BOOK REVIEW

On-line Rights for Employees in the Information Society: Use and Monitoring of E-mail and Internet at Work, Roger Blanpain, editor. (The Hague: Kluwer Law International, 2002, xxi + 280 pp., $102.00US)

reviewed by Paul Roth†

This book contains the papers from a conference held in Brussels in November 2000. The conference was organized by the Royal Flemish Academy in Belgium for Science and the Arts, Union Network International, UNI-Europa (a trade union umbrella organization), and the Euro-Japan Institute for Law and Business. The book consists of 8 chapters dealing generally with privacy at work and the monitoring of e-mail, and 10 chapters on the law and practice in Europe (Belgium, the Netherlands, the United Kingdom, France, Germany, and Italy—three chapters on the latter), Japan, and the United States. All in all, this collection provides useful discussion of relevant issues and a snapshot of developments in a number of countries at the time the material was written. Given the then cutting-edge nature of the topic, there was bound to be relatively rapid development in dealing with issues raised by e-mail in the workplace. In particular, the United Kingdom Information Commissioner is now in the process of issuing an Employment Practices Data Protection Code,[1] and the Article 29 Working Party of the European Union[2] recently adopted its *Working Document on the Surveillance of Electronic Communication in the Workplace*.[3]

There is a degree of repetition across the material presented in this book, a feature that is hardly surprising given the compactness of

† Associate Professor, Faculty of Law, University of Otago, Dunedin, New Zealand.

1. A code on Employment Records (Part 2) is forthcoming, and a further installment on Monitoring at Work (Part 3) is currently the subject of consultation.

2. This Working Party is an advisory body comprised of representatives of the European Commission and Member States. It is established under Article 29 of the European Union Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (95/46/EC). While the opinions and recommendations it issues on European data protection regulation are not legally binding, they are regarded as having great persuasive value.

3. 5401/01/EN/Final, WP 55, adopted on May 29, 2002.

the subject and the broad similarity of workplace cultures and modes of legal regulation in most of the countries covered. There is some indication that perhaps the topic was too narrow in relation to the size of the overall enterprise, as some of the country reports deal with privacy issues that are not really relevant to the on-line situation. This, again, is not surprising as there is not a lot of law in this area, and the subject of this collection comprises but one aspect of the larger area of employer monitoring and surveillance, central to which is the tension between employer prerogatives and employee privacy interests, set against a background of advanced technological developments.

While the country report approach taken in much of this book is illuminating, the collection would have benefited immeasurably from an introductory chapter that compared and contrasted the issues and approaches in the countries that are covered. Books based around country reports often end up comparing apples with oranges, but the nature of the topic covered in this collection particularly lent itself to an overview and analysis that brought the material together. Another criticism is that the book is heavily Euro-centric with the only non-European countries canvassed being Japan and the United States. In other words, the usual suspects have been rounded up. While the nature and degree of regulation in Japan and the United States contrast sharply with that in European countries whose approach is governed by the more strict requirements of the European Union Personal Data Directive, the net could have been cast a bit wider and included at least one report from a country with privacy regulation unlike the sort canvassed in this collection, such as Australia, Canada, Chile, Hong Kong, or New Zealand.

The main part of the book's title, "On-line Rights for Employees," seems odd at first glance. It probably should have ended with a question mark since the existence of such on-line rights seems rather tenuous. Would we have become excited about "typewriter rights" or "telephone rights" a century ago? Several authors go so far as to claim that employees may have a "human right" to use the employer's e-mail facilities for purposes that are not related to their work. It is not made entirely clear, however, why there should be human rights to utilize e-mail facilities, but not the company car.

The main issues that arise in this area are straightforward and generally well-known. The employer has legitimate interests in ensuring that its electronic communication facilities are not misused by employees to betray confidential business information, offend or harass co-workers or clients, or waste working time and resources.

