relevance, quality, proportionality, and finality for the use of the data.6

Part I of this Comment begins by discussing the impact of the development of recent technology on employee privacy and then gives a brief overview of some of the current privacy law in the United States as it impacts employment law and practices. It follows with an argument that courts may interpret recently-enacted state laws and future comprehensive federal legislation in accordance with the ECPA and its common law doctrines, thereby giving expansive rights to employers without addressing the privacy rights of employees. Next, Part II of the Comment discusses English law to identify an alternative to current American doctrine. A discussion follows as to the feasibility of adopting at least portions of English privacy law. Finally, Part III sets forth a proposal for the interpretation of new and future privacy statutes in the United States.

I
NEW TECHNOLOGY, CURRENT U.S. PRIVACY LAW, AND THE WORKPLACE

Part I starts with a description of the impact new technology may have on employee privacy. It then gives an overview of current U.S. regulations of employee privacy in the workplace. The discussion of current U.S. law begins with a description of the privacy protections provided by the common law, then continues with a discussion of federal and state legislation. Finally, Part I examines whether, in the context of employers' needs to promote productivity, current law sufficiently protects the privacy needs of employees and concludes that technology has changed the workplace to the extent that new law is needed to protect employee privacy.

6. These standards come from the Data Protection Act, 1998, c. 29, sched. 1, part I (Eng.):

"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 organisational measures shall be taken against unauthorised 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." See infra Part II.A.2 for a full discussion.
A. The "New" in New Technology

Several recent technological developments increase employers' ability to monitor and collect data about employees. In the end, these developments are persuasive evidence for a new doctrine in American employee privacy law that accounts for new technology.

One technological development is employers' ability to collect what has been termed "clickstream data," which is a record of each click made with a computer's mouse. Clickstream data differs from "transaction data," which only includes information about a communication (for example, who made the call, the day and time it was made, or who made an electronic payment and when). Clickstream data is novel because it makes enormous amounts of individual information available and removes the difficulty of compiling many otherwise separate pieces of information. Assembling these pieces of data can "reveal patterns of behavior, profiles, and an intimate slice of the lives of individuals, which can be used to categorize and segregate individuals in society."

Employee monitoring can also be conducted in other ways that were not possible until very recently. For example, some cellular telephones have built-in global positioning systems that enable employers to track the physical location of employees at all times. Thus, employers can now track every physical and electronic move an employee makes. Furthermore, employers now conduct their own private investigations into employment applicants, partly because of the reluctance of former employers to give references. So, instead, employers collect information about prospective employees from driving records, vehicle registration records, bankruptcy proceedings, Social Security records, property ownership records, military records, sex offender lists, incarceration records, drug testing records, professional licensing records, workers' compensation records, and credit reports. They can collect as much information as possible from former employers as well as from other people.

7. For further discussion of technology-related threats to employee privacy, see Michael Baroni, Employee Privacy in the High-tech World, 48 ORANGE COUNTY LAWYER 18 (May 2006) (discussing, for example, "spy-cams" and bugging).
8. See Reidenberg, infra note 26, at 1320.
9. Id.
10. Id. at 1322.
11. Id. at 1323.
13. See, e.g., STEVEN L. WILLBORN ET AL., EMPLOYMENT LAW: CASES AND MATERIALS 343 (3d ed. 2002) (discussing reluctance of employers to give references); Elizabeth Millard, Online Background Checks, 93 A.B.A. J. 37, 37 (2007) (discussing how employers search "profiles, blogs, and visible chat sessions" as part of employee background checks).
like coworkers, friends, and neighbors of prospective employees. Employers also may take advantage of the wealth of information available online about job candidates. These investigations can provide employers with far more information about their employees than traditional references. One especially new source of information on employees is the so-called “blog,” which can provide employers with a great deal of insight into potential employees and may actually expose current employees’ breaches of the duty of loyalty to employers.

Finally, the changing market for personal data affects the balance of employers’ and employees’ needs with regard to workplace privacy. One scholar argues that individual data has become a commodity that some large companies collect and invest in; the increasing financial value of this information has risen to the level of a corporate asset. Commodification of this information has become possible because electronic records in large databases provide affordable access to information needed on prospective employees. In turn, this builds “tremendous commercial pressures in favor of unanticipated or secondary uses” of personal information. Thus, the data collected by employers in the methods discussed above are vulnerable when profit-seeking companies lack legal limitations on their use of that information.

Employers may also threaten employees’ privacy rights through the use of other new, non-electronic technology. For example, employers may use genetic testing, personality testing, and predictive testing as tools to assess the performance and potential performance of employees. Employers also can

15. Id. at 187.
16. See, e.g., Erin Binns, What Does the Web Say About You?, 35 STUDENT LAW. 16, 16 (2007) (“In a recent poll conducted by the National Association for Law Placement, 85 percent of respondent employers admitted to using search engines and social networking sites like MySpace and Facebook to research candidates.”).
20. Reidenberg, Resolving Conflicting International Data, infra note 26, at 1324.
use credit reporting, physical surveillance, and drug testing on current and potential employees—all tools that may lead to the invasion of employees’ privacy. While this Comment emphasizes the threat newer electronic technologies pose, other scholars have detailed potential threats posed by these non-electronic threats.

Given these changes in technology, electronic or otherwise, does current U.S. privacy law sufficiently protect employees’ privacy?

B. Brief Overview of American Privacy Law and the Workplace

There is no comprehensive federal law on either privacy or employers’ use of private employee information. In fact, one scholar has written: “[N]o successful standards, legal or otherwise, exist in the United States for limiting the collection and utilization of personal data in cyberspace.” Instead, U.S. privacy law is a combination of statutory and common law; however, there is no specific legislation governing the collection of data about employees. The U.S.’s approach to privacy law is sectoral, with government intervention in only limited areas, compared to the approach of other countries.

I. Common Law

Several torts touch upon aspects of privacy, including defamation; intentional and negligent infliction of emotional distress; and intrusion upon seclusion. These and other privacy-related torts have developed through


23. See, e.g., King et al, supra note 21; Mulvihill, supra note 21; Steinforth, supra note 21; Rachinsky, supra note 21; Lorenz, supra note 21; Sismondo, supra note 21; O’Gorman, supra note 22; Gallagher, supra note 22; Kim, supra note 22.


25. See Finkin, Information Technology, supra note 1, at 472.

26. See Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 STAN. L. REV. 1315, 1331 (2000) (arguing that “[l]egal rules are relegated to narrowly targeted sectoral protections,” and providing an example of privacy protections in video rental but not in online streaming video) [hereinafter Reidenberg, Resolving Conflicting International Data].

27. See Finkin, Information Technology, supra note 1, at 472.
common law over the years, as the torts most closely linked to the core issues of this Comment. Thus, while this section discusses the common law of privacy generally, it focuses on the privacy torts most relevant in the employment context.

Invasion of privacy includes four types of invasion: "1) Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs. 2) Public disclosure of embarrassing private facts about the plaintiff. 3) Publicity which places the plaintiff in a false light in the public eye. 4) Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness."28 The Restatement (Second) of Torts defines intrusion upon seclusion as "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."29

While there is significant case law dealing with invasion of privacy in various circumstances, there are not many cases addressing an employer’s use of an employee’s data under the tort of inclusion into intrusion, or in general. The few cases dealing with these issues illustrate the courts’ reluctance to protect employees’ privacy. For example, in Smyth v. Pillsbury Co., a man sued his employer after he was fired for sending “inappropriate and unprofessional comments” over the employer’s email system, in spite of the fact that his employer told him that his email was confidential.30 The court granted the employer’s motion to dismiss, finding that a reasonable person would not think the interception of the email “highly offensive.”31 The court did not see the employer’s actions as analogous to drug testing or personal property search cases, which require “the employee to disclose . . . personal information about himself” and invade “the employee’s person or personal effect,” and found that the employer had a strong interest in constraining employees from such inappropriate and unprofessional emails.32 Thus, the court sided with the employer’s needs rather than the employee’s privacy interests.

