UIC John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 1 *Journal of Computer & Information Law - Winter 2007*

Article 2

Winter 2007

ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees, 25 J. Marshall J. Computer & Info. L. 37 (2007)

Colette Cuijpers

ICT AND EMPLOYER-EMPLOYEE POWER DYNAMICS: A COMPARATIVE PERSPECTIVE OF UNITED STATES' AND NETHERLANDS' WORKPLACE PRIVACY IN LIGHT OF INFORMATION AND COMPUTER TECHNOLOGY MONITORING AND POSITIONING OF EMPLOYEES

DR. COLETTE CUIJPERS, LL.M., PH.D†

I. INTRODUCTION

A. RESEARCH QUESTION AND APPROACH

During the past decades, the Internet and e-mail have been introduced into a variety of workplaces. The advantages of these technologies for employers have come with risks, which often relate to the use of these technologies by employees. For example, employees can cause financial damage to employers by leaking company secrets via e-mail or a mobile phone, or simply by surfing the Internet for private purposes during working hours. Also, they can cause damage to the company's reputation if they send pornographic or abusive messages from a company phone or e-mail address. To minimize these risks, employers often install devices to monitor Internet and e-mail.[1] The introduction of the Internet and e-

† I would like to thank Prof. Dr. Bert-Jaap Koops for his valuable comments on an earlier version of this paper.

1. AMA, *2004 Workplace E-mail and Instant Messaging Survey Summary*, http://www.epolicyinstitute.com/survey/survey04.pdf (accessed Nov. 29, 2007) The summary is based on the American Management Association Survey on Electronic Monitoring & Surveillance 2005. It becomes clear that computer monitoring takes various forms, with 36% of responding employers tracking content, keystrokes and time spent at the keyboard, and 50% store and review employees' computer file.

Companies also keep an eye on e-mail, with 55% retaining and reviewing messages. In the 2004 issue of this survey more general figures could be found regarding monitoring of e-mail; 60 % of the questioned companies monitored outgoing e-mail); *see also* Michael Rustad & Sandra R. Paulsson, *Monitoring Employee E-mail and Internet Usage: Avoiding the*

mail, as well as devices to monitor their use, greatly influences the relationship between employer and employee. On the one hand, Information and Computer Technology ("ICT") empowers employees, since it enlarges their communicative reach. On the other hand, ICT definitely increases the power of employers because it greatly facilitates monitoring of employee activity.

Given this dual influence, this article contributes to answering the following question: how does ICT affect the power balance between employer and employee, and is the legal framework adequate to deal with possible shifts in balances of power?[2] Because ICT is multi-faceted and pervasive in workplace environments—not all of which can be addressed in the scope of a single article—two specific scenarios are highlighted where ICT clearly affects the power balance between employers and employees. First, the more or less crystallized framework regarding the use of Internet and e-mail monitoring in the workplace will be addressed. The second scenario concerns the positioning of employees, within the boundaries of corporate premises as well as outside these premises. Positioning systems are becoming a new trend in employer surveillance.[3] With regard to this new method of surveillance, this article will address the question of whether the legal framework for e-mail and Internet monitoring might be applied in the same manner to positioning systems, and what consequences this might have for the relationship between employer and employee. With regard to the specific cases described, I will draw conclusions concerning the legislative framework and the balance of power associated with this framework. Both cases will be assessed from a comparative perspective, analyzing the United States and the Netherlands. These two countries are interesting to compare not only because they differ significantly in their way of thinking about privacy and privacy regulation, but also because their basic principles and regulations of labor law are very different.[4] Therefore, comparing these two

---

Omniscient Electronic Sweatshops: Insights from Europe, 7 U. Pa. J. Lab. & Emp. L. 829 (2005) (citing Reginald C. Govan and Freddie Mac, *33rd Annual Institute on Employment Law: Workplace Privacy*, 712 PLI/Lit 245 (2004) (A 2004 survey which revealed that "70% of responding employers have implemented a written e-mail policy governing use and content, 74% monitor employee outgoing and incoming e-mail, and 60% monitor employee Internet connections.").

2. This research forms part of a larger research project funded by the Netherlands Organization for Scientific Research on law, technology, and shifting balances of power, which, in addition to labor law, also addresses the fields of consumer protection and criminal law.

3. A simple Google search for 'gps monitoring employees' reveals a growing amount of services offered in this field.

4. *See* P. Blok, *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Boom Juridische Uitgevers, ch. 3-8 (2002) (analyzing U.S. and Dutch legal systems, summary in English), *see also* Antoine

countries will provide relevant insights into the effects of ICT monitoring and positioning on the balance of power between employers and employees.

B. BACKGROUND

The incentive to monitor employees' e-mail and Internet use is legitimate because it relates to the risks that result from the use of these means of communication by employees for private purposes.[5] Employee use of e-mail facilities and the Internet can not only have a negative effect on their productivity, but it can also lead to legal liability of the employer and, moreover, cause severe damage to an employer's reputation.[6]

In view of the foregoing conclusions, the easiest solution for employers would be to prohibit the personal use of e-mail and Internet in the workplace. However, research shows that this might also lead to loss of productivity, due to the negative effect on the employees' morale and because a certain amount of personal use of e-mail and the Internet might improve the use of these technologies for business purposes.[7] Practical arguments for how to prevent personal use without hampering normal business activities can also be compared to the use of the company's telephone for private purposes, which to a certain extent is quite commonly accepted. Instead of prohibiting personal use of the Internet and e-mail by employees, employers are now exploring ways to curb Internet use by installing surveillance technologies, such as video surveillance and Internet monitoring and positioning systems.[8] The risks attached to pri-

---

Jacobs, *Sociale rechten in Amerika*, Utrecht: LEMMA BV, 212 (2003) (describing differences between Dutch and the U.S. labor law), Antoine Jacobs, Labour Law in the Netherlands, Kluwer Law International (2004) (an English description of Dutch labor law).

5. Monitoring can also be justified by an employer's interest in controlling business operations and measuring productivity, efficiency and quality.

6. R. Blanpain & Michelle Colucci, *The Impact of the Internet and New Technologies on the Workplace. A Legal Analysis from a Comparative Point of View*, The Hague: Kluwer, 14-16 (2002) (giving an elaborate overview of risks); *see also* R. Blanpain, *On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work*, The Hague/London/New York: Kluwer, 44 (2002) (giving an overview of legal responsibilities and obligations for employers that justify some form of surveillance).

7. Blanpain & Colucci, *supra* note 6, at 18; *see also* Jay P. Kesan, *Cyber-Working or Cyber-Shrinking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 Fla. Law Rev. 289, 319 (2002); Rustad, *supra* note 2, at 19 (referring to an empirical study that demonstrates that workers who were electronically monitored manifest a higher rate of depression, anxiety, and fatigue than others in the same business that were not monitored); Peter Blackman & Barbara Franklin, *Blocking Big Brother: Proposed Law Limits Employer's Right to Snoop*, N.Y. L. J., at 5 (1993); Kenneth A. Kovach et al., *The Balance Between Employee Privacy* And Employer Interests', 105 Business and Society Review 289, 295 (2000) (stating "undeniably, an employee who does not trust his/her employer has much less of an incentive to be efficient, resourceful and productive").

8. Blanpain & Colucci, *supra* note 6, at 18.

vate use of the Internet and e-mail facilities justifies new control methods, which are more far-reaching than a pure productivity check. However, the employer's right to conduct business in a self-determined manner—which might include certain forms of workplace surveillance—could conflict with the employee's right to privacy. In order to balance these rights, monitoring should be subject to terms and conditions limiting the scope and impact on employees. Monitoring can easily go beyond the justified purpose of protecting pure business interest or property. Without proper safeguards, monitoring, as well as positioning systems, could enable employers to watch employees' every move. This would empower the employer to an unacceptable level. This article assesses whether American and Dutch law can offer these safeguards.

II. THE UNITED STATES' AND DUTCH APPROACHES TOWARDS INTERNET AND E-MAIL SURVEILLANCE

A. INTRODUCTION

This section discusses the similarities and differences between U.S. and Dutch legal approaches towards Internet and e-mail surveillance. These follow from the different starting points these countries take with regard to the right to privacy. In the U.S., privacy is viewed from a market-driven, property approach, as opposed to the Dutch tradition of regarding privacy as a fundamental human right.[9] Based on literature, legislation and case law, only general conclusions will be drawn regarding the questions of whether, and to what extent, Internet and e-mail monitoring by employers is allowed and what safeguards exist in relation to employees' right to privacy.

B. UNITED STATES[10]

1. *Constitution and Tort Law*

In the U.S., relief against employer surveillance in general can be sought on the basis of three[11] different sources of law relating to the

9. *See* Rustad *supra* note 2 (comparing the U.S. approach and the E.U. approach (on which the Dutch legal system regarding privacy is based)). A thorough analysis of the two legal systems will not be made in this article. For such an analysis, see Blok, P., *Het recht op privacy. Een onderzoek naar de betekenis van het begrip 'privacy' in het Nederlandse en Amerikaanse recht*, Boom Juridische Uitgevers, ch. 3-8 (2002) (analyzing U.S. and Dutch legal systems); *see also* Blanpain, *supra* note 7, at 95-125, 233-251.

10. With regard to the American situation, only very general conclusions can be drawn from the broad range of case law, which sometimes are drawn from differing state laws.

11. A fourth source, state law, is left out of the discussion. However, interestingly, state laws and proposed state laws regarding Internet and e-mail monitoring often focus on information to employees, instead of prohibition or limitation of the scope of monitoring. Two examples include *Connecticut Electronic Monitoring Law,* Pub. L. No. 98-142, which requires notice to employees of electronic monitoring by employers, and the bill proposed by

right to privacy: the Fourth Amendment of the Federal Constitution regarding unreasonable search and seizure,[12] the Electronic Communications Privacy Act ("ECPA"), and the privacy tort of "intrusion into seclusion." With regard to the Fourth Amendment and "intrusion into seclusion," the legality of Internet and e-mail surveillance depends on the question of whether the employee had a "reasonable expectation of privacy."[13] Referring to American case law, literature often states that there is no reasonable expectation of privacy in the workplace whatsoever.[14] If a reasonable expectation of privacy is assumed, employers can easily nullify this expectation by informing employees of the fact that their use of Internet and e-mail is being monitored.[15] From case law, it

---

Debra Bowen in California to protect the privacy of Internet and e-mail usage at work. This bill was vetoed by Governor Schwarzenegger. *See* Mark Sullivan, Wired, *Arnold Vetoes Privacy Bill*, Sept. 30, 2004, http://www.newstarget.com/002149.html (2007); Karen Eltis, *The Emerging American Approach to E-mail Privacy in the Workplace: Its Influence on Developing Case law in Canada and Israel: Should Others Follow Suit?*, 24 Comp. Lab. L. & Pol'y J. 487 (2003) (for a more elaborate overview of the right to privacy in the United States in relation to Internet and e-mail monitoring by employers); *see also* Blanpain, *supra* note 7, at 233-251; Blanpain & Colucci, *supra* note 7, at 155-157; Kesan, *supra* note 8; Rustad & Paulsson, *supra* note 2.

12. Individuals can only rely on the Fourth Amendment in relation to public employers.

13. O'Connor v. Ortega, 480 U.S. 709 (1987); *see also* Gellman, R., *A General Survey of Video Surveillance Law in the United States*, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, IT & Law Series 7, Den Haag: T.C.M. Asser press (2005) (Case law regarding video surveillance shows that the private or public nature of the area being surveyed is also of great importance, as there must be solitude or seclusion to be intruded upon. Not all spaces fall neatly into the public or private categories. A workplace can be an intermediate location between public and private. Therefore, the public-private criterion is not that suitable with regard to Internet and e-mail monitoring by employers. Further, enhanced surveillance technologies are eroding the relevance of the private and the public space. Privacy can be invaded by surveillance that occurs in wholly public space.).

14. *See e.g.* Rustad & Paulsson, *supra* note 2, at 10 (referring to Eltis, *supra* note 12, at 498 ("Employees have no reasonable expectation of privacy when using company e-mail/ Internet facilities. . . . [t]he employer's ownership of these work tools entitle her to monitor their use in any way she deems fit.").