Employers are also entitled to protect themselves from the risks posed by viruses and hackers, and harm or loss arising from the overuse of telecommunications and data systems. Moreover, there are legitimate employer concerns about incurring liability to third parties for defamation, breach of copyright, breach of confidentiality, breach of censorship laws, and the like. Accordingly, some allowance must be made for employers to monitor and control use of their electronic facilities. For their part, employees are entitled to be treated with dignity, fairness, and due process. The general consensus expressed in this collection is that:

> . . . employees do not abandon their privacy rights when entering into an employment relationship. At the same time, an employment relationship implies significant limitations of the right to privacy. The employee's fundamental rights will not be lost, but become qualified by conflicting rights and interests of employer, colleagues and third parties.[4]

While this is true as far as it goes, it begs the question of where the law should draw the line among the various competing interests. The book provides no easy answers and there are probably none to be found in such an area where cases turn largely on issues of fact and degree. However, there are a number of principles that can be brought into play within existing jurisprudence to deal with these issues and the book discusses these in the course of many of its chapters. For example, the concept of "privacy expectations"—how they can arise and their legal significance in various contexts and jurisdictions—is treated well in various places, which taken together forms a valuable contribution to the field. The reader, however, will have to do all the work in bringing the different aspects of this topic together since no one has done it for him.

The concept of "fundamental rights" is often invoked in this book with varying degrees of plausibility. I have my doubts as to the extent, much less the existence, of a "fundamental right to communicate" while at the workplace.[5] Yet more dubious, in my view, is the existence of a "fundamental right of access to information" for employees that should ideally include the right to surf the Internet while at work.[6] Even if there were such a right, there is the further issue of whether or not it would be legitimate to draw a line with

4. Frank Hendrickx, *Privacy and Employment Law: General Principles and Application to Electronic Monitoring*, *in* ON-LINE RIGHTS FOR EMPLOYEES IN THE INFORMATION SOCIETY: USE AND MONITORING OF E-MAIL AND INTERNET AT WORK Ch. 6 (Roger Blanpain ed., 2002).

5. Roger Blanpain, *Introductory Remarks and Some Conclusions*, *id.* at xii. Such a "right" is further discussed in more detail by Frank Hendrickx, *id*. at 47.

6. Blanpain, *id*.

respect to content and, if so, on what basis since a lot of "information" that is sought by employees on the Internet happens to be pornographic. There is an interesting New Zealand case involving two employees dismissed from the same workplace at the same time for Internet misuse. The Court awarded reinstatement to the employee who visited websites related to his interest in genealogical studies, but the employee who visited pornographic sites was denied reinstatement to his position.[7] The basis for this decision may seem obvious, yet at the same time, the result is difficult to justify in principle when, as one of the contributors to this collection notes, "you can legitimately buy pornographic magazines in shops."[8]

A number of the authors discuss privacy generally as a fundamental right that is not lost merely by entering into the employment relationship, but much of the discussion seems somewhat implausible, relying as it does on rights relating to free speech and privacy of communication. With one exception, this seems to me to be the wrong place to look for the fount of privacy rights in the workplace. In my view, the right is based, quite simply, on the fundamental right of workers to toil "in conditions of freedom and dignity," as provided for in the ILO Constitution.[9] This rationale expressly applies in Italy, which "does not have any equivalent of the English word 'Privacy,'" and where the 1970 Workers' Statute "sets narrow boundaries on managerial prerogatives in order to protect a worker's dignity and his private sphere at work."[10]

The one exception, not widely addressed in this collection,[11] is in relation to union-related communications. It would undoubtedly be a breach of the ILO principles of freedom of association if an employer were to intercept union-related e-mail communications as this could

7. Allerton and Offord v. Methanex (NZ) Ltd., WC 23/00, March 28, 2001.

8. Eamonn Sheehy, *Monitoring and Control of Use of E-mail and the Internet by the Employee: Management's Point of View*, *supra* note 4, at 32.

9. Declaration concerning the aims and purposes of the International Labour Organization, adopted by the General Conference of the International Labour Organization, Twenty-Sixth Session, Philadelphia, May 10, 1944.