In another case, Garrity v. John Hancock Mutual Life Insurance Co., the employer terminated three employees for receiving and forwarding to other employees emails with sexual content on their work computers.33 The fired employees presumed their emails were private, in part because their employer had showed them how to create private folders with passwords.34 The court found this to be an unreasonable expectation of privacy because they knew

31. Id. at 101.
32. Id.
34. Id. at *3–6.
their employer could look at their intranet email, they were aware that their emails might be forwarded, and the employer had a legitimate business reason to review the email, specifically to protect other employees from harassment. Again, the court focused on the employer’s interests rather than the employee’s privacy.

Likewise, in Zinda v. Louisiana Pacific Corp., an employee sued for invasion of privacy and defamation after his employer fired him for allegedly falsifying his employment application form; the employee had failed to disclose a back injury he received at home. The employer found out about the injury after the employee sued the employer, the manufacturer of the faulty roofing materials, for causing that injury. The employer distributed a company newsletter that listed the falsification of employment application forms as the reason he was fired. The employee asserted that the distribution of the newsletter, especially outside the workplace, was an invasion of his privacy. More specifically, the employee characterized the newsletter as “public disclosure of private facts,” because it offensively revealed sensitive information about him that was private: the reason he was fired. The court overturned the lower court’s finding as a matter of law that the employer had abused a common interest privilege, finding instead that it was a matter for the jury to determine if the employer had abused its privilege after it had published the reason the employee was terminated. The court thus allowed the jury to give more effect to the employer’s interests.

In Hines v. Arkansas Louisiana Gas Co., an employee also sued for defamation and invasion of privacy after his employer fired him based on an investigation showing the employee’s use of inappropriate language with subordinates. The reason for the employee’s firing was leaked. A jury found the corporation invaded the employee’s privacy “by placing him in a false light before the public and unreasonably disclosing private embarrassing facts about him to the public.” Nevertheless, the court reversed the jury’s verdict in favor of the plaintiff, finding that the employer’s privilege to investigate complaints protected it from former employees’ privacy claims.

These cases demonstrate courts’ reluctance to interfere with employer actions in common law privacy cases. As of the present time, the courts have frequently found the balance of interests to fall in favor of the employer.

35. Id.
37. Id. at 550.
38. Id. at 550–551.
39. Id. at 555 (The employee asserted that this was “[p]ublicity given to a matter concerning the private life of another, of a kind highly offensive to a reasonable person.”).
40. Id. at 553–54.
42. Id. at 649.
43. Id. at 658.
2. Legislation

a. Federal

In the United States, federal legislation addressing privacy has been largely sectoral. Congress has passed a number of federal statutes that protect the privacy of citizens from particular intrusions, but there is currently no overarching federal law on privacy in either the workplace or on privacy in generally.

One example of a statute that provides narrow protection is the Video Privacy Protection Act.\(^4\) The Act provides for a civil remedy, including compensatory and punitive damages, attorneys’ fees, and other equitable remedies as appropriate, should a videotape service provider disclose personally identifiable information to anyone outside certain permitted exceptions.\(^5\) Similarly, the Health Insurance Portability and Accountability Act (HIPPA) makes it a criminal offense to obtain or disclose personally identifiable health information relating to an individual.\(^6\) Another example is the Family Educational Rights and Privacy Act (FERPA), which, broadly speaking, protects the privacy of students by restricting federal funding to those educational agencies that do not allow “the release of . . . personally identifiable information” absent parental consent (or student consent, if the student is over eighteen), except in limited circumstances.\(^7\) The Americans with Disabilities Act (ADA) also requires that information collected about the health of employees be kept separately and confidentially.\(^8\)

Other federal legislation includes the Fair Credit Reporting Act, which requires credit-reporting agencies to use procedures that respect the privacy of consumers.\(^9\) Additionally, the Federal Trade Commission ("FTC") may impose a general duty to protect information by means of the Federal Trade Commission Act.\(^10\) For example, the FTC has brought at least one action against a company, DSW, saying that the company’s lack of data security was an unfair business practice.\(^11\) However, the FTC is not known for a proactive approach in protecting the information of prospective employees. A recent article quoted a Federal Trade Commission lawyer as saying that United States

\(^{7}\) 20 U.S.C. § 1232g(b) (2006).
\(^{11}\) See id. ("[T]he FTC ... claim[ed] that the alleged lack of security constituted an unfair business practice under the FTC Act, which in turn led to the FTC seeking significant sanctions against the company").
v. Imperial Palace, Inc., might "be the only pre-employment screening enforcement action ever taken by the agency."

Perhaps the most well known and most litigated statute concerning privacy is the Electronic Communications Privacy Act (ECPA). The Act proscribes, with certain exceptions, the interception and disclosure of wire, oral, or electronic communications. The Act also prohibits accessing stored communications without authorization. This statute is of particular importance because to employees since many employers monitor employees' communications at work. Thus, a short discussion of some of the case law interpreting the statute follows.

While at common law courts have been lenient with employers, under the ECPA the mere citation of a business reason for invading a person's privacy has not always been enough to justify interception. There have not been many cases to date dealing with employers monitoring employees' computer use, but case law interpreting interception of telephone conversations is instructive because it is likely to be similarly applied to electronic communications. For instance, the Sanders v. Robert Bosch Corp. court found that the business-use exception did not apply to the taping of phone calls by a security office, in spite of bomb threats made to the office, because it did not further the security office's business and the security guards could have been informed of the recording. In Adams v. City of Battle Creek the court also found that the ECPA's business-use and law-enforcement exceptions did not permit the City to tap a police officer's pager because the officer had no notice of the monitoring. This business-extension exception has, in fact, been a frequent issue of contention.

Sometimes, claims under both common law and statutes are made in the same cases. For example, in Fischer v. Mt. Olive Lutheran Church, the court

57. See Finkin, Information Technology, supra note 1, at 480.
58. 38 F.3d 736, 738, 740 (4th Cir. 1994) (finding that to meet the business-use exception of the EPCA, the business should have had the telephone line installed in the ordinary course of business and have used the line in the ordinary course of business).
59. 250 F.3d 980, 984 (6th Cir. 2001).
60. See, e.g., Berry v. Funk, 146 F.3d 1003 (D.C. Cir. 1998) (allowing a State Department employee to avoid summary judgment for factual development on the business-extension exception and other exceptions); Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553, 559 (2d Cir. 2000) (finding legitimate business reason for interception because of industry custom of recording all telephone calls to and from business).
61. See discussion infra Part (I)(A)(2)(b) for more on state statutory claims.
found that the defendant church did not have a legitimate business reason for taping a minister’s telephone conversation. The church asserted that the telephone conversation, which was sexually explicit in nature, was conducted in the minister’s job function because it may have included counseling. The court found that the church’s access and obtainment of the minister’s emails was an act that the jury could find to be in violation of the Electronic Communication Storage Act (ECSA). Summary judgment was thus not allowed on either ESCA or the ECPA claims.

One of the few cases that specifically involved electronic communications is *Konop v. Hawaiian Airlines, Inc.* There, a pilot sued an employer airline for accessing his personal website by using other pilots’ passwords. The court held that the employer airline did not violate the Wiretap Act (one portion of the ECPA) because the website was statically stored electronically, and thus an interception had not taken place. But the court also held that the airline might have violated the ECSA (the other portion of the ECPA) because the other pilots whose passwords it used may not have actually used the website, and thus the court reversed summary judgment in favor of the employee. The court thus chose a narrow, formal application of the statute, which unfortunately may not provide much guidance in other situations.