15. Robert Fragale Filhot & Mark Jeffery, *Information Technology and Workers' Privacy: Notice and Consent, A Comparative Study: Part III: Recurring Questions of Comparative Law*, 23 Comp. Lab. L. & Pol'y J. 471, 557-558 (2002) ("One such consequence may be to affect the recognition by the law of any expectations of privacy that the employee may have had. This position is clearest in the United States, where such protection as is afforded by the tort of invasion of privacy is not available to employees if they have been notified of the possibility of surveillance. According to this law, once notice has been given, an employee cannot reasonably expect any privacy and so there can be no question of wrongful harm. The very opposite position has been taken in France, where the highest appeal court has ruled that the expectation of privacy (at least, as regards the secrecy of communications) can never be over-ridden: Employees may be disciplined if, having been notified of a prohibition on the private use of their employer's computer facilities, they then

follows that employers might even monitor employees' use of Internet and e-mail without informing them about this practice.[16] In *Smyth v. Pillsbury Co.*, the court simply concluded that an employee does not have any expectation of privacy in his work e-mail, since the expectation is lost as soon as the employee voluntarily uses an e-mail account provided at work.[17] Even if the employer assures its employees that all e-mail communications will remain confidential and privileged, monitoring can still be judged admissible because "[t]he company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have."[18] As a result, the chances of employees winning lawsuits against their employers for invasion of privacy by monitoring employees' Internet and e-mail on the basis of the Fourth Amendment or "intrusion into seclusion" are very slim.[19]

With regard to the tort of "intrusion into seclusion," there is even a subsequent hurdle to establish a violation; the intrusion must be "highly offensive."[20] Internet and e-mail monitoring by employers is hardly ever qualified as such because it does not involve a physical invasion.[21] Moreover, the Fourth Amendment is limited in scope because it can only be invoked against public employers when their actions can be qualified as "state actions."[22] Also, the definition of what constitutes a "search" narrows the scope of the Fourth Amendment's protection. According to *Kyllo v. United States*, there is a "search" only if the government uses technol-

---

disobey this rule; but the legal protection of privacy remains unaffected, and so the employer may not examine the contents of any private files sent or stored in breach of the prohibition.").

16. *See* Garrity v. John Hancock Mut. Life Ins. Co., 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2000) (holding that employees have no reasonable expectation of privacy in e-mail messages transmitted over the network, and employers are, at times, obligated to investigate employees e-mails when allegations of sexually explicit e-mails are made).

17. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996); Kovach, *supra* note 8, at 294 ("The cases *Smyth* and *Bourke* strongly support the proposition that a well-written e-mail policy will be sufficient to render unreasonable any expectation of privacy.")

18. *Id.*

19. Filhot, *supra* note 16, at 560 (stating, "[n]evertheless, U.S. employers who have an official policy which involves an invasion of their employee's privacy - such as random personal searches - may be advised to make occasional searches, if for no other reason than to ensure that the policy remains 'active' and that the employees do not have any opportunity to develop a reasonable expectation of privacy.")

20. Miller v. Natl. Broadcasting Co., 187 Cal. App. 3d 1463 (Cal.App. 2nd Dist. 1986).

21. Dan Long, *The Electronic Workplace*, Modrall, Sperling, Roehl, Harris & Sisk, P.A., June 3, 2002, http://www.modrall.com/articles/article_100.html

22. Parry Aftab, *Monitoring Law: To Videotape or Not to Videotape. . .That Is the Question*, http://www.aftab.com/videotapinglaw.htm (last visited Feb. 2, 2007) (stating that the Fourth Amendment protects people from unreasonable searches and seizures by state action and some states, such as Massachusetts, California, and Florida, apply their Fourth Amendment equivalent to private parties as well).

ogy that is not in "general public use" to obtain information from one's private space without physical intrusion.[23] Therefore, visual surveillance possible with the naked eye or commonplace visual enhancement technologies does not constitute a "search."[24]

The *Ortega* case shows that the reasonableness of an employer's invasive conduct is assessed only when there is a reasonable expectation of privacy.[25] In this case, the argument focused on the legitimacy of warrantless searches of the workplace. According to the court, these searches must be deemed legal in exceptional circumstances when the burden of obtaining a warrant is likely to frustrate the governmental purpose behind the search.[26] According to the *Ortega* court, the realities of the workplace can create such exceptional circumstances.[27] Furthermore, the court states that both the inception of the search and the scope of the intrusion into the employee's privacy must meet the standard of reasonableness.[28] In the case of an investigatory search, reasonable grounds for suspicion of misconduct would meet this standard at the inception of the search.[29] The scope of the search would be reasonable when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct.[30]

As mentioned, by giving notice, it is easy to erase any expectation of privacy, resulting in a situation in which an employer can invade privacy as much as he chooses as his conduct will not be assessed. The reasoning behind this is that an employer's conduct can be unreasonable only in cases where the employee has a reasonable expectation of privacy. It is questionable whether this reasoning is rational. Even when an employee knows that his employer can monitor him, excessive conduct from the employer can still be damaging. In this respect, economic as well as psychological damage is imaginable, especially since the work sphere and the home sphere have become more and more interrelated.[31] On one hand, this leads to the situation in which employees have private prop-

23. Kyllo v. United States, 533 U.S. 27, 34 (2001).

24. Peter Caldwell, *GPS Technology in Cellular Telephones: Does Florida's Constitutional Privacy Protect Against Electronic Locating Devices?*, 11 J. Tech. L. & Pol'y 39, 44 (2006).

25. O'Connor v. Ortega, 480 U.S. 709 (1987)

26. *Id.*

27. *Id.*

28. *Id.*

29. *Id.*

30. David J. Phillips, *Privacy and Data Protection in the Workplace: the U.S. Case, Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, IT & Law Series 7, 42 (2005).

31. *See* Earnest & Young, *ICT Borometer*, http://www.ict-barometer.nl/rapporten.php (last visited Oct. 2, 2007).

erty or information present at their work office. On the other hand, business property and information are used or accessible at employees' homes. As evidenced by a yearly survey conducted by Ernst & Young, employers can even reach their employees on holidays by means of mobile phone or laptop.[32] As such, the reasonableness of employers' conduct is an aspect that should be taken into account separate from the reasonable expectation of privacy, and it should be possible to attach legal consequences to this conduct.

To conclude, it must be noted that even though U.S. courts do acknowledge a constitutional right to personal, autonomous privacy, they are reluctant to protect a right to control information, also known as the disclosural privacy right.[33] Tort law does offer a remedy against public disclosure of private facts; however, both elements are problematic in an employment relationship. "Public disclosure" is defined as disclosure to the public in general. Publishing data on a website only accessible to a restricted group of people, for example the management team of a company, does not meet this definition. Moreover, the disclosure of facts related to the employment relationship is not generally covered by the notion of private facts.[34]

2. *Electronic Communications Privacy Act*

More specific rules regarding monitoring of electronic communications can be found in the Electronic Communications Privacy Act ("ECPA").[35] Even though this Act prohibits intercepting of wire, oral, and electronic communications (which is interpreted as encompassing e-mail) and accessing stored communications, the exceptions to these prohibitions diminish their effect, making them virtually non-existent in the employment relationship. The first exception worth mentioning is the "provider exception." A broad interpretation of this exception allows

---

32. *See Id.* (There are several reports regarding ICT and work relationships which analyze ICT's influence on employee vacations. For example, Employers request, in 24% of the cases, that their employees are accessible during holiday, either through their mobile telephone or laptop.).

33. Caldwell, *supra* note 25, at 49; *see also* Whalen v. Roe, 429 U.S. 589, 605-06 (1977) (The court distinguishes between the "interests in independence in making certain kinds of important decisions" and "individual interest in avoiding disclosure or personal matters." The former interest is termed "privacy of autonomy" while the latter is termed "disclosural privacy." Although the court has repeatedly recognized the constitutional right to privacy of autonomy, disclosural privacy is rarely recognized. If recognized, it is rarely found violated.); *see also Index of /pub/97-98/bill/asm*, Number 1323_cfa_19970516, http://info.sen.ca.gov/pub/97-98/bill/asm (last visited Nov. 29, 2007).

34. Jill Yung, *Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should do About It*, 36 Seton Hall L. Rev. 163, 192 (2005).

35. 18 USCS §2510 (2007).

any private employer with a computer or network that stores e-mail communication to access this communication. The second exception is the "consent of the employee" exception, where the employer can monitor Internet and e-mail communications with the consent of employees. Consent can easily be obtained because the refusal of employees to give their consent will have consequences, and moreover, implicit consent is sufficient. When employers monitor employees, implied consent may be achieved when an employer gives prior notice to his employees that he will monitor e-mail communications.[36] The third exception relates to the "normal course of employment." This exception is applicable, for example, if an employer can show that monitoring was necessary to protect his company's property or if the monitoring was performed in order to provide the communication service in a proper manner.[37] Once an exception applies, the ECPA "places no restrictions on the manner and extent of monitoring, nor does it require that an employer notify employees of monitoring."[38] However, with regard to the "normal course of employment" exception, case law does require the employer to notify his employees about the monitoring.[39]

With respect to the foregoing discussion, it is important to mention that labeling e-mail communications or computer folders as "private" does not affect the employer's right to monitor these communications and folders.[40] Early judgments concerning paper mail and lockers acknowledge that individuals have a reasonable expectation of privacy regarding personal mail and personal belongings behind locked doors.[41] In the *Vernars* case, the court reasoned that individuals have a reasonable expectation that their personal mail, addressed to them and marked personal, will not be opened and read by unauthorized persons, even if the mail was delivered to the corporation's office.[42] To date, no court has extended this same logic to distinguish between personal and business e-mail communications.[43] The argument used to sustain this difference is that an employee is issued a locker with the specific purpose of storing personal belongings, whereas a computer is, in principle, provided solely

36. Rustad & Paulsson, *supra* note 2, at 29.

37. Arias v. Mut. Ctr. Alarm Serv., 182 F.R.D. 407 (S.D.N.Y. Sept. 11, 1998); *see also* Rustad & Paulsson, *supra* note 2, at 32 (explaining that the court's definition of what was included in the ordinary course of business exception was so broad in the *Arias* case, that it even included surveillance of conversations about personal relationships at the company).

38. Kesan, *supra* note 8, at 299.

39. Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001); Rustad & Paulsson, supra note 2, at 30.

40. Vernars v. Young, 539 F.2d 966 (3rd Cir. 1976).

41. *Id.*; K-Mart v. Trotti, 677 S.W.2d 632 (Tex. Ct. App. 1984).

42. *Vernars*, 539 F.2d 966.

43. Rustad & Paulsson, *supra* note 2, at 25.

for employment-related reasons.[44] Also, the accessibility of e-mail during transmission over the network is reason to judge that the reasonable expectation of privacy regarding e-mail is different form that of a sealed letter. This argument even precludes protection of stored e-mail communications when they are protected with a personal password.[45]

3. *Employment Law*

In the U.S., employment and labor law seems to play a much less important role in employee protection from Internet and e-mail monitoring by employers.[46] Within individual labor contracts as well as in more general codes of conduct, employers are free to determine the use and control of the Internet and e-mail within the company.[47] These rules do not seem to be bound to specific terms and conditions, and employees do not have much of a choice but to accept the rules.[48] It is possible for employees to negotiate for clauses in their collective bargaining agreement that would place some restrictions on their employers' use of information obtained from surveillance systems. However, this possibility is only feasible for unionized employees.[49]

With regard to the termination of employment relationships, the doctrine of employment at-will still provides the general rule.[50] Pursuant to this doctrine, employers and employees have unlimited discretion to terminate their employment relationships at any time for no reason,

---

44. McLaren v. Microsoft Corp., 1999 Tex. App. LEXIS 4103 (Ct. App. 1999).

45. Rustad & Paulsson, *supra* note 2, at 40.

46. Matthew T. Bodie, *The Potential for State Labor Law: The New York Greengrocer Code of Conduct*, 21 Hofstra Lab. & Emp. L.J. 183, 185 (2003) (stating labor law provisions govern the collective bargaining relationship between employers and their employees' representatives. Employment law provisions regulate the individual employment contract, usually by requiring or prohibiting certain terms of employment). In the United States, Section 8(a)(5) and (1) of the National Labor Relations Act requires notice and an opportunity to bargain in case of installing and using surveillance cameras in the workplace. *See* 11 U.S.C. § 365 (2006). This, however, does not extend to other monitoring devices used to control Internet and e-mail use. In the Netherlands, the employer needs the consent of the works council when he intends to implement, alter or withdraw rules on the processing of employees' personal data and concerning decisions aimed at the observation or control of employees' presence, behavior and output. Works Council Act, Art. 27. Even though this provision is applicable to Internet and e-mail monitoring, Article 27 does not play an important role in Dutch case law concerning this issue.