10. Michele Colucci, *Italian Law*, *supra* note 4, at 197. *See also* Vincenzo Ferrante, *Italian Law*, *supra* note 4, at 204.

11. Thord Wedlin (President, UNI-Europa), *Welcome*, *supra* note 4, at xx, advocates access by employees and trade unions to the employer's Internet facilities for union business. Roger Blanpain, *Employment and Labour Law Aspects. Setting the Scene: Asking the Right Questions?*, *id.* at 40, enumerates a number of issues relating to collective rights, but does not explicitly discuss this exception. Frank Hendrickx, *Belgian Law*, *id.* at 86, 89, and 91, mentions that the concept of freedom of association "implies the principle of non-interference by employers in trade union activities," and suggests that this may impose positive obligations on an employer to make the Internet available for union activities. The fullest discussion of this issue is in the United States country report, in relation to protected activities under the National Labor Relations Act, provided by Matthew W. Finkin, *United States Law*, *id.* at Ch. 16.

constitute "interference . . . in [trade unions'] establishment, functioning or administration."[12] Thus, the ILO Committee on Freedom of Association has stated that:

> The full exercise of trade union rights calls for a free flow of information, opinions and ideas, and to this end, workers, employers and their organizations should enjoy freedom of opinion and expression at their meetings, in their publications and in the course of other trade union activities.[13]

While there is an apparent difference between use of the employer's e-mail facilities on the one hand, and union "meetings," "publications," and "other trade union activities" on the other, in principle, there is arguably little difference in this context between sending and receiving union related e-mails in the workplace and having union related discussions or handing out leaflets in the workplace.[14]

There is also occasional mention of the relevance of electronic communications to homeworking, teleworking, and telecommuting, but no discussion of the full implications of this in relation to what one Dutch case has termed the "privatisation of the workplace."[15] The existence of the Internet has extended the possibilities of employer intrusion into the private lives of employees in other ways as well. There is an interesting discussion in the United States country report of Internet monitoring of employee's activities outside the workplace. Such monitoring may involve screening employee homepages for

12. ILO Convention 98, concerning the Application of the Principles of the Right to Organise and to Bargain Collectively, art 2(1). *See*, by way of analogy, the following Australian cases: Australian Municipal, Administrative, Clerical & Services Union v. Ansett Australia Ltd., FCA 441 (2000) (union delegate unfairly dismissed for use of employer's Internet facilities to advise union members regarding the work of a joint employer/union group; this case is referred to in Thord Wedlin's *Welcome*, *supra* note 4, at xxi); QTU v. Department of Education, QIR Comm. 131 (2000) (e-mail distribution of material critical of employer by teacher standing for union election); and, the New Zealand case of Howe v. The Internet Group Limited (IHUG), 1 ERNZ 879 (1999) (employees dismissed for offensive Internet use during industrial negotiations; Court found an arguable case of unjustified dismissal based, in part, on involvement in union activities).

13. *Freedom of Association: Digest of Decisions and Principles of the Freedom of Association*, Committee of the Governing Body of the ILO, International Labour Office, Geneva, ¶ 152 (4th rev. ed. 1996); *see also* ¶ 153: "The right to express opinions through the press or otherwise is an essential aspect of trade union rights." *See also Freedom of Association and Collective Bargaining: General Survey of the Reports on the Freedom of Association and the Right to Organise Convention (No. 87), 1948, and the Right to Organise and Collective Bargaining Convention (No. 98), 1949*, Report III (Part 4B), International Labour Conference, 81st Session, International Labour Organization, Geneva, ¶ 38 (1994).

14. *See* ILO Recommendation 143, concerning Protection and Facilities to be Afforded to Workers' Representatives in the Undertaking, cl. 15 (1971).