However, other cases have begun to address the issue of electronic monitoring more directly. In *Thygeson v. U.S. Bancorp* the plaintiff made a variety of claims against his employer after his employer fired him for excessive and inappropriate Internet use during work. The court dismissed the employee’s invasion of privacy claim because the employer had a clear policy prohibiting personal use of office computers. The intrusion was reasonable in spite of the fact that the employee labeled the folder in question “personal.” With regard to the plaintiff’s Internet usage, the court distinguished this case from the above-discussed *Fischer* case because, unlike in *Fischer*, the employer did not access plaintiff’s email; the employer had the express policy of monitoring computer usage; and the plaintiff could not expect privacy in regard to the Internet addresses—as opposed to the content—monitored. Thus, the ordinary course of business rationale for invading an employee’s privacy may be more readily recognized where an employee knows or should know that the employer is actively monitoring the employee. In this

---

63. Id.
64. Id. at 925–926.
65. Id. at 930–31.
66. 302 F.3d 868 (9th Cir. 2002).
67. Id. at 872.
68. Id. at 878, 880.
70. Id. at 72–73.
71. Id. at 74–75.
way, Thygeson shows the U.S. courts' tendency to find sufficient notice in instances where an employer does not actively or continuously monitor employee action and has implied that privacy exists where it may not.\textsuperscript{72}

\textit{b. State}

A number of states also have legislation on privacy and, more specifically, employee privacy. California has a right to privacy embedded in its constitution that applies to private as well as public actors.\textsuperscript{73} On the other hand, a California bill that would have mandated that employers give notice to employees of electronic monitoring was vetoed three times.\textsuperscript{74} Massachusetts also has a statute providing a limited right to privacy: "A person shall have a right against unreasonable, substantial or serious interference with his privacy."\textsuperscript{75} Connecticut's statute is more specific by requiring employers to give notice, which may be accomplished through a general posting prior to monitoring employees electronically.\textsuperscript{76} This law provides for a civil penalty, but allows an exception for the criminal investigation of an employee.\textsuperscript{77} Likewise, a Delaware law requires employers to give employees daily electronic notice or a general written notice signed by the employee prior to monitoring employees' phone, email, or Internet usage.\textsuperscript{78} Finally, Florida has a statute that is similar to the federal EPCA that limits the interception and disclosure of communications.\textsuperscript{79}

Beyond regulations about general privacy, at least eighteen states have laws that permit employees to see their personnel files and many permit the inclusion of a record of an employee's disagreement with the information contained in the file.\textsuperscript{80} Far fewer states have statutes that limit the use of data

\textsuperscript{72} This is not the case elsewhere. For example, in contrast, in England, notice may not suffice if an employer's practices do not reflect written policy. See Mark Jeffery, \textit{Information Technology and Workers' Privacy: The English Law}, 23 COMP. LAB. L. & POL'Y J. 301, 333 (2002) ("[E]ven where employees have been clearly notified that computer monitoring may occur, if the employer does not carry out such monitoring in practice then the employees will have been led to believe that their privacy will be respected and so a further warning will be necessary before the employer may lawfully start monitoring.").

\textsuperscript{73} CAL. CONST. art. 1, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are ... privacy."). For cases interpreting the article, see, e.g., TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155 (Ct. App. 2002), where the court allowed employer to use evidence of employees' access of porn sites on work computer used at home in wrongful termination suit, and Barbee v. Household Auto. Fin. Corp., 6 Cal. Rptr. 3d (Ct. App. 2003), where the court found an employee did not have a privacy interest with regard to romantic relationships.

\textsuperscript{74} See Finkin, \textit{Information Technology}, supra note 1, at 477 note 36.

\textsuperscript{75} MASS. GEN. LAWS ch. 214, § 1B (2005).

\textsuperscript{76} CONN. GEN. STAT. § 31-48d(b) (2006).

\textsuperscript{77} CONN. GEN. STAT. § 31-48d(c)-(d) (2006).

\textsuperscript{78} DEL. CODE ANN. tit. 19, § 705(b) (2006).

\textsuperscript{79} Security of Communications Act, FLA. STAT. § 934.03 (2007).

\textsuperscript{80} See Finkin, \textit{Information Technology}, supra note 1, at 492.
employers collect about employees. Michigan prohibits an employer from compiling information about “an employee’s associations, political activities, publications, or communications of nonemployment activities,” unless the employee provides the information in writing, gives written permission to such compilation, or the activity occurs at or during work. The only other state with such a protective statute is Illinois. The Illinois statute is almost identical to the Michigan statute, except that there are two additional exceptions for information gathered when the employee is acting criminally or in a manner that might hurt the employer, including when the employee’s actions may make the employer susceptible to liability.

Many of the state statutes were passed relatively recently, and few have been interpreted by case law. In the future, however, courts may interpret state legislation largely using ECPA and common law doctrine, thereby giving expansive rights to employers under the exception that allows monitoring and use of information in the ordinary course of business. No matter how courts ultimately interpret the state statutes, a comprehensive federal statute regulating employer use of employee data and employee privacy in the workplace does not exist.

C. Is Change Needed?

It is possible that the piecemeal and sectoral approach used in the United States has balanced the tension between employers’ needs to monitor employees and employees’ privacy needs. However, is it more likely that new technology is changing the balance of power between employers and employees to such an extent that a new system of regulation is needed in the United States?

There are at least three possibilities concerning the status of employees’ privacy. First, the current system may have sufficed for previous technology and may still suffice despite new technology. Under this view, it is arguable that “the law does not perceive of one’s conduct on the job as a ‘private’ matter; and not being subject to any notion of ‘the private,’ the additional features of technology that make it more pervasive, all-seeing and all-knowing, never forgetting (or forgiving), become legally irrelevant.” Or, doctrine may not need to change because the nature of the problem does not differ, despite change in the tools available for employers. Thus, new technology may

82. 820 ILL. COMP. STAT. 40/9 (2005).
83. Id.
84. A March of 2006 shepardization of the statutes revealed numerous cases interpreting the Massachusetts statute and to a certain extent the Florida statute, but none interpreting the Connecticut, Delaware, Illinois, or Michigan statutes, for example.
85. Finkin, Information Technology, supra note 1, at 503–04.
86. See Jeffery, supra note 72, at 335–37.
require legal limitations on employers’ use of these tools, but not to changes in the underlying doctrine. 87

According to a second view, the current system has not sufficiently regulated employer’s use of previous technology, nor will it suffice for new technology. Proponents of this view believe that employee privacy has never been adequately protected.

Finally, the current system may have sufficed for previous technology, but will not suffice for new technology. With regard to this last possibility, some academics have posited that new technology has so “changed the fundamental nature and terms of the debates about surveillance at work and about the processing of personal data about workers” that the old system is no longer sufficient. 88

While some may argue that employee privacy issues remain the same and that only the tools available for employers to monitor and collect data about employees have changed, the new tools described at the beginning of this Part are very powerful and tilt the balance of power towards employers. Whether employers simply should be restricted from using these tools to their full extent or whether the new technology is sufficiently different from the old technology to justify new law altogether, some additional controls should be placed on employer action in the workplace in either case. Regardless of where one falls in the debate, new insight into employee privacy may be helpful in shaping the future of employee privacy law. Developments in English and European Union legal thought on employee privacy can instruct American lawmakers as they cope with new technologies and evolving privacy concerns.

II
LOOKING TO ENGLISH LAW FOR INSIGHT

Part II leaves American law, and turns to international law and English law in particular, to determine if another legal system can provide new direction to American employee privacy law. This Part begins by examining English common law and its emerging protection for privacy rights. It then examines both English legislation prompted by the United Kingdom’s membership in European organizations and legislation developed domestically. Next, it compares the American and English workplaces and societies to determine whether it is culturally feasible to adopt the English model in the United States. Finally, this Part concludes with a brief examination of the differing cultural concepts of what an employee is and how the feasibility of privacy legislation depends upon this understanding.

87. See id.
A. What Can be Learned from an Alternative System?

One place to look for ways to address the new challenges in employee privacy law is other common law systems. England, with its influence on early American law, is an obvious starting point. 89

1. Privacy Rights in English Common Law

There was no common law right to privacy in England. 90 Only recently have courts begun to recognize such a right, and it is still “underdeveloped, complicated and fragmentary.” 91 However, England explicitly recognized a right to privacy in 2001 in Douglas and Others v. Hello! Ltd. 92 There, the court discharged an injunction prohibiting publication of photographs taken absent permission by Hello! Ltd. at the wedding of Michael Douglas and Catherine Zeta-Jones. 93

The court discussed arguments by both academics and judges suggesting that a breach of confidence tort might fill the role of a privacy tort as developed in other countries. The court also noted that the European Commission of Human Rights and the Human Rights Act of 1998 supported this view. 94 The Douglas court gave two reasons for recognizing a common law right of privacy. First, there is a need to “respond to an increasingly invasive social environment by affirming that everybody has a right to some private space.” Secondly, the Human Rights Act of 1998 mandated that courts respect privacy. 95 In the end, the court discharged the injunction because Douglas and Zeta-Jones had already sold their privacy rights to another magazine (the other plaintiff). In such circumstances, compensation would suffice, where an injunction might do permanent damage to Hello Ltd! should it later win at trial. 96

In subsequent years, however, an employment tribunal held against an employee who was fired for sending hundreds of personal emails despite

89. England is discussed rather than Great Britain because Scottish law is not purely common law.
91. Jeffery, supra note 72, at 302 n.3 (citing BASIL MARKESINUS & SIMON DEAKIN, TORT LAW 648 (4th ed. 1999)).
92. [2001] 2 W.L.R. 967, 997–98 (Eng. C.A. 2000). While in the U.S. the Douglas case would usually be interpreted as a right of publicity case, the English court in Douglas treated the issue as one of the actors having the right to privacy at their wedding. See id. at 1005 (Sedley, L.J.) (“For reasons I have given, Mr. Douglas and Ms. Zeta-Jones have a powerful prima facie claim to redress for invasion of their privacy as a qualified right recognised and protected by English law”).
93. Id. at 972.
96. Id. at 1006–07.
knowledge that the employer monitored company email for extreme or improper personal usage. The emails contained disparaging comments about other employees and revealed private information to the employer’s competition.