47. Blanpain & Colucci, *supra* note 5, at 138 (explaining that the National Labor Relations Board affirmed that an employer's e-mail policy which prohibits non-business e-mail use can be prima facie valid and fairly applied).

48. This practice is also criticized in view of privacy. *See, e.g.*, Phillips, *supra* note 22, at 59 ("Terms of employment, including privacy provisions, are negotiated in the labor market. This reliance on the market as a policy mechanism for privacy protection reinforces and exacerbates unequal power relations between employers and employees.").

49. Yung, *supra* note 35, at 181.

50. Jacobs, *supra* note 5.

even if the decision to terminate is based on false information, without being thereby guilty of a legal wrong.[51] This doctrine has declined over the years in the sense that several exceptions to the at-will doctrine have been acknowledged in case law because of the growing awareness that employees are in a weaker position than their employer.[52] The acknowledgement of the different exceptions varies from state to state.[53] The three exceptions most commonly accepted are: (1) breach of an implied contractual right to continued employment;[54] (2) terminations contrary to public policy; and (3) violations of an implied covenant of good faith and fair dealings.[55] These exceptions mainly focus on the existence and breach of contractual or implied procedures governing termination and the absence of "just cause" regarding the termination of the employment relationship.[56] In cases concerning dismissal based upon evidence obtained by Internet or e-mail monitoring, "just cause" is not the problem. The legality of the way in which the cause was obtained and the admissibility of the evidence is contested. With regard to Internet and e-mail monitoring, the best option for employees might be to claim wrongful termination because the termination was contrary to "public policy," in the sense that employees' right to privacy was violated.[57] In the *Borse* case,

51. *See* Electronic Privacy Information Center, *Workplace Privacy*, http://www.epic.org/privacy/workplace (last visited May 24, 2007).

52. The employers' power to terminate at will has not been absolute for some time. Major pieces of federal legislation protect the employment rights of minorities, union members, persons over the age of 40, and persons with disabilities. *See, e.g.*, Title VII of the Civil Rights Act of 1964, 42 U.S.C. 2000 (2007); Civil Rights Act of 1991, 42 U.S.C. 2000 (2000); National Labor Relations Act, 29 U.S.C. 158 (1968); Age Discrimination in Employment Act of 1967, 29 U.S.C. 621 (2001); Americans with Disabilities Act of 1992, 42 U.S.C § 12101 (2000); *see also* David H. *Autor, Outsourcing at Will: The Contribution of Unjust Dismissal Doctrine to the Growth of Employment Outsourcing*, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=281418 (last visited Jan. 18, 2008). Engeline Grace van Arkel, *A Just Cause for Dismissalin the United States and the Netherlands* (Doctoral Thesis, Erasmus University Rotterdam), https://ep.eur.nl/bitstream/1765/9080/1/001-552_536974.pdf (last visited Jan. 9, 2008).

53. *See, e.g.*, Smyth vs. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (describing the Pennsylvanian perspective).

54. As opposed to the Dutch situation, written employment contracts are not that common in the United States. Also, the percentage of employees governed by a collective agreement is rather low in the United States, totaling approximately 15 % of the private American business world. Jacobs, *supra* note 5, at 214.

55. Not all states recognize all three exceptions. *See generally* Charles Muhl, *The employment-at-Will Doctrine: Three Major Exceptions*, Monthly Labor Review, Jan. 4 2001.

56. The requirement of just cause is the core of the only state law concerning wrongful discharge; *Montana Wrongful Discharge from Employment Act*, Mont. Code ANN. § 39-2-901 (1987).

57. Jacobs, supra note 5, at 226 (The author mentions the "public policy" exception in the same breath as "surrounding circumstances." "An exception to the at-will-doctrine might exist if the surrounding circumstances of the termination give rise to a tort action. Violation of the right to privacy could be such a surrounding circumstance.").

the Court of Appeals predicted that in any claim where the employee stated that his discharge related to an invasion of his privacy, "the Pennsylvania Supreme Court would examine the facts and circumstances surrounding the alleged invasion of privacy.[58] If the court determined that the discharge was related to a substantial and highly offensive invasion of the employee's privacy, it would conclude that the discharge violated public policy."[59] In *Smyth,* the Court states that the public policy exception to the employment at-will doctrine must be based on a clear mandate of public policy which can be found embodied in the state's common law tort of "intrusion into seclusion." So, from employment law, we return to privacy law in which the protection against the wrongful termination must be sought. As described above, for "intrusion into seclusion" a reasonable expectation of privacy is required. With regard to e-mail and Internet communication, such an expectation is hardly ever acknowledged. Another problem in this respect is that increased employee monitoring powers raise the risk that false inferences can be drawn about employee contact.[60] On the Web site of the Electronic Privacy Information Center ("EPIC"), the following example is given: "An employee might accidentally visit whitehouse.com, a pornographic web site, while attempting to access whitehouse.gov. An employee network monitoring appliance can detect access to the inappropriate site, but not the intent of the employee."[61] The potential that monitoring provides to draw false inferences about employees increases the necessity to have basic due process protections against monitoring such as the right of notice and some opportunity to be heard.

4. *Data Protection*

As opposed to the E.U., where data protection is regulated by two directives,[62] the U.S. does not have federal laws regarding data protection. As a consequence, in the U.S., little if any consideration has been given to providing: (1) surveillance subjects with access or correction rights; (2) requiring purpose specifications, imposing limitations on use

58. Borse v. Piece Goods Shop, Inc., 963 F.2d 611 (3rd Cir. 1992).

59. *Id.*

60. *See* Office of the Federal Privacy Commissioner, Speaking notes for Malcolm Crompton, Federal Privacy Commissioner, Current Workplace Privacy Issues (Oct. 23, 2003), *available at* http://www.privacy.gov.au/news/speeches/sp72notes.doc.

61. *See* Electronic Information Privacy Center, *Workpalce Privacy*, http://www.epic.org/privacy/workplace/ (last visited Oct. 12, 2007).

62. European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 of 31 July 2002.

or disclosure; (3) disposal policies, and (4) other basic fair-information practices.[63] Also, there is no data protection authority with the power to provide a forum for disputes, impose fines on those who invade privacy, or issue other orders. This can be seen as a deficiency, as pursuing cases in court is not always a practical remedy. Litigation can be expensive; plaintiffs can have great difficulty finding lawyers willing to take the cases; proving damages is difficult; and the prospects for relief are uncertain.[64] The problem of representation also exists with regard to wrongful termination cases, as civil lawyers will only represent these cases if high compensation for damages is likely.[65] As described, the chances of a successful claim are very limited with regard to wrongful termination on the basis of illegal Internet and e-mail monitoring. However, if the conclusion of wrongful termination is drawn, compensation under U.S. law can be considerably higher than in the Netherlands.[66]

5. *Employer Liability for Employee Conduct*

Via the recent expansion of the strict liability doctrine of *respondeat superior*, an employer may be held strictly liable for the foreseeable torts and crimes of employees.[67] Sexual harassment can be mentioned as an area of risk for the employer. Without a sexual harassment policy and enforcement of such a policy, an employer risks liability in connection with workplace harassment claims.[68] Additionally, employee use of Internet and e-mail facilities presents the risk of illegal behavior that can lead to employer liability.[69] The increasing burden on employers with regard to liability for actions of their employees is explicitly mentioned in literature as a reason to monitor those actions closely.[70] Employers' lia-

63. *See* Gellman, *supra* note 14.

64. *Id.*

65. Jacobs, *supra* note 5, at 227.

66. *Id.* at 219.

67. Kesan, *supra* note 8, at 311 (referring to M. Ishman, 'Comment', *Computer Crimes and the Respondeat Superior Doctrine: Employers Beware*, 6 B.U. J. Sci. & Tech. L. 6 (2000) and J.E. Davidson, *Reconciling the Tension Between Employer Liability and Employee Privacy*, 8 Geo. Mason U. Civ. Rts. L.J. 145, 147 (1997).

68. *See* B.P. Miller, *Title VII Affirmative Defense in the Real World: Recent Application of Ellerth / Faragher and What They Require*, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=909661 (Aug. 28, 2005) (last visited Oct. 12 2007).

69. *See* Proofpoint Inc., *Outbound Email and Content Security in Today's Enterprise 2006*, http://www.proofpoint.com/id/outbound/index.php? id= (last visited Oct. 12, 2007) (This report provides results from a survey by Proofpoint Inc. May 2006 and shows the importance for companies to reduce legal and financial risks associated with outbound e-mail. Not only confidential or proprietary information bear risks, but also exposure of sensitive or embarrassing information and the improper exposure of theft of customer information.).

70. *See* Phillips, note 31; *see* also Amanda Richman, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 Iowa L. Rev. 1337, 1337-1364 (2000-2001) (noting that

bility for employee action is also a justification for employers to keep tabs on employees' off-duty conduct, as far as this conduct could, for example, lead to threats or workplace safety that may result in liability claims.[71] Accordingly, an employee's private life can, under certain circumstances, become of legitimate interest of the employer, depending on the impact the employee's private life has on workplace responsibilities. Employers risk liability for employee conduct not only in the case of a normal employment relationship, but also in the case of co-employment.[72] Co-employment is a legal doctrine which applies when two businesses exert some control over an employee's work or working conditions.[73] Relationships between temporary staffing agencies and business clients are typical examples.[74] Since 2003, outsourcing is also viewed as co-employment.[75] With regard to the foregoing, in order to improve privacy protection within employment relationships, it might be necessary to soften the concept of employer liability for the fraudulent behavior of employees.

6. *Conclusion*

No general clause regarding the right to privacy, let alone a specific right to privacy within the workplace, exists in the U.S. Still there are three main grounds employees can rely upon in case of Internet and e-mail monitoring by their employer: (1) the Fourth Amendment; (2) the tort of "intrusion into seclusion;" (3) and the ECPA. With regard to the Fourth Amendment and "intrusion into seclusion," the concept of a rea-

---

the rise in claims regarding intentional or negligent employee acts on the basis of the tort of negligent retention, which is an attractive claim because, unlike claims under respondeat superior, negligent retention suits allow recovery for offensive employee acts made outside the scope of employment). *Contra* Yung, *supra* note 35, at 222 (stating that surveillance can also increase the likeliness of employer liability as it widens the ability of employers to control their employees' actions, which is one of the criteria for vicarious liability).

71. Jonathan Canter, *Drawing the Line on Privacy at Work*, http://www.careerjournal.com/myc/legal/19990209-canter.html (last visited Oct. 12, 2007) ("An employer could be liable if it ignores an employee's off-duty conduct. For example, an employer who negligently hires or supervises an incompetent or unfit employee may be liable to those injured because of the employer's negligence."); Yung, *supra* note_35, at 193 ("The few statutes that do protect a more general category of off-duty conduct tent to provide employers with an exception for conduct that conflicts with the employer's business interests.")

72. Ronald E. Wainrib, *Co-employment Raises New Legal Risks in Contingent Workforce Management*, Jan. 15, 2005, http://www.contingentlaw.com/Coemployment.htm.

73. *See id.*

74. *Id.*

75. *Id.* (noting that in December 2003, the Second Circuit Court of Appeals greatly expanded co-employment to include outsourcing firms in the landmark case of *Zheng v. Liberty Apparel Co. Inc*, No. 02-7826 (2d Cir. Dec. 30, 2003)). In *Zheng*, a six-factor test was established to determine whether a company is a joint employer of an employee of a subcontractor.

sonable expectation of privacy prevents proper privacy protection. First, if the employer gives notice of (possible) monitoring, the employee no longer has a reasonable expectation of privacy. Second, employees waive their right to privacy when using an employer's property. Even if a reasonable expectation of privacy is assumed, this interest is outweighed by the employer's legitimate interest in preventing inappropriate or unprofessional communications over its e-mail system. Regarding the ECPA, the exceptions to this law virtually lead to the non-existence of privacy protection in the employment relationship. This is because an employee's use of the employer's computer network implies his consent to the employer's monitoring of this use. Once an employer meets an exception, the ECPA places no restrictions on the manner and extent of monitoring, nor does it require that an employer notify employees of monitoring.