15. Court of Harlem, June 16, 2000.

content and checking what is said about the business in chat rooms and on bulletin boards.[16]

There is occasional reference to the ILO Code of Practice on the Protection of Workers' Personal Data (particularly by Frank Hendrickx in his chapter "Privacy and Employment Law: General Principles and Application to Electronic Monitoring"). This collection might have gone on to address the question of whether there is a need for binding international standards in the area, particularly in view of Peter Johnson's point that "a global networked economy, with larger businesses and world-wide employment markets, erodes the ability of Governments to impose good business practices through legislation."[17] Johnson is a booster of self-regulation, but without an assessment at least of its current implementation and effectiveness at protecting the privacy of consumers (the prime examples of this form of "regulation" being found in the United States and Japan), who is to say that self-regulation could really safeguard employee privacy? It would seem particularly vital that there should be legal guarantees in the employment context. Under data protection legislation generally, data subject consent provides the justification for any privacy intrusion and "procured consent" is especially easy to obtain where there is a disparity in bargaining strength between parties.

One surprising gap in this book is that with the exception of the Dutch and French country reports (and there only briefly),[18] there is little discussion of the law relating to ordinary correspondence ("snail mail") and how this might relate to e-mail. If anywhere, this is where one should look first for the sorts of principles that ought to govern employers' monitoring of e-mail. There is an interesting, but brief, attempt to analogize from one to the other in the chapter by Jay Kesan,[19] which suggests that the privacy expectations with respect to personal e-mail should be no different than those that apply to ordinary mail.

The sending of e-mail is undoubtedly subject to lawful employer control and the possibility of sanctions because the employee is using the employer's equipment and time. The same principles, however, do not necessarily apply to the receipt of e-mail. An important

16. *See* Finkin, *supra* note 11.

17. Peter Johnson, *Employment in a Global Knowledge Economy*, *supra* note 4, at 9.

18. Taufan C.B. Homan, *Dutch Law*, *id.* at 108 and 119; Jean-Emmanual Ray & Jacques Rojot, *French Law*, *id.* at 154-155.

19. Jay P. Kesan, *A 'First Principles' Examination of Electronic Privacy in the Workplace*, *id.* at 257.

distinction, therefore, needs to be drawn here as legal principles governing the receipt of mail addressed to employees at the workplace already exist. Although Eamonn Sheehy draws a distinction between "personal" use and "private" use of an employer's e-mail facilities ("in the work place there may be 'personal' use of equipment and services, but not 'private'"),[20] this distinction does not necessarily apply to the receipt of e-mail addressed to an employee.

It is not uncommon for employers to open employees' mail on the generally sensible assumption that mail addressed to an individual at work relates to business matters rather than the employee's personal affairs. Moreover, in many larger workplaces, systems are in place to open mail automatically, whether or not the envelope is marked "personal," "confidential," or "private."[21] In most countries, however, the opening of mail is governed by specific legislation regulating postal services and the delivery of mail. In common law countries, there are also some judge-made laws that are relevant to the area. For example, merely reading a letter that is already open (without touching it) or a postcard will not incur liability. Such situations might be analogous to the display of an opened e-mail message on a computer monitor. In a well-known phrase, Camden, L.C.J., in the eighteenth century case of *Entick v. Carrington*, stated "the eye cannot by the law of England be guilty of a trespass."[22]

Two nineteenth century British cases shed some light on the common law position in relation to the opening of employees' mail. They elucidate what can be taken to constitute "reasonable cause or excuse" for opening mail as provided for now in the postal legislation of many common law countries. Both cases deal with a situation where a former employee directed that mail be forwarded to a new address, which meant that some mail intended for the former employer was forwarded to the new address and some mail intended for the employee continued to be sent to the former employer's address. It was not always apparent from the face of the correspondence whether it was intended for the former employee personally or in his capacity as an employee. The issue in these cases was whether the employee had any rights with respect to such

20. *See supra* note 8, at 30.

21. The New South Wales Privacy Committee has described such automatic opening of mail as among the more objectionable invasions of privacy in the workplace: *see Employment Guidelines: The Privacy Aspects of Employment Practices in the Private Sector* ¶ 3.2(c) (Sydney, October 1979).

22. 19 HOW. ST. TR. 1030, at 1066 (1765).

correspondence. In both cases, the Courts found that the employer had no absolute right with respect to the opening of such correspondence, but that the employee had rights too.