Similarly, in *A v. B Plc and Another*, the court limited the right to privacy in a case involving celebrities. There, a professional soccer player procured an injunction prohibiting a national newspaper from publishing information sold to it by two women disclosing extramarital affairs with the soccer player. The court set aside the injunction for various reasons, including the women’s freedom of expression rights, the potential public interest in a celebrity’s actions, and the lower court’s improper assumption about the interest of the player’s wife not to know of his extra-marital relationships.

These cases show that England is beginning to recognize a common law right to privacy; however, the case law is limited and in its infancy. By far the greater delineation of rights of privacy has occurred in legislation, which is also quite new.

2. English Legislation

English privacy statutes are more comprehensive than in the American system. While the American system has laws for specific issues like health data, English laws apply to all categories of data, including health data, financial data, or employment record data. This subsection briefly discusses the main laws relating to employee privacy: the Human Rights Act of 1998, the Data Protection Act of 1998, and the Regulation of Investigatory Powers Act 2000 and its accompanying Lawful Business Practice Regulations 2000.

As a member of the European Union (EU), the United Kingdom must implement legislation the EU and its institutions pass. The main institutions of the EU are the European Commission (EC), the Council, and the Parliament. The EC “proposes legislation, policies and programmes of action and . . . is responsible for implementing the decisions of Parliament and the Council.”

---

98. Id.
100. Id. at 202.
101. Id. at 216–18.
103. See id.
PRIVACY AND PRODUCTIVITY

“Directly applicable” EU regulations mandate the implementation and substance of member countries’ domestic laws. Directives, on the other hand, are “directly effective” such that members can meet the policy goals of the directive in their own manner and form of implementation.

The Council of Europe, separate from the EU, was created in 1949 to protect human rights and help Eastern and Central European countries reform as they emerged from prior regimes. Every EU member first joined the Council of Europe; thus England, through the United Kingdom, is a member of the Council of Europe. The Council of Europe passed the European Convention on Human Rights, a major piece of legislation in which signing nations have promised to respect citizens’ basic human rights and provide certain guarantees of those rights.

a. Codified EU and Council of Europe Law

Thus, England has had to implement various international treaties relating to privacy because of its membership in the EU and the Council of Europe. England’s Human Rights Act of 1998 (the “Act”) implements the European Convention on Human Rights (“Convention”). The Act embodies fundamental principles that apply to all law in England. This has had dramatic impact because the Act mandates that all law—past, present, and future—must be interpreted and created while taking these principles into account. Significantly, under Article Eight of the statute, individuals’ private and family life should be respected. This right to privacy is an actual human

105. “See Europa, How does the EU work, supra note 102.
106. IAN WARD, A CRITICAL INTRODUCTION TO EUROPEAN LAW (2nd ed. 2003).
107. Id.
109. Id.
110. See European Court of Human Rights, Frequently Asked Questions, http://www.echr.coe.int/ECHR/EN/Header/Applicants/Information+for+applicants/Frequently+asked+questions/ (last visited Jul. 29, 2007) (“The European Convention on Human Rights is an international treaty which only member States of the Council of Europe may sign. The Convention, which establishes the Court and lays down how it is to function, contains a list of the rights and guarantees which the States have undertaken to respect.
111. See Jeffery, supra note 72, at 304.
112. See id.
113. See id.
114. “Article 8 Right to respect for private and family life 1) Everyone has the right to respect for his private and family life, his home and his correspondence. 2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.” Human Rights Act, 1998 c. 42, § 8, sched. 1 (Eng.).
right that should not be interfered with except as needed for national or economic security, public safety, prevention of crime, or the protection of health, morals, or other rights or freedoms of other citizens. \(^{115}\) Also, when the EU issued Directive 95/46/EC, \(^{116}\) which concerned the rights given under the Convention, England had a duty to implement the Directive in some form or another. \(^{117}\) The Directive was later implemented in the Data Protection Act of 1998 ("Data Act"), but it is worthwhile to first examine the Directive itself. \(^{118}\)

As laid out in Article One of the first chapter, the Directive’s objective is to “protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.” \(^{119}\) Personal data includes data pertaining to identified or identifiable “natural” persons. \(^{120}\) The Directive covers the “processing” of personal data, except for national security issues, criminal issues, and activity that is “purely personal or household activity.” \(^{121}\) Section One sets out the principles relating to data quality, which require data to be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. \(^{122}\)

One scholar interprets the Directive as exemplary of a trend whereby EU legislation provides individuals and the private sector more decision-making

\(^{115}\) Id.


\(^{120}\) Id. art. 2.

\(^{121}\) Id. art. 3.

\(^{122}\) Id. art. 6.
power than prior legislation, putting individuals in set categories with fixed rights.\textsuperscript{123} It appears that the EU is able to adapt to changing conditions in society, perhaps making it also responsive to changes in technology. The element of individual autonomy espoused in the Directive may make it particularly appealing as an example for the United States. More will be said about this idea in Part III.

In England, an Information Commissioner promotes and enforces the Data Act, which is comprised of eight principles. The structure of the act is unusual because traditional English law is based on rules rather than principles.\textsuperscript{124} The principles are as follows:

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 organisational measures shall be taken against unauthorised 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.\textsuperscript{125}

Specific clauses of the Data Act give the individual about whom data is collected substantial control over that information. Part Two of the Data Act entitles individuals to require data controllers (those who process data) to stop processing their data if processing "is causing or is likely to cause substantial damage or substantial distress to him or to another, and that . . . damage or distress is or would be unwarranted."\textsuperscript{126} Another clause generally prohibits the

\begin{itemize}
\item \textsuperscript{123} Claudia Faleri, \textit{Information Technology and Workers' Privacy: Public and Private Regulation}, 23 \textit{Comp. Lab. L. \\& Pol'y J.} 517, 523 (2002).
\item \textsuperscript{124} See Jeffery, \textit{supra} note 72, at 304.
\item \textsuperscript{125} Data Protection Act, 1998, c. 29, part I, sched. 1 (Eng.).
\item \textsuperscript{126} \textit{Id.} part II, § 10(a)–(b).
\end{itemize}
processing of data unless the data controller is registered with the Commissioner.\textsuperscript{127} Another clause states that one must not intentionally or recklessly obtain or disclose or procure the disclosure of personal data without the permission of the data controller.\textsuperscript{128} Additionally, recruiters or employers may not require an individual to disclose relevant records.\textsuperscript{129} However, Schedule Seven provides limited exceptions to a person’s right to access processed information. Notably, information pertaining to trade secrets, management forecasts and planning, employment negotiations, and corporate financial services affecting the value of the company or substantial national economic interests does not have to be revealed.\textsuperscript{130}

\textit{b. England-Initiated Legislation.}

Besides the Data Protection Act, England has an act similar to the American Electronic Communications Privacy Act, the Regulation of Investigatory Powers Act 2000 (\textquotedblleft RIPA\textquotedblright).\textsuperscript{131} RIPA creates a “general legal framework” making it illegal to intercept any type of private or public communication without the consent of both parties.\textsuperscript{132} RIPA, of course, provides exceptions for postal and telecommunications workers acting in their work capacities and for the prevention and detection of interference with wireless telegraphy.\textsuperscript{133} RIPA calls for the development of regulations regarding monitoring of employees in the workplace; however, these regulations have caused significant confusion by seeming to give employers broad authority to intercept communications.\textsuperscript{134}