Within individual labor contracts, as well as in general codes of conduct, employers are free to determine the use and control of Internet and e-mail within the company. These rules do not seem to be bound by specific terms and conditions, and employees do not have much of a choice but to accept the rules. Initiatives for improvement of employee privacy within the workplace often focus on "clear and conspicuous" notice before monitoring e-mail or Internet usage of employees. However, they do not focus on a prohibition or limitation on the right to monitor.[76] Several state proposals concerning such prohibition or limitation did not make it into law. Therefore, stronger legal protection for employees against Internet and e-mail monitoring within the U.S. is not to be expected in the near future.[77] Similar to privacy law, employment law in the U.S. does not protect employees from employer conduct that invades employees' privacy. First, this is because the doctrine of employment at will is still the general rule. Second, because the exception to this rule, in the case of wrongful termination based on employers Internet and e-mail monitoring, leads back to the question of whether the employee had a reasonable expectation of privacy.

Another difficulty for employees to contest privacy infringements by employers is the fact that litigation often does not offer a practical remedy because: (1) it can be expensive; (2) lawyers willing to take the case are hard to find; (3) proving damage is difficult; and (4) the prospects for relief are uncertain. In this respect, the lack of a data protection authority in the U.S. and the fact that little consideration is given to fair information practices increases the weak position of employees to protect their privacy in the workplace. Finally, the rules concerning employer

76. Electronic Information Privacy Center, *Workpalce Privacy*, http://www.epic.org/privacy/workplace/ (last visited Oct. 12, 2007) (giving the examples of the Privacy for Consumers and Workers Act (1993, Senator Paul Simon) and the Notice of Electronic Monitoring Act (2000, Senator Charles Schumer) - neither measure left committee).

77. *See id.*

liability give employers a legitimate reason for extensive monitoring of employees' behavior.

The foregoing statements lead to the overall conclusion that in general, U.S. employees have no right to privacy with regard to their use of Internet and e-mail in the workplace.

C. THE NETHERLANDS

1. *Introduction*

In this section, the different legal rules that govern the use and control of Internet and e-mail within the Dutch workplace are discussed. In the Netherlands, no specific legislation exists regarding workplace privacy. Cases are judged on the basis of general rules and regulations laid down in employment law and privacy law. Case law shows that in the Netherlands, similar cases are brought before the court on different legal grounds. Irrespective of the chosen ground, the outcome of the cases can differ. Therefore, it is difficult to draw a general conclusion regarding Internet and e-mail monitoring in the Dutch workplace. However, some general remarks can be made, which make an interesting comparison to the Internet and e-mail monitoring situation in the U.S.

2. *Human Rights*

The Dutch approach towards the right to privacy is based upon the European Convention for the Protection of Human Rights and Fundamental Freedoms ("ECHR") and the European data protection directives.[78] Article 10 of the Dutch Constitution corresponds with these European provisions.[79] Contrary to the U.S., the European Directives, as well as the Dutch Constitution, explicitly acknowledge a right to protection of privacy in relation to the processing of personal data.[80] Westin has labeled this notion as informational privacy, which has become a

78. Convention for the Protection of Human Rights and Fundamental Freedoms CETS No.: 005, Rome 4 November 1950; European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 of 23.11.1995; Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201 of 31 July 2002.

79. Grondwet voor het Koninkrijk der Nederlanden van 24 augustus 1815, *Stb.* 1987, 458. An unofficial translation in English of the Dutch constitution can be found at: http://www.servat.unibe.ch/icl/nl00000_.html

80. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) Official Journal L 201 , 31/07/2002 P. 0037 – 0047; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the

well-known concept in Europe.[81] Unlike the U.S., where the right to privacy in the workplace is questioned, the European Court of Human Rights has explicitly acknowledged this right on the basis of article 8 of the ECHR.[82] This article, as well as article 10 of the Dutch Constitution, can be invoked in relation to public as well as private employers.[8384] Despite the explicit acknowledgement of the right to privacy in the workplace, Dutch case-law reveals that this right is often not mentioned in cases concerning Internet and e-mail monitoring by employers.[85] Instead, other legal grounds, notably employment law concepts, are used to sue employers for invasion of employees' privacy.

3. *Employment Law*

In the Netherlands, just as in the U.S., Internet and e-mail monitoring by employers is regarded as justified because of the risks associated with employee use of these technologies. Article 7:660 of the Dutch Civil Code grants the employer authority over the employee within the employment relationship. Article 7:611 and 6:162 of the Dutch Civil Code

---

processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 31–50 and article 10 of the Dutch Constitution.

81. Alan F. Westin, *Privacy and Freedom* (The Boldley Head) (1967).

82. European Court of Human Rights Portal, http://cmiskp.echr.coe.int/tkp197/search.asp?skin=hudoc-en (accessed Oct. 12, 2007); Eur. Ct. H. R. 16 December 1992 (Niemietz) and Eur. Ct. H. R. 25 June 1997 (Halford).

> 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.

83. Dutch Supreme Court, 19 January 1987, *Nederlandse Jurisprudentie (NJ, Dutch Case Law)* 1987/928.

For the Netherlands, this Convention came into force the 31st of August 1954. Article 8 of this Convention is interpreted in the Netherlands as having horizontal effect; individuals can claim this right in public as well as private relationships.

84. Dutch Const. art. 10 (Provides that: 1. Everyone shall have the right to respect of his privacy, without prejudice to restrictions laid down by or pursuant to Act of Parliament. 2. Rules to protect privacy shall be laid down by Act of Parliament in connection with the recording and dissemination of personal data. 3. Rules concerning the rights of persons to be informed of data recorded about them and of the use that is made thereof, and to have such data corrected, shall be laid down by Act of Parliament.). Translation from Hendrickx, F., *Privacy and Data Protection in the Workplace: The Netherlands*, in: Siaak Nouwt, C. Prins, & Berend Vries, *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy* 140, Information Technology & Law Series 7 (The Hague: T.M.C. Asser Press) (2005).

85. Homan, *infra* note 88 (giving an overview of Dutch case law); *see*, Blanpain, *supra* note 8, at 95-124; *see also* Hendrickx, *supra* note 86.

limit this authority. An employer must act as a "good employer," and his actions must be lawful.[86] In the Netherlands, questions regarding the lawfulness of Internet and e-mail monitoring are most often dealt with in claims concerning wrongful termination.[87] The legality of monitoring as such is not disputed. The dispute concerns the legality of the consequence that is given to the evidence gathered through monitoring, that is, the dismissal of the employee. The termination of the employment relationship, and in relation to that, the legality of the Internet and e-mail monitoring by the employer, is determined by an assessment of the facts of the case. The interests of the employer and the employee are balanced against each other, often without any reference to a legal ground. The inadequate use in employment law of the fundamental right to privacy and the right to data protection, as discussed below, is heavily criticized by Dutch privacy advocates.[88] It is possible to rely on these rights. Not only can a claim be based directly upon article 8 ECHR or article 10 of the Dutch Constitution, the right to privacy can also be interpreted in article 7:611 and 6:162 of the Dutch Civil Code. However, judges do not seem to give significant weight to arguments relating to privacy and data protection. This might be the main reason why privacy and data protection claims do not appear before the Dutch court in cases concerning the monitoring of Internet and e-mail by employers. The three circumstances that are usually taken into account in these cases are: (1) is there sufficient ground to support the chosen means of control; (2) the principles of proportionality and subsidiarity;[89] and (3) the existence of a company code concerning its policy with regard to Internet and e-mail. Case law shows that the existence of a policy regarding use of

86. In the United States a similar duty exists in general contract law: "the duty of good faith and fair dealing" This duty extends to employment contracts, but the practical meaning of this duty is very limited. Article 7:611 of the Dutch Civil Code does not only impose a duty on the employer, but also requires 'good employeeship.'

87. This might be explained through mentioning the fact that the Netherlands have a strict regime concerning wrongful termination, while the compensation awarded for the violation of the right to privacy is close to non-existent. *See* Cuijpers, C.M.K.C., *De prijs van privacy*, Computer & R 6:272 '04 (discussing a Dutch case in which the court concluded that the plaintiff's right to privacy was violated; however, her claim for compensation for damages was rejected and, because her claim was in part rejected, she had to pay for her own costs of suit).

88. Hendrickx, *supra* note 86, at 141 (referring to: M.A.C. de Wit, *Het goed werkgeverschap als intermediair van normen in het arbeidsrecht* 161-164, Deventer: Kluwer (1999); D.J. Kolk and M. Verbruggen, *Het verborgen bestaan van de Wet bescherming persoonsgegevens* 3-10, Arbeids R. 6/7 '02.; L. Bijlsma and T.C.B. Homan, *Toepassing Wbp door Kantonrechter bij ontslag werknemer, de Wbp ontslagen?* 167 (No. 5 Arbeid Integraal 2003).

89. The principles of proportionality and subsidiarity require that Internet and e-mail monitoring must achieve its intended objective but not go beyond what is necessary to achieve this objective. If possible, the objective should be achieved with less intrusive means.

Internet and e-mail by employees is often decisive in cases concerning termination of employment on the basis of the unjust use of these technologies by the employer.[90] In general, termination is justified if a company has a decent code of conduct, otherwise the dismissal might be void. Employees must be properly informed about the existence of a company code of conduct. As such, the code must contain rules regarding: (1) the use of Internet and e-mail by employees; (2) the way in which this use is controlled by the employer; and (3) the consequences of use in violation of the code.

The Netherlands has a strict legal framework regarding the protection of employees against wrongful termination of employment. However, fraudulent behavior by employees justifies termination in almost every case.[91] The fact that the evidence of fraudulent employee behavior was obtained through a violation of the employee's right to privacy often does not change the court's opinion regarding the legality of the termination. On the basis of existing case-law, it can be concluded that a violation of plaintiff's right to privacy very seldom leads to proper legal consequences. The conclusion that the right to privacy is violated is often followed by the statement that this violation was justified.[92] Even if the violation was not justified, case law indicates that this does not necessarily lead to the reinstatement of an employee, the inadmissibility of evidence, or an employer's duty to pay damages.[93] Even European case law reveals that evidence obtained through a breach of a suspect's right to privacy does not have to lead to the exclusion of this evidence in criminal proceedings.[94] It is not unlikely that this ruling may be used in cases where evidence of employee's misbehavior has been obtained

90. J. Bom, *Rechters toetsen gedragscodes* 16-18; People Planit Profit (Autum 2003), http://www.p-plus.nl/beelden/rechters.pdf (last visited Oct. 12, 2007) (Recent case law shows that informing employees of secret camera surveillance is necessary in order for this surveillance to be legitimate. Under circumstances employers can be allowed to make use of secret surveillance camera's. However, employees must be properly informed by the employer about the possible use of these camera's. If not, dismissal based on evidence gathered through this surveillance will be void. In this respect it is of importance that secret camera surveillance is governed by the Dutch Penal Code, Aarticles 139f and 441b. LJN: AR8052, Rechtbank Haarlem, 22-12-2004, 108067 / KG ZA 04-630, *available at* www.rechtspraak.nl).

91. *See* Hendrickx, *supra* note 86, at 141; Kolk and Verbruggen, *supra* note 90; Bijlsma and Homan, *supra* note 90.

92. Dutch Supreme Court, 27 April 2001, *NJ* 2001/421 (*Wennekes*).

93. *Id.*; *See* P. de Hert and B-J Koops, *Privacy is nog steeds een grondrecht. Pleidooi voor de uitsluiting van onrechtmatig bewijs', Ars Aequi 50* 972-975 (2001); Dutch Supreme Court, 27 April 2001, *NJ* 2002/91 (providing information with regard to immaterial damages and noting that reinstatement after dismissal is often rejected because the relationship between employer and employee has been disrupted).

94. *See* Kahn v. United Kingdom, 2000 ECHR (2007), *available at* http://www.echr.coe.int/Eng/Press/2000/May/Khan%20jud%20epress.htm

through a violation of employee's right to privacy.[95] In my view, the lack of consequences for a violation of the right to privacy can be seen as a major defect in Dutch privacy protection.