In the earlier case of *Stapleton v. The Foreign Vineyard Association,*[23] the Court of Chancery refused to grant an injunction restraining the former employer from opening letters addressed to the former employee when they did not have any external indication that they were intended for the former employer. While the Vice-Chancellor stated that "*Prima facie*, letters must be taken to be intended for the person to whom they were addressed," some letters addressed to the employee and sent to the company related to the company's business rather than the employee's private affairs. As a result, the Vice-Chancellor preferred to leave the situation as it was after the defendant company undertook that it would allow the plaintiff to be present when his letters were opened. This undertaking, however, would not prevent the opening of any letter if the plaintiff, on due notice, should not choose to be present for the opening of the letters.

In the later Court of Appeal case of *Hermann Loog v. Bean*,[24] an employer applied for an injunction against a former employee who had resided in the company premises, to restrain him from having the Post Office forward to his new residence letters addressed to him at the company's office. The employee admitted that among the letters that had been forwarded were two that related to the company's business and these he returned to the sender instead of forwarding them to the company. The Court ordered that the Post Office no longer forward letters addressed to the company on to the former employee and that the company instead should be able to open them, but only at specified times during the day when the mail arrived so that the former employee might be present when the letters were being opened. Bowen, L.J., stated:

> . . . letters addressed to an agent at the office of his principal are frequently addressed to him as a servant, though there may of course be among them private letters which belong in law to him. There may be signs which will shew whether the letters belong to the servant or to his master, for instance, words written on the envelope. But the servant has no right, merely because letters are addressed to him, to say that they are his own, if there is nothing

23. 4 New Rep. 217 (1864); 11 LT 77; 28 JP 612; 12 WR 976.
24. 26 Ch. D. 306 (1884).

> on the envelope to shew that they are his own and not his employer's letters.[25]

These cases indicate that where a letter is addressed to an employee at the employer's address, the employer may not open any letter that is clearly for the employee personally. If there is any doubt whether or not it is for the employee personally, the employee still has a right with respect to them, but that right can be qualified in light of the employer's possible interest in them. The equitable compromise reached in both of the above cases was that letters addressed to the (former) employee could be opened by the employer after the employee was given an opportunity to be present to safeguard his privacy interests in them.

Existing legal principles that may be applied to the receipt of e-mail, therefore, include the following:

- Where an employee has received an e-mail message that indicates on its subject heading that it is "personal" or "private," the employer may not open it.
- Where an employee has received an e-mail message and there is doubt as to whether or not the message is private, the employer is not entitled to open it unless the employee is given the opportunity to be present so that its contents can be protected if the message does not relate to the employer's business. This principle would also serve to protect the confidentiality of any of the employee's original outgoing messages that have been quoted in the message that has been received. Thus, employees arguably have stronger privacy rights with respect to what is in their "inbox" than in relation to the contents of their "sent messages" folder.
- An employee cannot be disciplined for something over which he or she has no control. Therefore, it would be impermissible in terms of unfair dismissal laws if an employee were to be disadvantaged for the mere receipt of unsolicited e-mail messages.

In relation to the law relating to on-line privacy in the employment context generally, the summary of the Dutch case law provided in this book can be applied to the situation in most other countries as well. The courts are not attracted by arguments founded on privacy rights and, following this lead, employees tend not to raise them in their own defense. Discussions concerning Internet use and workplace privacy rights are, therefore, largely academic.[26]

25. *Id.* at 316-317.
26. *See* Homan, *supra* note 18, at 108.

The current position, then, is that workplace privacy issues in the courts are generally being treated in accordance with existing employment law, not in terms of privacy rights *per se*. As Matthew Finkin comments in his United States country report, "more has been written about [workplace privacy] law than there is law to write about."[27] Accordingly, the jurisdictions whose law will be the ones to watch will be those with legally enforceable workplace privacy standards: Hong Kong and the United Kingdom.

27. *See* Finkin, *supra* note 11, at 233.