The regulations, called the Lawful Business Practice Regulations, permit employers to monitor employees’ data 1) to demonstrate facts or establish compliance with regulations or self-regulatory practices in order to carry out business; 2) for national security reasons; 3) to prevent crime; 4) to investigate or detect unauthorized use of communication technology; 5) to determine whether communications are relevant to the employer’s business purposes; or 6) to monitor anonymous counseling by phone services, as long as communication systems’ users are notified, if possible, of such monitoring.\textsuperscript{135}

As Mark Jeffery concluded, despite substantial constraints on employers’ monitoring and use of employee data in England now, the Lawful Business

\begin{itemize}
\item \textsuperscript{127} \textit{Id.} part III, § 17.
\item \textsuperscript{128} \textit{Id.} part VI, § 55.
\item \textsuperscript{129} \textit{Id.} part VI, § 56.
\item \textsuperscript{130} \textit{Id.} sched. 7.
\item \textsuperscript{131} 2000, c. 23 (Eng.).
\item \textsuperscript{132} \textit{See} Jeffery, \textit{supra} note 72, at 305.
\item \textsuperscript{133} 2000, c. 23, § 3 (Eng.).
\item \textsuperscript{134} \textit{See} Jeffery, \textit{supra} note 72, at 305.
\item \textsuperscript{135} Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations, 2000, No. 2699, c. 23, § 3 (Eng.).
\end{itemize}
Practice Regulations contradicted those restraints, seeming to give employers significant authority to continue monitoring employees. As a result of the confusion, the regulations' scope may only be determined with future litigation. Because employee privacy law in England has left many issues unresolved, one may conclude that England has little to offer the United States by way of advice. However, that conclusion would be hasty because the groundwork laid in England is largely absent in the United States. Thus, the fundamental structure of English data privacy law may provide a useful model to future U.S. legislation.

Moreover, there is at least one more aspect of English law of great relevance that has not been discussed: namely, the role of the Information Commissioner Office (the "Commissioner") created under the Data Protection Act as discussed above. The Data Act provides the Commissioner, an independent government agency, with broad authority of investigation and enforcement. As described in the Office's Fiscal Year 2005 Annual Report, the Commissioner is an "independent public body set up to promote access to official information and protect personal information," reporting directly to Parliament. The Commissioner provides information via a "Helpline," investigates complaints, and enforces the law by ordering compliance, issuing decisions, and prosecuting noncompliant parties. In Fiscal Year 2005 the Commissioner completed more than 20,000 complaint cases and had almost 260,000 registered data controllers. The Commissioner also prosecuted twelve cases that year, which resulted in fines and conditional discharges.

An illustration of how the Commissioner works is as follows: if a person believes he or she has had personal data mishandled, the person should first try to work with the organization that is using or storing the data to fix the problem. The person can also call the Commissioner's Helpline for suggestions on this first step. If that does not work, the person can submit a "Data Protection Act Complaint Form" to the Commissioner along with supporting documentation. If the complaint appears legitimate, the

136. See Jeffery, supra note 72, at 332.
137. See id. at 324.
139. Id.
140. Id. at 57–58.
141. Id. at 59.
143. See id.
144. See id. at 3.
Commissioner will try and resolve the problem with the organization\textsuperscript{145} and if the organization does not fix the problem after a request to do so, the Commissioner may order the organization to do so by means of an enforcement notice.\textsuperscript{146} The person can also take the organization to court in order to try and gain compensation under the law for the improper handling of the data.\textsuperscript{147}

The Commissioner's interpretation of the Data Act is "highly persuasive" in court.\textsuperscript{148} For example, the Commissioner issues the Employment Practices Code ("Code"), which is meant to give employers guidance on how to handle data in the workplace.\textsuperscript{149} The Code can be very influential, though not legally binding.\textsuperscript{150} The Code, issued under Section Fifty One of the Data Protection Act, lays out the Commissioner's suggestions for employer compliance.\textsuperscript{151} The Code consists of four sections: recruitment and selection of employees; maintenance of employment records; monitoring employees at work; and managing information about employees' health. Each section includes specific recommendations on best practices.\textsuperscript{152}

Regarding early views on employee privacy, Jeffrey writes that the Commissioner suggested employees must be notified each time data is matched.\textsuperscript{153} In fact, the Commissioner's view was that employers must have permission to use data from outside the realm of employment and must use the same care when dealing with potential and past employees.\textsuperscript{154} Additionally, employees should be told that they may be monitored electronically and why they may be monitored.\textsuperscript{155} Finally, employees may require further notice of monitoring, if employers lead employees to believe that they are operating privately.\textsuperscript{156}

In summary, England's new privacy legislation establishes some definite boundaries for monitoring employees at work and for using data collected

\textsuperscript{145} See id. at 4.
\textsuperscript{146} See id. at 4–5.
\textsuperscript{147} See id. at 4.
\textsuperscript{148} See Jeffrey, supra note 72, at 339.
\textsuperscript{150} See Jeffrey, supra note 72, at 307.
\textsuperscript{152} Id. at 2.
\textsuperscript{153} See Jeffrey, supra note 72, at 314.
\textsuperscript{154} See id. at 313–24.
\textsuperscript{155} Id. at 333 ("She argues that even where employees have been clearly notified that computer monitoring may occur, if the employer does not carry out such monitoring in practice then the employees will have been led to believe that their privacy will be respected and so a further warning will be necessary before the employer may lawfully start monitoring.").
\textsuperscript{156} See id.
about employees. To an extent, the legislation works together toward the aim of protecting personal privacy. In order to meet the EU Directive and the European Convention on Human Rights, the English Human Rights Act and Data Protection Act will have to be interpreted broadly.\textsuperscript{157} And the Lawful Businesses Practice Regulation must bow to the broader limitations of RIPA, because it is only a regulation.\textsuperscript{158} In aggregate, the laws require that employee monitoring be specific and related to employers’ businesses, that the monitoring be proportionate to the employers’ needs and balanced against the employees’ privacy rights, and that monitoring not be done any more than necessary.\textsuperscript{159}

\textbf{B. Can the United States Adopt the English Model?}

This section compares the United States and England with the goal of examining the feasibility of integrating some of the concepts of English law into American workplace privacy law.

\textit{1. Societal Background}

\textit{a. First Principles}

Academics have posited that there are certain “first principles” that delineate internationally shared norms about data use and privacy in general.\textsuperscript{160} These principles express concern about the quality of data, transparency in the processing of data, the extra care warranted by sensitive personal data, and how standards should be enforced.\textsuperscript{161} In fact, as some scholars have pointed out, there is nothing stopping employers from setting their own standards based upon “the fundamental privacy principles of legitimacy, transparency, proportionality, finality and data accuracy and security.”\textsuperscript{162} How these basics are interpreted and incorporated into national legal systems may be a function of societal and cultural characteristics of nations.

\textit{b. Comparison of American and English Society}

One major aspect of American information privacy culture is its emphasis on classically-derived economics, where society is market dominated and rights are political rather than social in nature.\textsuperscript{163} Such an environment breeds a
"political philosophy of nonintervention which has led to the law only providing limited safeguards of employee privacy."\(^{164}\) The American legal framework also places greater emphasis on freedom of contract.\(^{165}\) Employees are thereby free to choose where to work, but are not free to dictate how the workplace operates, a choice that is left to the employer.\(^{166}\) The freedom of contract thus allows American workers to waive their rights in exchange for employment.\(^{167}\)

In England, however, privacy may now be considered a political right under overarching EU legislation that created a new fundamental human right for its citizens, the “data subjects” of the Directive.\(^{168}\) Instead of being gained by bargaining and agreement through contract, privacy is now seen as an inherent human right. Privacy is essentially part of human dignity that the community at large accords to individuals.\(^{169}\) Therefore, as the individual does not generate privacy, one cannot contract away her rights.\(^{170}\)

American philosophy tends to favor the free flow of information.\(^{171}\) Any restriction on the use of individual data, therefore, is a violation of that value.\(^{172}\) As James R. Maxeiner describes it, people are interested in the individuals who run businesses; they seek information about who owns a business, what experience they have, and what experience managers have.\(^{173}\) So, what might be intended to be governmental protection of information, instead might be seen as a paternalistic restriction on that free flow of information.