4. *Personal Data Protection Act*

The Personal Data Protection Act ("PDPA") provides specific rules governing the processing of personal data.[96] Employer monitoring of Internet and e-mail use entails the processing of personal data and as such, is governed by the PDPA. As already mentioned, claims involving the PDPA seldom appear before the Dutch court in cases concerning workplace privacy.[97] A reason for such "concealed existence" of data protection within employment matters might be that judges believe that similar results can be obtained on the basis of "good employership."[98] However, this argument overlooks the fact that the PDPA can bring clarity regarding the vague notion of "good employership." It can give guidance for weighing interests on the basis of this notion. Moreover, the PDPA contains clear rights and duties, and possible violations of such rights and duties must be assessed in order to give an unambiguous answer on the legality of Internet and e-mail monitoring. The core clause of the PDPA itself is an open norm, requiring the processing of personal data to be fair and lawful. The rights and duties that must be fulfilled in order for the processing to meet these requirements are provided in the PDPA.[99]

---

95. De Hert and Koops, *supra* note 94 (recognizing the influence the Kahn judgment has had on Dutch employment case law; violations of privacy are observed, but no proper consequences are attached to this conclusion).

96. This act has it's origin in the duty to implement Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. *Official Journal* L 281 of 23.11.1995. In its Opinion 8/2001, the Article 29 Data Protection Working Group makes it abundantly clear that the rules concerning data processing as laid down in Directive 95/46/EC are applicable to the use of surveillance systems within the workplace: "There should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of e-mail use, Internet access, video cameras or location data." Article 29 Data Protection Working Group, Opinion 8/2001 on the Processing of Personal Data in the Employment Context. EU. Doc. 5062/01/. WP48 (Sept. 13, 2001); see also the subsequent Working Document on the Surveillance of Electronic Communications in the Workplace. E.U. Doc. 5401/01/. WP55 (May 29, 2002).

97. Hendrickx, *supra* note 86, at 141 (referring to de Wit, *supra* note 86, at 161-164 and Kolk and Verbruggen, *supra* note 90, at 3-10).

98. Hendrickx, *supra* note 86, at 141.

99. Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens), *Stb.* 2000, 302 (Act of 6 July 2000 containing rules regarding the protection of personal data) (2006), *available at* http://www.ivir.nl/wetten/nl/wbp.pdf (Unofficial English translation available at: http://www.dutchdpa.nl/indexen/en_ind_wetten_wbp_wbp.shtml).

Briefly put, the PDPA prescribes that the processing of personal data must have a legitimate purpose and that the processing must be proportionate in relation to that purpose. Also, the gathered information may not be processed in a way incompatible with that purpose. Furthermore, the PDPA exhaustively lists the grounds on which the processing of personal data can be based.[100] In comparison to the U.S., it is important to mention that one of these grounds is the consent of the employee. In the U.S., consent of the employee is easily assumed; however, the Dutch requirement that consent must be freely given is often interpreted to the effect that consent in an employment relationship is not possible.[101] This is because of the subordinate position of the employee in relation to his employer. Therefore, Internet and e-mail surveillance must be based on another ground, usually the legitimate interest of the employer. This entails the so-called "privacy check," and can only be used if the interest of the employer to monitor the employee outweighs the employee's interest in privacy. Besides the requirements relating to purpose and grounds for monitoring, the PDPA contains obligations for employers concerning information, security and confidentiality, as well as rights for employees to access and rectify their personal data and to object to the processing of these data.[102]

A final point regarding the PDPA concerns the National Data Protection Authority ("NDPA").[103] This authority is responsible for monitoring the application of the PDPA. The NDPA has an advisory role and provides a forum for disputes relating to the PDPA. The NDPA is also endowed with investigative powers and is authorized to impose an *astreinte*, or fine. The NDPA has published some basic rules for employers on how to establish a sound policy for monitoring employee use of Internet and e-mail.[104] These rules can also be used as guidelines by the

100. *Id.* Article 8.

101. OPINION 8/2001 OF THE ARTICLE 29 WORKING PARTY (2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf. This view is based on Opinion 8/2001of the Article 29 Working Party on the processing of personal data in the employment context: "The Article 29 Working Party has taken the view that where as a necessary and unavoidable consequence of the employment relationship an employer has to process personal data it is misleading if it seeks to legitimise this processing through consent. Reliance on consent should be confined to cases where the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment. Under article 29 of Directive 95/46/EC this working party is established. The Working Party is made up of the Data Protection Commissioners from the E.U., including the Irish Data Protection Commissioner, together with a representative of the E.U. Commission. The Working Party is independent and acts in an advisory capacity.

102. Hendrickx, *supra* note 86, at ch. 2 and 6.

103. College Bescherming Persoonsgegevens, CBP News, http://www.cbpweb.nl (last visited Feb. 15, 2008).

104. College Bescherming Persoonsgegevens, Goed werken in netwerken, April 2002, *available at* http://www.cbpweb.nl/downloads_av/av21.pdf?refer=true&theme=purple.

Dutch courts. However, it is not surprising that no reference to these rules can be found in Dutch case law concerning Internet and e-mail monitoring. This is because the right to privacy and data protection is usually disregarded in these cases.

5. *Employer Liability for Employee Conduct*

The Dutch Civil Code contains provisions regarding employer liability for the conduct of his employees.[105] However, this liability is restricted to "tortuous acts within the scope of his working activities."[106] It is doubtful whether the private use of the employer's property falls within this scope, even during working hours. As far as this author is aware, there is no Dutch case law concerning employer's liability for tortuous acts committed by an employee when using the employer's Internet or e-mail facilities. If the employer is held liable, it is likely that he can reclaim damages from the employee because of his intentional or reckless behavior. However, this would not resolve the damage done to the employer's reputation.

6. *Conclusion*

The description of the Dutch legal situation with regard to Internet and e-mail monitoring gives a rather muddled impression. However, this impression certainly lends itself to some general conclusions regarding the way in which Dutch case law deals with questions relating to Internet and e-mail monitoring within an employment relationship.

There are no specific rules or regulations in the Netherlands concerning workplace privacy. Both Dutch case law and European case law have acknowledged the applicability of the fundamental and constitutional right to privacy, as well as the general rules on data protection within the employment relationship. However, case law shows that these rights do not play an important role in cases concerning Internet and e-mail monitoring. The legality of Internet and e-mail monitoring is in general judged within the context of a wrongful termination suit. The outcome of these cases strongly depends on assessing the facts of the case and weighing the interests of employee against those of the employer. In this respect, the principles of proportionality and subsidiarity play an important role.[107] Depending on the nature of the facts of the case, the balance between the employer's interests and those of the employee often favors the employer. The existence of a company code of conduct regarding the use of Internet and e-mail is often decisive in cases concerning the legality of dismissal on grounds discovered through

105. BW Art. 6:170.
106. *Id.*
107. Bom, *supra* note 91.

Internet and e-mail monitoring. Employees must be properly informed about the existence and contents of such a code. However, it is acknowledged that for some behavior employees should understand that it is not allowed, even though not explicitly forbidden by an employer's code of conduct.

Despite the legislation regarding privacy and the employment relationship, the employee has no strong protection against employers' privacy invasive conduct. The first reason behind this is the fact that an employee's fraudulent behavior legitimizes the violation of his right to privacy by his employer. The notion of 'fraudulent' encompasses criminal activity as well as conduct in violation of the company's code of conduct.[108] The second reason is that the acknowledgement of a violation of the right to privacy is often followed by the statement that this violation was justified. The third reason is that, even if a violation of the right to privacy is not justified, this very seldom leads to legal consequences, such as the reinstatement of an employee, the inadmissibility of evidence, or the duty to pay for damages. This lack of consequences for a violation of the right to privacy might be the main defect in Dutch privacy protection.

D. Comparison between the Netherlands and the United States

Even though privacy advocates in the U.S. refer enviously to the European human rights approach to privacy, the Dutch situation shows that this approach is no guarantee for proper privacy protection. At least not in cases regarding dismissal on grounds discovered through employer's Internet and e-mail monitoring. Even though the paper rules regarding privacy and data protection, as well as those regarding wrongful termination, are stricter in the Netherlands than in the U.S., it is questionable whether in practice the protection of employees against Internet and e-mail monitoring is not just as weak. The problem with Dutch, as well as European, case law lies in the lack of attaching the appropriate consequences to the finding that the employee's right to privacy is violated. In this respect, the situation in the U.S. might even be more favorable, at least with regard to compensation for damages.[109] If a violation of privacy is found in the United States and damages are awarded, the amount is most likely to be higher than if the case had been

108. *Id.*

109. *Supra*, pt. I.B. As seen in the subsection regarding labor law, reinstatement was not awarded. However, the question is whether reinstatement will also be the course of action to take in claims regarding wrongful termination. With a view to the high claims for compensation in the United States, it might be more beneficial to sue for damages than to claim reinstatement.

tried in Europe.[110] Whether the U.S. employee is better off in the long run depends not only on the amount of compensation awarded, but also on the legal framework regarding unemployment benefits. Even though in the Netherlands the social safety net is better equipped then in the U.S., this reality does not legitimize the statement that in the long run the Dutch employee is better off. As already mentioned, in this respect, the amount of damages awarded is an important factor, but mention can also be made of studies showing that unemployment benefit schemes can hamper reintegration into the workforce.[111] Further research into this subject is needed in order to give clear insight into the position of the employee after termination in violation of privacy rights. Without proper compensation, the value of the right to privacy remains inconsequential. Thus, without pleading for an American-like claim culture with exorbitant claims for damages,[112] it is essential to compensate for the damages suffered through the violation of the right to privacy in order to give this right some practical meaning.

It is also true that if violation of privacy is hardly ever acknowledged and no proper protection exists against the power of employers to end the employment relationship at will, higher compensation for a breach of privacy or wrongful termination in the U.S. remains without value. Undoubtedly, there are some major defects regarding the current U.S. protection against far-reaching employer power in cases concerning Internet and e-mail monitoring. The most important defect might be that the conclusion that employees do not have a reasonable expectation of privacy in Internet and e-mail communications over an employer's network is too easily drawn. As a consequence, no further attention is given to the means and intrusiveness of the monitoring. Also, on the basis of the ECPA, the surrounding circumstances, like scope and duration of the monitoring, do not play any role as soon as one of the ECPA's exceptions is applicable. In this respect, mention can also be made of the fact that an employee's consent to monitoring is too easily assumed in the U.S. As such, the U.S. approach toward Internet and e-mail monitoring favors the employer's position unacceptably.

---

110. Jacobs, *supra* note 5, at 219 (Compensation based upon intrusion of tort law is higher than compensation for breach of contract. In general, claims for damages are substantially higher in the United States than is the case in the Netherlands.).

111. P. Van Rompuy, *De Houdbaarheid van de Europese Welvaartstaat', K.U.Leuven Departement Economie*, Leuvense Economische Standpunten (October 2005), http://www.econ.kuleuven.be/CES/les/LES112.pdf; A. Van der Horst, *Structural estimates of equilibrium unemployment in six OECD Economies*, CPB Discussion Paper No. 19 (June 2003), http://www.cpb.nl/nl/pub/cpbreeksen/discussie/19/disc19.pdf.

112. *See* Hartlief, T., 'Leven in een claimcultuur: wie is er bang voor Amerikaanse toestanden?', *Nederlands Juristenblad,* (Dutch Legal Journal) 2005-16, p. 830-834. Undoubtedly there are also big disadvantages to high claims and awards for damages. In the Netherlands the discussion about the pros and cons of a 'claim culture' is on-going.

The same can be concluded with regard to the termination of employment relationships. The legal proposals to enhance privacy within the workplace focus on transparency. While a policy concerning the use of Internet and e-mail facilities is preferable, this is, arguably, only the case if the content of an employer's code also takes into consideration the interests of employees as well as the principles of proportionality and subsidiarity. A company code should not be a one-way declaration by the employer in which he can nullify all legitimate interests of employees. The lack of consideration towards employee interests and the way in which monitoring is conducted, constitute the main defects in the U.S. protection against Internet and e-mail monitoring. The conclusion that no reasonable expectation of privacy exists should not lead to a situation in which an employer is free to do whatever he wants. There should be ground rules to protect the employee that can be found in the principles of proportionality and subsidiarity, but also in general rules regarding fair information practices. At least the possibility to apply less intrusive means of surveillance—such as filters, block lists, or firewalls—should be taken into account, as well as the level of monitoring.[113] Also, the way in which the information obtained will be used, stored, and disclosed should be elucidated. This course of action might lead to employees regaining some kind of privacy expectation, which also has consequences with regard to the public policy exception to the employment at will doctrine in cases concerning wrongful termination. Another issue to be addressed is the concept of consent of the employee within the employment relationship. This concept should be surrounded with some guarantees to counterbalance the subordinate position of the employee. Contrary to other authors who strongly plead for better or more legislation in the U.S.,[114] a reinterpretation of existing rules could lead to better protection of workplace privacy.