Consequently, American society tends to trust the private sector to safeguard information.\(^{174}\) Consistent with the Lockean view of the state,

---

\(^{164}\) Reidenberg, Resolving Conflicting International Data, supra note 26, at 1343.


\(^{166}\) See id.

\(^{167}\) See id. at 563 (discussing a New York court’s embracement of the “‘liberal’ conception of the employment contract”).

\(^{168}\) See id.

\(^{169}\) See Reidenberg, Resolving Conflicting International Data, supra note 26, at 1330–31.

\(^{170}\) See Lasprogata et al., supra note 149, at 8.


\(^{173}\) See Reidenberg, Resolving Conflicting International Data, supra note 26, at 1345 (“The American liberal philosophy minimizes execution of the First Principle of finality. Purpose limitations on the use of collected personal information are seen as contrary to the ideology of free flows of information.”).

\(^{174}\) See id. at 1345.
government is designed to only protect property and therefore takes a hands-off approach to regulation.\textsuperscript{175} A requirement to report data collection to the government might even go against a constitutional tradition leery of government intervention.\textsuperscript{176} Together with the emphasis on freedom of contract, any regulation of data and privacy should arguably be left to contract by individuals protecting their own privacy rights.\textsuperscript{177} In fact, privacy becomes personal property, a commodity subject to contract; thus people can contract away their right to privacy from employer monitoring by consent.\textsuperscript{178} As one academic describes, "duties were uncoupled from rights as the latter became subject of unfettered commodification."\textsuperscript{179}

England neither has a codified constitution nor an ideological repugnance to governmental intrusion.\textsuperscript{180} The autonomy of individuals, after all, is a political right, given by law.\textsuperscript{181} In Europe, the public generally trusts the government more than the private sector with respect to the protection of personal data.\textsuperscript{182} The state is thought to protect weaker citizens from stronger individuals who occupy the private sector.\textsuperscript{183} Thus, while the Directive, as discussed above, has moved in the direction of giving the private sector and individual citizens more freedom of choice, it remains the realm of the state to enforce privacy law.\textsuperscript{184} Individuals cannot contract away their privacy rights by consenting to monitoring.\textsuperscript{185} Instead, personal data must be processed in a legal and just manner, regardless of an individual’s consent.\textsuperscript{186} Furthermore, to the extent that the Directive allows individuals to consent to monitoring, any consent must be actual consent "freely given." In other words, people must

\begin{flushleft}
citizens. Instead of public sanction, private initiative offers the principal means of enforcement of fair information practices. By relying on private action, citizens must vindicate their own interests and the opportunities for state interference with information privacy are limited.
\end{flushleft}

\textsuperscript{175.} See id. at 1342.
\textsuperscript{176.} See id. at 1335.
\textsuperscript{177.} See id. at 1342.
\textsuperscript{178.} See Lasprogata et al., supra note 149, at 109.
\textsuperscript{180.} See, e.g., History Learning Site, The British Constitution, http://www.historylearningsite.co.uk/british_constitution1.htm (last visited Jul. 29, 2007); cf. Reidenberg, \textit{Resolving Conflicting International Data, supra} note 26, at 1347 (discussing European countries’ view that “the state [is] the necessary player to frame the social community in which individuals develop.”).
\textsuperscript{181.} Cf. Reidenberg, \textit{Resolving Conflicting International Data, supra} note 26, at 1347 (“Citizen autonomy, in this view, effectively depends on a backdrop of legal rights.”).
\textsuperscript{182.} See id. (discussing European attitudes towards government).
\textsuperscript{183.} See Faleri, supra note 123, at 524.
\textsuperscript{184.} See id. at 525.
\textsuperscript{185.} Cf. id. at 519 ("[E]ven the U.K. Legislature [in 1984] chose to create laws that set out specific obligations rather than to leave space for the parties concerned to decide the matter for themselves: the law was thus essentially public, rather than private in nature.").
\textsuperscript{186.} See Reidenberg, \textit{Resolving Conflicting International Data, supra} note 26, at 1348.
have the real option to say no to monitoring. 187

Unlike the Directive, the American legal framework makes a distinction between employer surveillance of employees and the use of that data. 188 This bifurcation allows separate regulations to be adopted for each area. 189 Recently-enacted laws dealing with interception of communications such as the ECPA only address the specific contents of those communications; such regulations fail to recognize the significance of intercepted communication's collateral information, such as the identity of the sender. 190 By comparison, the EU's Directive covers both monitoring and processing of individual information. 191

c. Employee or Citizen?

The cultural role of the worker may also affect the feasibility of a change in employee privacy law. Is a worker an employee in the American sense of human capital or commodity? Or is a worker primarily a citizen with individual rights that do not disappear at the workplace door? These differing views describe a fundamental divide between the American and English/European approaches to privacy law in the workplace and may be the biggest influence on the success of any proposed doctrinal change. 192

Historically, "[e]mployment on a continuing basis, apart from the guild regulated master/journeymen (and master/apprentice) relationship, most often was of domestic service, which was scarcely distinguishable in law from servitude; it included, for example, the master's power to inflict corporal punishment on the servant . . . [and] service was entered into by contract." 193 This relationship eventually became contractual rather than status-driven, both in Europe and in the United States. 194 These contracts allowed employers more or less to rule all aspects of employees' work lives. 195 American employees were able to win rights like minimum wages, overtime compensation, and regulations against child labor only after great struggle. 196 The concept of

188. See id. at 554; Lasprogata et al., supra note 149, at 22.
189. See Filho & Jeffery, supra note 165, at 554.
190. See Lasprogata et al., supra note 149, at 22 (explaining that addressing data for an email might include the identity of the sender of the email, the date the email was sent, the recipient, etc.).
191. See Filho & Jeffery, supra note 165, at 554; Lasprogata et al., supra note 149, at 22.
192. See Finkin, Menschenbild, supra note 179, at 637 (summarizing the significant difference between the United States and European countries, where in the latter, employers may not unilaterally impose monitoring to ensure work productivity). This remains a philosophical argument largely beyond the scope of this Comment, but having a basic grasp of the arguments will provide an understanding of the policy implications of the proposal set forth below.
193. See id. at 600.
194. See id. at 612–13.
195. See id. at 577.
196. See, e.g., WILLBORN ET AL., supra note 13, at 618–39 (discussing the history of the
employment must thus be seen in the context of employees’ historical efforts for workplace rights and rights as citizens in general.\textsuperscript{197}

While the United States evolved with Europe to the extent of viewing employees and employers as contracting agents rather by means of a class-based master-servant relationship, other countries may have evolved further toward recognition of employee rights than the United States. The employment relationship in Germany, for example, carries similar economic and contractual overtones of the master-servant relationship, but includes social attitudes influenced by the eighteenth-century view of citizens as having inalienable rights.\textsuperscript{198} A German employee is also perceived as a citizen, and therefore enjoys certain rights that cannot be left at the workplace door. This concept of rights and dignity through citizenship is difficult to translate, both literally and culturally, to the American context.\textsuperscript{199} Loosely, German\textsuperscript{200} employees actually have a “general right of personality” that employers must acknowledge such that German employers are more likely than American employers to “codetermine” the rules of the workplace with employees or employee representatives.\textsuperscript{201} The United States has not taken these steps, but instead continues to allow employers to control employees both within and outside the workplace (sometimes called creating “corporate culture”), even to the extent of requiring employees to contribute to specific charities.\textsuperscript{202}

The proposal made in Part III will be incremental and will take as its reference point England, which has closer ties and a more similar legal structure to the United States than does Germany. Ideally, the United States may arrive at the point where employers and employees work together to codetermine the workplace environment; however, until American perception of the employment relationship shifts to acknowledge a stronger role for the employee as citizen, this is unlikely to happen.\textsuperscript{203} In the absence of cultural change such that American workers are seen as citizens and not just employees, courts or the United States government will have to proactively protect employee privacy.

\begin{footnotesize}
\begin{enumerate}
\item[198.] See Finkin, \textit{Menschenbild}, supra note 179, at 625.
\item[199.] See id. at 580–81.
\item[200.] Note that Germany does differ significantly from the United States in that its unions play a very strong role in employment relations both with employers and the state. See id. at 619 (discussing the importance of unions and union-like activity in Germany after World War I).
\item[201.] See Finkin, \textit{Menschenbild}, supra note 179, at 580–84.
\item[202.] See id. at 627.
\item[203.] Cf id. at 580 (noting that the role of the worker in the United States remains “largely rooted in the nineteenth century,” with employees having little say over the workplace).
\end{enumerate}
\end{footnotesize}
2. Surmountable Differences

At first glance, the societal differences between the United States and England (much less the United States and Germany) seem significant and appear to pose barriers to successful implementation of English and European doctrines into United States privacy law. However, there are key similarities between American and English societies beyond a shared legal heritage arising from competition in the global marketplace. Legal change in the area of employment privacy law is entirely possible, as England has shown. In part, becoming a member of the EU required England to transition from its customary approach “based on semantics, to an approach in which the policy objectives behind the law are considered.” Additionally, the very existence of the EU and English law favoring protection of employee privacy is putting pressure on the United States to adopt similar law.

III

PROPOSAL FOR CHANGE OF AMERICAN EMPLOYEE PRIVACY LAW

This last Part defines and analyzes a proposal for changing American employee privacy law to address the tension between what information an employer reasonably might gather and how that information might later be aggregated for inappropriate purposes. It also briefly considers some alternatives, proposed by other scholars, to the proposal for comprehensive legislation or judicial flexibility given here. Either way, with the increasing sophistication of technology and communication, this tension is likely to grow into a truly global issue. Furthermore, the problem has become even more significant as the boundaries between work and personal time and workplace and home become less clear than they once were. American employment law needs to provide employers with more guidance on the collection and use of private employee data and provide more protection for their privacy.

A. Proposal

The suggested change comes in two parts. The first relates to judicial interpretation of current American state and federal legislation, and could be implemented today. The second part is forward-looking, calling for broad, overarching federal legislation that would provide both rules guiding employer
PRIVACY AND PRODUCTIVITY

monitoring of employees at work, as well as the collection and use of employee data.

The first proposal suggests that judges should interpret both state and federal legislation as broadly as possible to craft standards of relevance, proportionality, quality, and finality, and establish transparent and predictable procedures for employers to follow. Relevancy requires that an employer's actions in monitoring, collecting and using employee data must relate to a specific business-related goal. Data gathered via monitoring should not be used for inappropriate purposes. The relevance requirement can also be called a legitimacy requirement since not only should the reason for monitoring or gathering data be legitimate, the means used for such actions must also be as unintrusive as possible. Judges should examine not only the purpose and legitimacy but also the methods of information gathering to assure a minimal invasion of employee privacy. Courts should balance the needs of the employer against the potential impact on the employee to ensure that the employer only impacts the employee's privacy in proportion to the employer's need.

Additionally, the accuracy of any data gathered about employees should be of the highest quality. New technology facilitates data collection and storage, but does not assure accuracy; data accuracy remains dependant on the accuracy of the humans who enter the data into the technology in the first place. Judges should scrutinize an employer's monitoring and data collection methods to determine whether accuracy in data recording is achieved. Inaccurate data could lead beyond mere privacy claims to include defamation claims as well. Likewise, data should not be kept indefinitely. The finality element ensures that once has data served its purpose, it is disposed of appropriately. This will aid the relevance determination by ensuring that the

208. For a description of the relevance concept, see Vigneau, supra note 88, at 508.
209. See Lasprogata et al., supra note 149, at 107 (explaining that legitimacy is a “non-partisan principle[] that [is] fundamental to employee privacy in light of technological advances and the evolution of the modern day workplace” and that “[l]egitimate purposes include those that are necessary for compliance with a legal obligation of the employer, or necessary for the performance of a contract between the employer and the employee, or necessary to ensure system security and proper functioning. If there is a less intrusive means to satisfy the employer’s purpose, those means should be implemented.”).
210. See Vigneau, supra note 88, at 511.
211. Inaccurate data could constitute defamation because defamation can include a “false written or oral statement that damages another’s reputation,” and the release of false data could harm the person whose personal data it was. BLACK’S LAW DICTIONARY (8th ed. 2004).
212. See, e.g., Lasprogata et al., supra note 149, at 107 (defining finality as requiring that information “only be processed for a specific, explicit and legitimate purpose and not processed in any way incompatible with that purpose. Personal data may be retained only so long as necessary to fulfill the stated purpose”). Therefore, once data has served its purpose, it should be destroyed, by shredding of paper documents or overwriting computer hard drives. See, e.g., Robert Vamosi, Data destruction—it’s harder than you think, CNET NEWS.COM, June 10, 2005, http://reviews.cnet.com/4520-3513_7-6245517-1.html (describing means to destroy data and the difficulty in doing so).
data actually collected relates to a specific business-related goal and by reducing the possibility for future, inappropriate use.

An employer’s adoption of specific procedures for monitoring and processing data about employees may prove to be another way of balancing employers’ needs and employees’ privacy.\textsuperscript{213} Judges, as part of their privacy-intrusion analysis, could look to whether employers had such procedural policies in place and whether employees were given notice of those policies. This would ensure consistency in the treatment of employees, inform employees about their rights, and ensure that employees had notice (actual or constructive) of employers’ actions. A court might have to further inquire as to the adequacy of notice, however. While actual notice might not be required, a court could adopt an objective standard such that a reasonable person in the employee’s position would have read or known of the policy. This would address concerns that notice was inadequate under an unconscionable contract theory.\textsuperscript{214}

The second proposal is more sweeping and echoes scholars who have called for the establishment of a comprehensive federal statutory scheme to address employee privacy needs.\textsuperscript{215} This would provide clarity on notice and consent requirements, delineate appropriate use and lifetime of data, and afford an employee the capacity to correct false data.\textsuperscript{216} Comprehensive legislation would lead to federal preemption of current and diverse state privacy laws—an additional benefit of such comprehensive legislation. Without preemption, the most permissive and lax state laws will be the standard since many companies will tend to process electronic information within those states. The law of corporations provides an example of this phenomenon—most corporations now incorporate in Delaware because of its lenient laws.\textsuperscript{217}

More specifically, the eight principles of the Data Protection Act of 1998 should be incorporated into United States law. Thus, data would have to be fairly processed and relevant to a specific purpose; accurate and current; kept

\begin{footnotes}
\footnote{213. See id.}
\footnote{214. An unconscionable contract is one that a court may not enforce because it is so substantively or procedurally unfair or oppressive that it should not be enforced. See, e.g., BLACK'S LAW DICTIONARY, supra note 211.}
\footnote{216. See id.}
\footnote{217. See, e.g., Lawyers.com, Choosing a State of Incorporation, http://corporate-law.lawyers.com/Choosing-a-State-of-Incorporation.html (last visited Jul. 29, 2007) (“Delaware remains a preferred state of incorporation for public companies or companies that will be doing business in various states. Delaware’s tax structure for corporations is considered by some observers to be competitive with or even more advantageous than tax structures in other states, and Delaware has a well-developed body of corporate law and judicial precedent that can provide a sense of certainty in corporate transactions.”).}
\end{footnotes}
no longer than needed; processed with reference to employees' rights; kept securely; and not allowed outside of the United States unless the other jurisdiction matches these requirements. The burdens of proof and persuasion under the proposed federal statute would lie with the employer. An employer would have to establish that its policies met these standards, and that the employer had made reasonable efforts to comply with the standards. The United States may not be ready for an agency with the same powers of registration and enforcement as the English Information Commissioner, due to American aversion to regulation of businesses. Nonetheless, some agency or governmental department could be designated to fill an advisory role similar to that of the English Commissioner under the Data Act. Employers would appreciate a resource to turn to for guidance in these issues.