Another problem that needs to be resolved, both for the Netherlands and the U.S., is that of access to the courts. The main barriers are the cost of litigation and the uncertainty with regard to the award of damages. In the Netherlands, the limited height of damages is even an additional burden regarding access to the courts. The NDPA offers some relief, but cannot fully compensate for the threshold towards litigation. For example, the NDPA cannot order the reinstatement of employees.[115]

113. Monitoring can have different gradations. For example the lowest gradation might be scanning the volume of sent e-mail messages or checking the time spent on the Internet on a section level. The most intrusive means of monitoring is assessing the contents of e-mail messages and visited Web sites on an individual level.

114. *See* Yung, *supra* note 35, at 163-222; *See also* Richman, *supra* note 72, at 1337-1361.

115. *See* Personal Data Protection Act, *supra* note 99, at ch. 10. (listing the authorities of the act).

The practical value of the NDPA is also diminished by the fact that dispute resolution is not the NDPA's main priority.[116] Nevertheless, a data protection authority could prove its value in the U.S. by providing guidance on fair information practices, which at this moment do not seem to play any role in the U.S. [117]

III. POSITIONING SYSTEMS

A. INTRODUCTION

With positioning technologies, a new kind of employer surveillance is emerging.[118] From the load of advertisements on the Internet about black boxes, Global Positioning Systems ("GPS"), and Radio Frequency Identification ("RFID") chips, it becomes clear that these new technologies are booming business. These technologies enable employers to pry into an employee's private life, maybe even more than is the case with Internet and e-mail monitoring. The scope of the surveillance can be extended beyond company territory, as well as beyond working hours. For Internet and e-mail monitoring, this is only the case if employees can access the company's network through their home computer and this use is monitored.

However, this merely gives an insight in the employee's virtual whereabouts, whereas positioning technologies can give an insight in the employee's actual whereabouts. As a consequence, the boundaries between the private sphere and the employment sphere become blurred, making possible a state of total disciplinary control by the employer.[119] As such, positioning systems might be more intrusive within the employment relationship than is the case with Internet and e-mail monitoring. Therefore, it is important to compare these two types of monitoring, and to inquire whether it is likely that positioning systems will be dealt with in the same manner as Internet and e-mail monitoring and what consequences this might have on the employer-employee relationship.

---

116. *See* College Bescherming Persoonsgegevens, Uitgangspunten en beleidsregels klachtenbehandeling http://www.cbpweb.nl/documenten/bel_klachtbehandeling.stm?refer=true&theme=purple (last visited Oct. 12, 2007). The Dutch Data Protection Authority has a strict selection policy in dealing with complaints.

117. *See* Yung, *supra* note 35, at 217-218. Even though there is no Data Protection Authority within the U.S., there are some agencies that could perform a role in protection of employees against employer surveillance by means of localization techniques , such as the Department of Labor, the Equal Employment Opportunity Commission, and the Federal Trade Commission.

118. In this article the terms 'positioning' and 'localization' will be used as synonyms.

119. Roberto Fragale Filhot and Joaquim Leonel de Rezende Alvim, *Information Technology and Workers' Privacy: Old and New Paradigms*, 23 Comp. Lab. L. & Pol'y J 527, 527-532 (Winter 2002).

Before addressing this issue, the characteristics of the four best-known positioning technologies will be briefly discussed: video surveillance; RFID tags; Cell ID; and GPS.[120] All of these technologies can be used for several purposes. In this article only the functionality of localizing employees is assessed. At least for now, video surveillance and RFID are best suited for application within a confined workspace.[121] Cell ID and GPS involve local and global positioning. Even though video surveillance and RFID bear their own privacy risks, which will be touched upon later in the article, the main focus in this section lies with the extended scope of employer surveillance outside the company's premises and outside working hours.

B. Video Surveillance and RFID

Video surveillance resembles the monitoring of Internet and e-mail to a large extent. The installation and use of video surveillance in the workplace has already been the subject of several court decisions. For video surveillance to be admissible, the main two questions are whether the surveillance takes place in a public or a private space and whether a reasonable expectation of privacy exists.[122] The first question is difficult with respect to workplace privacy because it is not clear whether a workplace should be seen as a public or a private space.[123] The second question is often answered in the negative, especially if the employer informs his employees about the video surveillance.[124] The reason for video sur-

120. *See* James C. White, *People Not Places: A Policy Framework for Analyzing Location Privacy Issues*, Electronic Privacy Information Center, Spring 2003, http://www.epic.org/privacy/location/jwhitelocationprivacy.pdf (suggesting that the reference to these four positioning systems does not exclude that other technologies can be used for the same purpose. For example, when wireless access to the Internet becomes readily available, WIFI and Bluetooth present privacy issues as the access points a user employs become easy to identify, it becomes possible to use the Internet to track the location of mobile users).

121. Ronald Leenes & Bert-Jaap Koops, *'Code' and Privacy: Or How Technology is Slowly Eroding Privacy*, The Hague, 43 (Asscher Press 2005), *available at* http://ssrn.com/abstract=661141 (Provides the following examples of RFID use: Employers in harbors are equipped with tags, allowing a detailed log of who has been involved with particular shipping containers, and RFID cards in Alexandria Hospital in Singapore were used for patients visitors and staff after the SARS outbreak in order to trace all movements of people within the hospital.).

122. R. Gellman, *A General Survey of Video Surveillance Law in the United States*, in: J. Nouwt, B.R. de Vries and J.E.J. Prins, *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, IT & Law Series 7, Den Haag: T.C.M. Asser Press (2005).

123. *Id.*; *see also infra* pt. I.B.1 (explaining that the work sphere and private sphere become more and more interrelated).

124. Sixto Ortiz Jr., *Technology The Boss Uses To Spy on You*, Enterprise Security Today, October 11, 2006 http://www.enterprise-security-today.com/story.xhtml?story_id=111000CXP653&page=4.

veillance is often control over the work process or the gathering of evidence of fraudulent employee behavior. However, video surveillance can also be used to track and trace employees within the premises of a company. A network of video surveillance is also possible in a larger context, for example to trace traffic violations. Ultimately, unless employers are granted access to these kinds of existing systems, it is unlikely that they will provide such a system themselves. The costs relating to the installation of such a network are too high, especially with regard to existing alternatives like Cell ID or GPS. The network connected to these technologies already is in place and open for commercial use.[125] Video surveillance, therefore, will be left out of the discussion as the extended risks for privacy related to the use of positioning systems are more closely connected to the localization of employees outside the company's premises.

RFID is a generic term for technologies that use radio waves to automatically identify individual items and is currently often explored for military, health, and retail purposes, but it is also used in workplaces as access-control mechanisms.[126] An RFID system consists of a tag capable of transmitting, and sometimes receiving, information by means of radio waves.[127] The radio signals can be picked up by a radio receiver for further processing.[128] Tags can carry chips or sensors. Passive tags are activated by the reader, active tags contain a power source and an active transmitter capable of sending the signal over a larger distance (sometimes up to several kilometers, although normally much less).[129] Because of this, RFID is not suited for the global positioning of employees. With regard to the positioning of employees within company premises the use of RFID does not seem to be more invasive to privacy then the use of video surveillance. However, with RFID it is possible that the points of time an employer passes certain readers are directly stored and processed within an underlying database, which even might be linked to other databases. Moreover, because data can be gathered over a distance and without direct contact, the possibilities for secret surveillance increase.[130] Nevertheless, Ronald Leenes and Bert-Jaap Koops conclude

125. Adam Theiss, David C.Yen & Cheng-Yaun Ku, *Global Positioning Systems: an analysis of applications, current development and future implications*, 27 Computer Standards and Interfaces 89, 90 (2005), *available at* http://www.elsevierscience.com (stating that in 1993 GPS was opened for civilian use both in the United States and internationally).

126. C.M. Roberts, *Radio Frequency Identification (RFID)*, Computers & Security 25, 18-26 (2005), *available at* www.sciencedirect.com.

127. *Id.*

128. Leenes, *supra* note 96, at 42.

129. *Id.*

130. J. Verwer, 'Werknemers en RFID, in *Privacy en andere juridische aspecten van RFID: unieke identificatie op afstand van producten en personen,* 73, 80 Nederlandse Ver-

that the current applications of RFID are fairly straightforward and do not tilt the privacy balance too much.[131]

However, future and widespread use of RFID can certainly become a major threat to individuals' privacy. For example, this threat is related to the linkage of data stored on different RFID tags or the linkage of such data to external data, for example stored in databases. This combination of data can lead to profiling and monitoring of individuals. However, corporations, as well as the government can also keep track of people by following the tags they wear or carry. Since tags can have an individual identification code, tracing individuals is possible.[132] If and to what extent RFID will become a threat to privacy will depend on how RFID tags will be used, for how long, who will be able to read them, and under what conditions they are used.[133]

At this point, RFID tags seem interesting for employers to use as a system of access to and within the company's premises. RFID tags on personal cards can grant or deny an employee access to certain parts of the company. It is also possible to follow an employee's trail within the company by checking all the RFID readers he passed. This may have privacy implications, for example the detection of an amorous company affair. But this could just as easily be discovered through other means of surveillance such as video surveillance, e-mail monitoring, or gossip. Another interesting use of RFID tags could be to protect company assets. Not the employee, but the asset can be tagged. If the RFID tag passes the reader at the door, this will be recorded. In combination with employees' personal cards, it is possible to identify who left the company's premises with what company asset. As previously mentioned, better alternatives exist for employers tracking employees outside the company.

---

eniging voor Informatietechnologie en Recht (Den Haag: Elsevier Juridisch 2005), *available at* http://www.nvvir.nl/doc/rfid-tekst.pdf; *see also* M. Jeffery, *Information Technology and Workers' Privacy: Introduction*, 23 Computer Labor L. and Pol'y J. 251, 251-280. However, it is questionable whether this is unique for RFID or is more closely related to the general introduction of the personal computer. Jeffery rightfully states that computers have made it practically possible to collect piles of data, to store them, to search them and to compare them against other piles of data, without unbearable cost and time for the employer. The processing capacity of computers also allows them to be used as a means of intensive surveillance. Computers Make Surveillance Imperceptible, employers can access any data stored in a "stand-alone" computer or on a networked system without the employees being aware. Any legal rights or opportunities that employees may have to control the processing of their personal data are clearly dependent on their being aware that such processing is being done.

131. Leenes, *supra* note 96, at 44.

132. *Id.* at 45.

133. *Id.* at 46.

C. CELL ID AND GPS

Cell ID and GPS both work with the same kind of principle, but in a somewhat reversed fashion. With Cell ID's a network-based system is able to locate a cell phone.[134] The network knows in which area a phone is located.[135] With GPS, satellites can determine the location of a handheld device.[136] Contrary to the network-based location, the GPS satellite network does not know where the device is. The GPS device itself computes location based on the satellites. Through the combination of a mobile phone or wireless radio transmitter (in a GPS transceiver), or with a disk and program that stores co-ordinates every minute (a GPS recorder), GPS can also give information about the location to third parties.[137] The accurate positioning provided by GPS is created through triangulation, or the process of finding a particular place on earth by knowing the distance between the GPS handheld receiver and three or more GPS satellites.[138] Triangulation is also used to improve the localization with Cell ID.[139] Cell phones can not only be used in Cell ID, but they can also be integrated with a GPS beacon.[140] Also, PDAs are popular carriers for such beacons.[141]

As is the case with Internet and e-mail monitoring, the use of localization technologies by employers can be easily justified. A combination of mobile phone, PDA, and GPS technologies enable businesses to provide an excellent source of communication with their workers in the field. For example, reference can be made to the taxi business. Localization can be used to dispatch the different taxis as efficiently as possible. It can also help to locate cars after they have been stolen. Also, car hijackers might be discouraged from stealing a car that can be traced. Localization may lead to a higher sense of security for car owners and taxi drivers. Moreover, traffic jams could be avoided by diversion based upon information obtained through a GPS unit. However, localization technologies also offer employers the possibility to track and control employees' every move, twenty-four hours a day. The danger lies in the fact that the delicate line between what is employment-related and what is private

134. *See Location Management in GSM*, http://www.volny.cz/drd/gsm/GSMLocationManagement.html (last visited Oct. 15, 2007) (for a technical description).