**B. Merits of Proposal**

Employers have legitimate reasons for monitoring and using employee data. One reason employers give for monitoring is reputational concerns, fearing that employees' actions, if unsupervised, might reflect badly on the organization. Employers also worry that employees' misuse of work time could result in several negative effects: 1) it may strain communication systems; 2) result in unintentional disclosure of confidential company information; 3) cause destruction of evidence for potential litigation; and 4) open the employer to potential sexual harassment liability. Other legitimate reasons for monitoring and collecting data include ensuring employee compliance with company policies, preventing employees from committing or facilitating patent or trademark infringement, computer hacking, industrial espionage, or other crimes. Both proposals described above allow employers to continue monitoring and collecting employee data so long as their reasons for doing so are legitimate. The proposed changes will clarify for employers what American law requires of them, thus providing consistency and security.

From employees' perspective, new technology may have changed the workplace enough to justify new privacy regulation. As many have noted, the line between what is private and public life is being blurred by technology that allows employees to access work remotely and stay in constant communication with employers and clients. In addition, "the law may imply a general term into all employment contracts, according to which the parties

---

218. See Data Protection Act, 1998, e. 28, part 1, sched. 1 (Eng.).
219. See Reidenberg, Resolving Conflicting International Data, supra note 26, at 1342.
220. See Jeffery, supra note 72, at 335.
221. See Finkin, Information Technology, supra note 1, at 474–76.
222. See Lasprogata et al., supra note 149, at 3.
223. See Vigneau, supra note 88, at 506 (stating that some people see new technology as different enough to require new laws).
224. See, e.g., Lasprogata et al., supra note 149, at 2; Vigneau, supra note 88, at 505.
must act in good faith or show loyalty to one another: undeclared surveillance may well be considered incompatible with such a condition . . . . It may be that the secret surveillance of employees is socially unacceptable – it may be seen as sneaky, underhanded, unfair, devious, or even sinister. Employees would also likely argue that consent does not equal free choice, and that the current scheme is therefore not working. In fact, some scholars argue that the new technology has had such an impact that it is actually creating new forms of subordination in the workplace. Thus, employees would probably favor changes in current American law to strengthen their privacy rights.

It seems very clear that the privacy rights of employees could easily become lost if something is not done to strengthen those rights. The question remains as to the best way to strengthen these rights. One argument is that it is preferable to leave employee protection efforts to the private labor market. In that scenario, employers may offer higher wages for the additional pressure and decreased autonomy that comes from the monitoring of employees in exchange for the higher productivity that monitoring may bring. If employers do not pay more to compensate employees for their loss of autonomy, they will have a harder time hiring employees, thus putting them at a competitive disadvantage. But a counterargument is that employees do not care solely about absolute wages, but also about relative wages, and will therefore accept the high-stress job in order to move into the upper middle class. Since everyone cannot be in the upper middle class, employees will take the high stress job in a perpetual “rat race,” though many would be more satisfied in jobs with less pressure. This contention supports the argument for at least judicial precedent strengthening employee’s privacy rights, as well as for additional, comprehensive legislation.

Judicial interpretation of current legislation to include standards such as relevance, proportionality, and procedure are small, incremental changes that employers might not find threatening. In fact, some employers may be satisfying those standards to a large extent already. While judges may be reluctant to impose these standards without more explicit direction, judges often incrementally alter precedent to meet the changing needs of society. This proposal at least, seems simple, achievable, and would be a much-needed step in the right direction.

New overarching federal legislation may be more difficult to draft, pass,

225. Filho & Jeffery, supra note 165, at 553.
226. Cf. Faleri, supra note 123, at 525 (discussing the Directive’s requirement of actual consent, which leads to the inference that employees prefer actual consent).
227. See Filho & Alvim, supra note 197, at 571.
228. See Willborn et al., supra note 13, at 267.
229. See id. at 268.
230. See id.
231. See id. (citing ROBERT H. FRANK, CHOOSING THE RIGHT POND (1985)).
and implement. The strong employer lobby may react negatively to any proposal for such legislation, arguing that it is unwanted and unneeded government intervention that will add yet another level of time-consuming, expensive bureaucracy to the regulatory state. Nevertheless, without such legislation the balance of power is tipping ever more in favor of employers at the price of significant privacy rights of employees.\(^\text{232}\) Comprehensive federal legislation has been possible in the medical and educational fields under HIPPA and FERPA, giving some hope that overarching federal legislation on privacy in the workplace may be feasible.\(^\text{233}\)

Some might argue that overarching federal legislation would be ineffective in creating actual change in employer practices.\(^\text{234}\) Indeed, some studies have found that enforcement of the new laws in England may be problematic.\(^\text{235}\) There may be a real concern that the United States would have to face similar enforcement issues. But as the Commissioner gains momentum, this is likely to be less of a problem in England,\(^\text{236}\) and with time, would become less of a problem in the United States.

### C. Alternatives

There are several other alternatives besides formulating a comprehensive federal legislation of employee privacy rights based on English law or simply importing a few of the tools of English law to the task of interpreting new state legislation.

Joel Reidenberg, has suggested creating an intra-governmental agreement similar in some aspects to the General Agreement on Trade and Tariffs (GATT).\(^\text{237}\) Reidenberg argues that the best solution to the issues created by new technology would be a “General Agreement on Information Privacy”

---

232. Cf. Vigneau, *supra* note 88, at 505–06 (“Many commentators seem to think that the law does not yet provide adequate tools to deal with these [employee privacy] issues and that the development of adequate responses requires the enactment of new laws.”).


234. Another alternative might be a market-based resolution where industries self-regulate employee privacy issues in order to keep government from intruding on the market while still addressing the concerns of the public. The problem with this alternative is that employee privacy issues are found in all industries, leading to the very problem inherent in current sectoral legislation where there is no uniform policy on employee privacy. While one industry might self-regulate to the point of adequately protecting employee privacy, another might not. When employee data is later shared between industries, say when an employee changes careers, the inadequacy of the system in one industry violates the integrity of the system set up in the other industry.

235. See, e.g., Jeffery, *supra* note 72, at 301; Reidenberg, *Resolving Conflicting International Data, supra* note 26, at 1315.

236. Statistics from the annual report show increasing levels of action by the Commissioner. See, e.g., *Annual Report, supra* note 138, at 57-58.

237. See Reidenberg, *Resolving Conflicting International Data, supra* note 26, at 1360.
signed by many countries. He sees the creation of such an entity as the "first step toward effective international cooperation." This argument draws on notions of globalization, but might not be realistic or effective, at least in the immediate future, because of the likelihood that a great deal of time and effort would be needed before such an agreement could be reached. Until such an international agreement becomes reality, the United States will have to further develop its own privacy regulations and standards. Judicial interpretation of current U.S. law provides at least an interim and immediate means by which to address employee privacy rights. It might also be easier to develop comprehensive, federal legislation that could successfully be passed by Congress where only American cultural views need be considered, than to reach an agreement that multiple countries need agree to at the international level.

Another approach Reidenberg offers to address the problem of data privacy is to allow the computer industry to drive standards for data protection. In other words, "[t]echnical rules and default settings [would] establish data privacy norms." However, current examples in other substantive legal areas show that private industry is not always effective at devising self-prescribed standards for regulation. One problem is that uniform protection is not possible where old technology has not been replaced by new technology that incorporates the industry privacy standards. Furthermore, this approach leaves data protection to the marketplace which, given the commodification of data discussed above, may be dangerous. In contrast, judicial enforcement of common law and statutory privacy rights provides both uniform protection and keeps privacy outside of the realm of commerce, as would comprehensive, federal legislation enacted to protect privacy.

238. Id.
239. Id.
240. Id. at 1331.
241. Id.
242. Examples where industry has been slow in resolving and regulating standards without governmental oversight are:
While some may argue that tensions remain constant between employers' desire to control the workplace and employees' rights to privacy, this Comment contends that new technology may actually poses more difficult challenges than American employers, employees, and laws have had to face in the past. These new challenges require additional legal protection of employees' privacy rights. Modern English law, as influenced by the EU, provides a strong model for America in adding this needed protection. Incremental change to judicial interpretation of current legislation is a good starting point for adding protections of relevance, proportionality, quality, finality, and procedure. A better, long-term goal is the passing of overarching federal legislation to address the privacy rights of employees in the American workplace.

243. This view is described by Finkin, Information Technology, supra note 1, at 503-04.