135. Leenes, *supra* note 96, at 29.

136. *See* Garmin, *Garmin: GPS for Beginners*, http://www8.garmin.com/aboutGPS/manual.html (last visited Oct. 15, 2007) (illustrating a simple GPS explanation).

137. Leenes, *supra* note 121, at 29.

138. Theiss, *supra* note 125, at 91.

139. *See* Leenes, *supra* note 121, at 29 (stating that the same goes for Cell ID where the localization is enhanced by triangulation using the speed and angle with which a mobile phone enters or leaves a cell and comparing signals received by various cells at the same time).

140. Theiss, *supra* note 125, at 98.

141. PDA stands for Personal Digital Assistant.

becomes blurred. Localization is possible on a much wider scale than is possible with just Internet and e-mail monitoring. In fact, employees may not be able to disappear from the employer's sight at all.

The employee can avoid being monitored by not using the gadgets provided by the employer during his spare time, or, if possible, by turning off the functionalities of the localization device.[142] An employer may argue that the employee should not use his cell phone or PDA for private purposes. The employee should leave these devices at home in the employee's spare time so they cannot be traced. However, the employer usually benefits employees with the use of these devices so that the employer can have more access to the employee. For example, in exchange for the permissible private use of a company's cell phone, the employer is able to reach his employee for work-related matters, even when the employee is officially off-duty. This development is closely connected to the abandonment of working nine to five, which is no longer desirable in the new economy. With regard to a company car, there might not even be a choice for employees to leave it in the driveway outside working hours. For a lot of employees it might be too expensive to have their own private car. Therefore, in practice, a lot of employees will also carry traceable devices in their spare time. Without the option to turn off the localization function, the privacy risk of global positioning is lifted to a higher level than is the case with Internet and e-mail monitoring. Similar to Internet and e-mail monitoring, a danger exists in the fact that control can be executed after the fact. Most GPS units offer the possibility to retrieve stored location information. Not only in actual time, but also after acts are committed, the evidence hereof can be retrieved by the employer.

Positioning technologies, like Internet and e-mail monitoring technologies, only link person, time and place. The reason why a person is present somewhere at a given moment in time cannot be detected with the technology. When an employee enters a restricted red light district with his company car, the employee may be doing something wrong or may have just gotten lost .[143] Also, positioning technologies generally establish the position of only the device and not the employee entering the forbidden zone. If the employee's car is stolen, for example, then the positioning technologies would provide misleading information. Location

142. *See* Caldwell, *supra* note 25, at 40 (quoting, "[s]ome sophisticated cellular telephones even transmit GPS location data when the handset is turned off"); *see also* Yung, *supra* note 35, at 173 (explaining further,"[e]ven where the devices appear to be turned off, they still emit signals that can be detected").

143. *See generally* Xora, *GPS Time Track for Workers; Track and Manage Your Workers in Real Time*, http://xora1.securesites.net/timetrack/productinfo.html (last visited Oct. 15, 2007) (selling technology system called a "geofence," which sets off an alarm as soon as an employeeenters a preprogrammed off-limits site).

data obtained through technologies such as GPS can be used to find a reason to fire the employee purely because the employer wants to get rid of him for whatever reason.[144] Technology, and especially those in a developing stage, is not flawless. An employee may find it difficult to prove that his positioning technology malfunctioned. Technology can also be fooled or results falsified beyond the knowledge of the employee.

Triangulation, a function for determining a GPS device's position, is difficult to perform in dense areas. Strong solar flares may also cause device malfunction.[145] Many possible causes for GPS malfunction can be mentioned: atmospheric effects, multipath effects, spoofing and selective availability.[146] Not only may the GPC device malfunction, but there may also be an intentional compromise of the device's accuracy.[147] Therefore, employers should be aware that information gathered through this technology might not always be trustworthy.

D. The Legal System Regarding Internet and E-mail Monitoring Applied to the Localization of Employees

1. *The United States' Approach*

Although proposed in 2001, there is no specific legislation in the U.S. regarding location privacy.[148] The federal statute Title 18, Section 2702 provides a framework regarding disclosure of customer communications or records.[149] This statute provides that persons or entities providing electronic communication services or remote computing services may not knowingly divulge the contents of a communication, nor other information pertaining to a subscriber, such as location data.[150] However, this provision does not offer much protection because of exceptions for the lawful consent of the customer or subscriber.

---

144. Yung, *supra* note 35, at 180) (illustrating an example of an employee fired for his union activities, and not, as alleged, for his inaccurate account of his whereabouts while off the company clock).

145. Steve Bush, *Solar Flares Can Cause GPS Malfunction, Say Researchers*, Electronics Weekly, Oct. 13, 2006.

146. Greg Pendleton, *The Fundamentals of GPS*, Directions Magazine (July 16, 2002), *available at* http://www.directionsmag.com/article.php?article_id=228&trv=1.

147. Bob Brewin, *Homemade GPS jammers raise concerns*, Computerworld.com., http://computerworld.com/securitytopics/security/story/0,10801,77702,00.html (last visited Oct. 15, 2007).

148. Location Privacy Protection Act of 2001, S. 1164, 107th Cong. 1st Sess. (1999). Even if this Act was introduced, it is doubtful whether it would be applicable to employees.This Act was aimed at the protection of the privacy of consumers. This Act not only required notice, but also authorization to use data and a restriction to disclose location data to third parties.

149. 18 U.S.C. § 2702 (2006) (voluntary disclosure of customer communications or records).

150. *Id.*

Besides the federal statute concerning disclosure of communications or records, the general rules as described in section II.B are applicable to positioning technologies. Internet and e-mail monitoring provide insight to a property-based approach that should be followed with regard to positioning technologies. The question of whether an employee has reasonable expectations of privacy is the main issue to be solved.

There are three important factors that affect whether an employee has a reasonable expectation of privacy: (1) the nature of the data; (2) the technology involved; and (3) the voluntariness of handing over otherwise private information to third parties. Regarding (4) the nature of the data, it could be argued that Cell ID and GPS merely provide non content-based data. However, Cell ID and GPS data can disclose a great deal about someone's personal life. The Washington Supreme Court acknowledges this in the *Jackson* case, where the Court refers to the possibility that a GPS device can provide a detailed record of such things as travel to doctors' offices, gambling casinos, the strip club, and the labor rally.[151] The government's recognition of the intrusiveness of new technologies led to the *Kyllo* rule, mentioned previously: "The government can only conduct warrantless searches of constitutionally private information and places if it does so with unenhanced human senses or, at the very least, with sense-enhancing technologies which are in widespread use."[152] According to the *Kyllo* rule, whether one has a reasonable expectation of privacy depends on whether the information could have been obtained through ordinary visual surveillance.[153] Rarely, identical information can be obtained by visual surveillance. Electronic tracking devices may track information for longer periods of time than is otherwise possible through visual surveillance. For example, the use of a GPS device for a month is conceivable; whereas, 24-hour visual surveillance for such a period of time is not.

In *Jackson,* the Court explicitly stated that a person has a reasonable expectation of privacy in his locational data, and that GPS tracking should not be viewed the same as mere visual surveillance. However, in *United States v. McIver,* it was concluded that there was no violation of privacy because the tracking device was attached to the exterior, not the interior, of a car.[154] *McIver* hinged not on the invasiveness of the locational data itself, but the placement of the tracking device. In view of the technological and societal trend towards embedded tracking possibilities within individual's property – such as cars and cell phones – the need to actively place devices becomes obsolete, making the reasoning in *Jack-*

151. Washington v. Jackson, 76 P.3d 217, 223 (Wash. 2003).

152. Kyllo v. United States, 533 U.S. 27, 34 (2001).

153. Caldwell, *supra* note 25, at 67.

154. 186 F.3d 1119 (9th Cir. 1999).

son more likely to prevail.[155] In view of the employment relationship this does not offer any guarantees, as employers can easily nullify existing expectations of privacy by means of notification. Law enforcement may need to obtain a warrant for GPS-surveillance, but employers may perform the same surveillance through agreement, by informing their employees that this kind of surveillance is a condition for employment.

However, case-law shows that in private relations the expectation of privacy depends merely on the voluntariness of turning over otherwise private information to third parties. In *Smith*, the Court found that there was no reasonable expectation of privacy in telephone numbers dialed by an individual in the privacy of his home.According to *Smith*, the individual dialing from his home voluntarily turns over these numbers to third party telephone companies, elimating any expectation of privacy in the numbers.[156]

There is some expectation of privacy with regard to cellular telephone communications in private spaces.[157] However, as described before, rights that go along with this expectation are easily waived within employment relationships. For example, if an employee uses company property like a cell phone or PDA, he waives all of his rights to privacy. The employee no longer has a reasonable expectation of privacy when using company property. Even if it is assumed that the employee has some reasonable expectation of privacy, the employee's interest is probably outweighed by the employer's legitimate interest in preventing inappropriate or unprofessional use of his property.

An employer may be obliged to inform his employees about the use of positioning systems. Case-law on Internet and e-mail provides some guidance on the employer's duty to inform, but the law is also unclear on whether employers have a duty to inform employees about Internet and e-mail surveillance. Under *Smith,* one could conclude that informing the employee is not necessary.[158] However, there are two arguments why employers might be obliged to inform employees about the use of Cell ID or GPS. First, the localization of employees is not as well accepted within society as the use and control of Internet and e-mail. Second, the fact that localization goes beyond the employer's premises, which expands the scope of his control over employees, might require an obligation to

155. Caldwell, *supra* note 25, at 70.

156. Smith v. Maryland, 442 U.S. 735, 742 (1979); *but see* Caldwell *supra* note 25, at 65 (suggesting that several state courts do not treat passing information to the phone company as voluntary disclosure, and, in contrast, the state courts have ruled that individuals do not voluntarily surrender their numbers to their telephone company). As such, under the rationale of several state courts, individuals have a reasonable expectation of privacy with regard to the telephone numbers they dial. *Id.*

157. Caldwell, *supra* note 25, at 57.

158. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996).

inform. This approach has been used in American case law for the use of localization technologies.[159] If an employer's policy informs employees about the fact that their use of company vehicles will be monitored by some kind of localization device, the employee has no reasonable expectation of privacy. The same reasoning applies to policies concerning private use of cell phones and PDA's, regardless of whether they are used as localization devices. The reasoning to be applied to positioning technologies would be the same as that applied to Internet and e-mail monitoring. When using company equipment for Internet and e-mail, the employee waives his right to privacy, especially when there is a code of conduct informing him about the surveillance.[160]

However, even if the employee is informed, the employer's code of conduct is not necessarily reasonable. . From the case law it also appears that with regard to positioning technologies, employee consent to the use of these technologies is assumed.[161] The subordinate position of the employee in relation to his employer should be a factor in the reasonableness determination. It is also questionable whether the factual circumstances surrounding the localization of the employee play any role with regard to the legality of the employer's use of positioning technologies. In this respect, the verdict given by the Oregon Supreme Court regarding an employer's tracking of a company vehicle provides some hope. Even though the court unanimously held that the employee did *not* have an interest "in keeping her location and work-related activities concealed from the type of observation by her employer that the transmitter revealed," the court emphasized that the transmitter disclosed only the vehicles' location, and nothing else.[162] The court refers to two important circumstances that should be part of the reasonableness determination. First of all, the court explicitly mentions that the positioning technology was used on work-related activities. The outcome of the case therefore might have been different if the employee was traced while using the company's car in her spare time, as far as the employer allowed private use of the car.[163] Secondly, the kind of information the transmitter

159. People v. Zichovic, 94 Cal. App. 4th 944 (Cal. App. 6th Dist. 2001); Osburn v. Nevada, 44 P.3d 523 (Nev. 2002); State v. Meredith, 337 Ore. 299 (2004); *see also* Nixon Peabody LLP, *Employers Tracking Device Does Not Violate Employee's Privacy Rights*, Employment Law Alert (2005), *available at* http://www.nixonpeabody.com/linked_media/publications/ELA_01012005.pdf.

160. *See Zichovic*, 94 Cal. App. 4th 944 (stating that individuals have no reasonable expectation of privacy when law enforcement agents attach tracking and electronic monitoring devices to their vehicles); *see also Osburn*, 44 P.3d 523; *see also* Nixon Peabody LLP, *supra* note 159.

161. *See* Nixon Peabody LLP, *supra* note 159.

162. *Meredith*, 337 Ore. 299.

163. If not the positioning of the car could be to gather evidence of inappropriate private use of company property.

makes available is taken into account. The transmitter may reveal the employee's location, but it is questionable whether other information should be made available to the employer.

Unlike in *Ortega*, the Oregon Supreme Court took into account the reasonableness of the surrounding circumstances before a reasonable expectation of privacy was found.[164] The first step towards a more proportionate approach regarding workplace privacy in the U.S. would then have been taken. Also, there should be a second reasonableness test. The second test would not relate to the expectation of privacy, but to the reasonableness of employer surveillance. This second test should not only be introduced with regard to positioning systems, but should also apply to all technologies that have been or will be introduced to enhance an employer's surveillance of his employees. If the general approach towards Internet and e-mail monitoring is applied to positioning systems, then privacy will be degraded to a meaningless concept. The employer would have the right to observe his employees even outside workplace premises and during off-duty hours using the simple argument that, because the employee is using the employer's property, the employee has no reasonable expectation of privacy whatsoever. Informing the employee of the possibility of constant positioning surveillance would further strengthen the employer's position. No rules regarding fair information processing exist in the U.S. The technical specifications of the positioning system can offer the employee some relief if the specifications provide the possibility to turn off this system. However, the employer, on the basis of his property right, may be allowed to forbid the employee from turning off this system, even in the employee's off-duty hours.

The question of whether the surrounding circumstances will improve privacy protection, is also decisive for the acceptance of the public policy exception to the employment at will doctrine, based upon a violation of the right to privacy. Enhancing the chances of a successful claim for such a violation could also decrease the problems that exist with regard to litigation.

2. *The Dutch Approach*

In the Netherlands, some specific provisions regarding the processing of traffic and location data are embedded within the Dutch Telecommunications Act ("Telecommunications Act").[165] These provisions have their origin in European Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communi-

164. *O'Conner*, 480 U.S. 709 (1987).

165. Telecommunicatiewet: Wet van 19 oktober 1998, *Stb.* 1998, 610. English translation can be found in Peter V. Eijsvoogel en Hendrik Jan De Ru, *A practical introduction to the telecommunications laws of the Netherlands,* Dutch Telecommunications Law (2001).

cations sector.[166] The provisions 11.5 and 11.5a of the Dutch Telecommunications Act state that providers of public Electronic Communications Networks and Services are allowed to process traffic and location data only on the basis of consent, unless the processing is necessary with regard to billing purposes or the data have been made anonymous.[167] This legislation may not apply to employment relationships. First, an employee may not be able to freely consent to being tracked and traced by his employer. Moreover, as the provisions in the Telecommunications Act only apply to public networks and services, an employer may easily circumvent these rules by making use of a private localization system.

Besides the provisions in the Telecommunications Act there is no specific legislation in the Netherlands regarding the use of location information. Therefore, disputes arising over this use need to be decided on the basis of existing laws as described in section II.C.

Until now, only one known Dutch case concerned an employer's use of GPS to keep track of his employees in company vehicles. This case has not officially been published, but a description of the case can be found at the Web site of a law firm.[168] According to this Web site, the information of the GPS unit was used to verify an employee's registration of working hours. The employee was aware of the fact that the company car he used during working hours was equipped with a GPS system that registered when and where the vehicle was driven. The records did not match the employee's registration of his working hours. Because the employee could not sufficiently explain the difference in the number of registered working hours, the employer decided to terminate his employment relationship. According to the judge, the evidence obtained through the GPS system was admissible and the termination was justified. The following circumstances were taken into account:

> The employee knew about the GPS unit and its functions so there was no question of unexpected secret surveillance by the employee.
>
> The GPS unit only registered data concerning the location of the employee during a certain time of the working day. So, the system is nothing more than a driven clock. Such a clock is a commonly accepted form of employer control.
>
> The vehicle is a company car which justifies the employer's checking the use of this car during working hours.

The Dutch case seems to apply the same approach as that applied to Internet and e-mail monitoring in the U.S. The core of the case concerns wrongful termination, and the outcome of the case is assessed mainly on

166. *Id.*

167. *Id.*

168. *See* Fillet Advocaten, *De rijdende prikklok*, http://www.fillet.nl/archief/0703.htm (last visited Jan. 15, 2008).

the basis of the facts of the case. The fact that the employee is informed about the surveillance is important. Also important is the type of information gathered through the GPS unit and the hours during which the surveillance took place. These considerations relate to the principles of proportionality and subsidiarity. Also in this case, the assessment of the facts and weighing of interests results in a favorable outcome for the employer. This outcome may also be due, in equity, to the employee's fraudulent behavior. However, this raises the question as to whether fraudulent behavior legitimizes an established violation of privacy. Because of the favorable outcome for the employer, it is not possible to draw a conclusion as to whether an established violation of privacy is useless; no consequences are attached to this violation. If there are minimal consequences in cases regarding localization, as they, in general, in cases regarding Internet and e-mail monitoring, the further degradation of workplace privacy may be inevitable.

IV. CONCLUSION

The foregoing analysis shows that the U.S. as well as the Dutch legal frameworks regarding Internet and e-mail monitoring, and presumably positioning systems as well, do not provide proper guarantees for employees' privacy. Case analysis shows that ICT tends to shift the balance of power between employers and employees in favor of employers. In the Netherlands, appropriate legal rules seem to be in place, but their practical value is often negligible. With regard to the American system, the legal framework offers less protection than is the case in the Netherlands. The U.S. case-law tends to strongly favor invasion of the employee's privacy so long as the employee is informed of the invasion. As mentioned in section III.D, several changes are needed to improve employee protection. Employee protection is needed in order to regain an acceptable power balance between the employer and the employee. This conclusion holds true for the U.S. as well as for the Netherlands.

However, it could also be argued that the American approach towards employer surveillance is justifiable. Why should employers not have an extensive right to check employees' behavior? The employer might be held liable for the employee's behavior, and the employer should be able to check for what activities he is paying wages. Furthermore, the employee is using the employer's property, and the employer should be able to determine and control this use. In other words, the need for privacy protection in the workplace can be doubted. If the employee does not use an employer's property for private purposes, the surveillance of this property cannot invade an employees' private sphere. However, there are several flaws in deferring the employee's right of privacy to the employer's right over his property. First of all, the constant

monitoring of employees can be perceived as an invasion into employees' dignity, regardless of whether this monitoring takes place in the employees' private sphere. Moreover, new surveillance technologies are not confined to the workplace and employees' work-related behavior.

This brings up the second point. The prohibition of the private use of employer's property does not coincide with the reality of the new economy in the United States or in the Netherlands. The private use of the employer's property is often regarded as a kind of fringe benefit. Employees expect some leniency with regard to the private use of company assets, and the employer often encourages this use to circumvent employees' nine-to-five mentality. A lot of companies provide employees with home computers or mobile telephones, which they can use for private purposes. The added value for employers lies in the fact that the employee can be reached for business related purposes 24-hours-a-day. Even if the employer has a strong right to check the employees' behavior, the question arises as to whether this right should extend beyond working hours and company premises. Should an employer have the right to pry into the employees' private relations, and furthermore, is it justified for the employer to attach consequences to an employee's behavior during spare time? In this respect, David Phillips points out that in the U.S.:

> In the absence of public policy to the contrary, private employees are free to discipline or fire workers on the basis of their off-site activities. The public policy barring such discipline may be in the form of state constitutional privacy protections, or explicit legislation. Even though there are some state exceptions to the at-will doctrine, they are relatively rare.[169]

On the basis of Dutch case law concerning Internet and e-mail monitoring, the discovery of employees' fraudulent behavior, even off-duty, might lead to the conclusion that the employer's violation of his privacy was justified. If this violation is not deemed justified, the question remains whether the Dutch court is willing to attach the proper consequences to the employer's actions. Moreover, from Dutch case law concerning the use of private investigators to control employee's behavior, it follows that the reasonable expectation of privacy is not always deemed higher if employees are off-duty or outside the premises of the company.[170]

Third, an unfettered right for employers to control their employees can easily lead to the misuse of this right. When there are no proper safeguards regarding the means applied in executing this control, em-

169. *See* Phillips, *supra* note 31 (referring to an example of a 1993 New York State law that prohibits employers from firing employees for engaging in lawful recreational activities off-duty and off-premises).

170. For example, Supreme Court 18 March 2003, NJ 2003/527 and Court of Appeal 's Hertogenbosch 2 December 1992, NJ 1993/327; *see also* Hendrickx, *supra* note 86.

ployers may misuse this right and leave the employee without recourse. There may be an enormous impact from an unfettered right to control employees in combination with a weak employee protection against dismissal. For example, Michael Rustad and Sandra Paulsson point to the possibility that this right gives employers "the perverse incentive to pretextually terminate employees to save the money from paying retirement or severance benefits."[171] The case *TBG Insurance Services Corp.* v. *Superior Court* is illustrative in this respect.[172] In this case, Zieminski's employment relationship was terminated because TBG learned of Zieminski's repeated accessing of pornographic Internet sites. However, Zieminski alleged that he did not visit those sites intentionally, but that they "popped up" automatically. Furthermore, he sued TBG, alleging that they had in fact fired him to prevent his stock options from vesting. Employers indeed will use surveillance technologies to discover a ground on which the employee can be fired, even though the real reason for termination is related to another issue not severe enough to justify the termination. Employees will have a difficult time provingthat the termination is grounded on a basis other than the fraudulent use of Internet or e-mail facilities. In addition to having negative effects from wrongful termination, loss of privacy can also lead to discrimination. On the basis of the information gathered about the employee by means of monitoring or positioning, the employer can exclude the employee from certain employee benefit schemes.

A fourth, and final, remark that can be made regarding the scope, as well as the means, to control employees is that these both grow larger and more sophisticated each and every day.[173] Because we apply the legal concepts of privacy from older technologies to newer technologies, the employers' right to control employees increases further and further. Greater employer control leads to the complete erosion of employees' right to privacy. In this respect, consider what David Phillips refers to as the "vicious circularity to the practice and justification of ever more invasive surveillance techniques."[174] He illustrates this circularity as follows:

> For example, courts have found that employees reduce or extinguish their reasonable expectation of privacy when they explicitly consent to employers' search policies. Employers, then, demand such consent as a

171. Rustad, *supra* note 2, at 45.

172. 96 Cal. App. 4th 443 (Cal. App 2d Dist. 2002).

173. American Management Association, Internet Monitoring, http://www.amanet.org/research/pdfs/IM_2004_Summary.pdf (last visited Oct. 16, 2007) (stating that the latest report of the American Management Association concerning e-mail and Internet monitoring, '2004 Workplace E-mail and Instant Messaging Survey Summary' states that 60 % of employers use software to monitor incoming and outgoing e-mail).

174. *See* Phillips, *supra* note 31, at 60.

> matter of standard business practice. That standard practice then becomes implicit in the community norms generally governing the workplace surveillance. Eventually, consent to search becomes implicit in the employment relationship.[175]

He concludes his reasoning by stating that "legal arguments around privacy have, on the whole, served to advance the power of employers vis-à-vis their employees."[176] Because technology is slowly eroding privacy,[177] proper guarantees for employees should be created in order to maintain, and even yet, restore, the balance of power between employers and employees. These guarantees must be created both in law, by adapting the legal framework, as well as in technology itself (code as law), in order to rule out abuse of the power that employers increasingly have over employees through monitoring their every move.

---

175. *Id.*

176. *Id.*

177. Leenes, *supra* note 121, at 48. (concluding that technology slowly erodes privacy can be supported by video surveillance, Internet and e-mail monitoring and positioning systems). With regard to video surveillance the public or private nature of the area under surveillance is of great importance. Internet and e-mail monitoring is also deemed justified with regard to e-mail communications and Internet folders which are explicitly labeled private (at least this is true with regard to the United States). The monitoring is also justified with regard to the permitted personal use of employees' equipment during non working hours. The best example is the home computer, which might not only be used by the employee himself but also by his family. Positioning technologies do not only extent to non working hours, but also to surveillance outside the workplace premises. Positioning technology can offer the employer insight into employee's factual whereabouts twenty-four hours a day. *Id.*