Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Monitoring Employees: Striking a Balance

October 2007

by Ann Bevitt, Marian A. Waldmann, Teresa Basile, Peter J. Edlind, Gordon Milner

Related Practices:

- Employment and Labor

PDF Version

The monitoring of employees' electronic communications can be undertaken for various reasons, and is now standard practice among most, if not all, employers. However, when undertaking such monitoring, employers must ensure that they both comply with legal requirements and do not unduly affect their working relationships with their employees *(see* The Impact of Employee Monitoring*)*.

The regulation of employee monitoring varies greatly between jurisdictions, raising complex issues for multinational employers. For instance, when an employer monitors all of its employees' electronic communications in the course of multi-jurisdictional litigation, there can be a conflict between EC data protection laws and US document retention and production requirements. The US Federal Rules of Civil Procedure require companies to retain all documents that may be relevant to pending and reasonably foreseeable litigation and then, during the discovery process, to search and produce all relevant records. Such an obligation can directly conflict with EC law, which allows individuals the right to object to the processing and cross-border transfer of their personal information. In addition, EU companies can retain information only for the period strictly necessary to accomplish the purpose for which it was collected.

In view of issues such as the above, this chapter:

- Considers the applicable legal frameworks governing the monitoring of employees' e-mail and internet usage in Europe (specifically, Germany, Sweden and the UK), the US and the Asia-Pacific region (Australia, Hong Kong, Japan, New Zealand, South Korea and Taiwan).
- Provides practical guidance on complying with these frameworks (see box, Ensuring compliance: some tips).

Europe

In Europe, the general right to privacy is derived from the:

- European Convention on Human Rights (Convention), which governs the 47 Council of Europe member states (including EU member states).
- Data Protection Directive (*95/46/EC*) (Directive), which applies to EU member states.

There are differences, however, in the way that EU member states such as Germany, Sweden and the UK have implemented the Directive's provisions.

Germany

The monitoring of employees' internet use is governed by employment law, collective agreements, data protection legislation, constitutional and human rights law, and telecommunications law. The result is complex, and whether internet use can be monitored depends on a number of individual

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

circumstances.

As the constitutional and human rights law overlays all other regulation, the general view is that blanket monitoring infringes an employee's rights and, because they cannot be waived, collective or individual agreements to allow blanket monitoring of internet use are unlikely to be valid.

The Telecommunications Act 2004 (*Telekommunikationsgesetz*) specifically provides for the privacy of electronic communications. The law applies in different ways, depending on whether the employer has allowed or tolerated private internet use at the workplace or whether such use is expressly forbidden. It is largely thought that, by expressly or impliedly permitting private use of the internet by employees, an employer becomes a provider of telecommunications services to them. This triggers privacy rights under the Telecommunications Act and the Telemedia Act 2007 (*Telemediengesetz*). These can be waived, within the limits of constitutional boundaries, but an employer that has tolerated private internet use at work without an express written policy may find itself in a difficult position, because it would already be bound by the privacy obligations under the Telecommunications Act and the Telemedia Act, and the workforce or the works council might resist a change of policy.

Where an employer has expressly forbidden private use of the internet at work, data protection law, employment law and the constitutional principles combine to form a set of complicated rules. In essence, where there is no express internet monitoring agreement, individually with the employee or collectively with the works council, monitoring is only allowed to the extent that it is either:

- Based on a concrete suspicion against an individual employee for breaching the internet policy.
- Necessary to assess the employee's performance due to the nature of his job.

Any monitoring must be kept to the necessary minimum and must be announced in advance. If a works council exists, it must expressly consent to each individual monitoring measure.

Because of employers' limited rights to monitor, express agreements with employees or works councils are advisable. However, there is a risk that agreements will be void on the basis that they were obtained under duress, especially if they are wide-ranging and presented as a condition of employment. The best way forward is usually an express detailed agreement with the works council on a policy for the use of technology and its enforcement.

Sweden
The monitoring of employees in Sweden is governed by:

- The Data Protection Act 1998 (*Personuppgiftslagen 1998:204*) (Act).
- Employment legislation.
- Collective agreements with trade unions.

Since the adoption of the Act, the Swedish Data Protection Authority (DPA) has received a substantial number of requests from businesses and public authorities on how the law applies to the monitoring of employees.

In 2002, the DPA carried out a series of inspections of businesses and public authorities to assess the overall application of the law and identify areas of difficulty. Its report was published in 2003 and, following further inspections in 2005, a further report was issued that year (*Behandling av personuppgifter för kontroll av anställda – Datainspektionens Rapport 2003:3 (Processing personal data to monitor employees*) and *Övervakning I arbetslivet – Kontroll av de anställdas Internet- och e-postanvändning – Datainspektionens rapport 2005:3*). In the absence of specific legislation and given that there is limited jurisprudence, DPA guidance remains important in Sweden.

In its 2003 report, the DPA found that employees were often informed that monitoring by the employer might take place, but they were not told of the reasons for it. The report concluded that employers need a proper legal basis for monitoring, that is, one of the following:

- Voluntary, specific, unambiguous and informed consent, retractable with no negative consequences.
- The balance of interests. However, very strong grounds for monitoring are required in this case.

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

- The employee's contract, when monitoring employee performance.

Whichever legal basis an employer uses, all monitoring must conform with "good practice on the labour market" (although this concept is not defined by the DPA).

The DPA's 2005 report also found that employees are in most cases not provided with sufficient information on the extent of the monitoring and that the terms for employees' use of IT equipment generally needs to be better regulated by the employer.

The DPA's 2006 opinion concerning the Swedish pharmacy monopoly (*Apoteket*) sheds further light on the DPA's approach to employee monitoring (*DPA opinion 2006-10-04, see www.datainspektionen.se/pdf/beslut/apoteket_samrad.pdf (in Swedish)*). Apoteket registered in a database the number of prescription products that each employee handled and sold. The pharmaceutical employee trade union complained to the DPA that this practice was contrary to the Act's provisions.

In this case, the DPA found that the Act did not contain any general provisions preventing an employer from monitoring employees. An employer has the right to lead and delegate work assignments, and following up on an individual employee's performance may be justified in this context. As there was no applicable case law on the monitoring of employee performance, and taking into account the fact that labour laws and collective agreements also regulate employee work assignment and performance, the DPA recommended that this question be resolved between the employer and the trade union.

Finally, in a 2006 decision, the DPA found that an employer has a right to monitor suspected abuse of working hour accounts by checking employees' logging in times on IT equipment (*DPA decision 2006-09-22, see www.datainspektionen.se/pdf/beslut/ Sahlgrenska_kontroll%20_av_anstallda.pdf (in Swedish)*). The DPA found that the employer's interest in monitoring the employee outweighed the employee's right to privacy. However, the employer was criticised for not having satisfactorily informed employees of the extent and purposes of its monitoring.

UK

The Information Commissioner, the UK's data protection authority, issued the Employment Practices Data Protection Code (Code) to assist employers in complying with the Data Protection Act 1998, which implements the Directive in the UK. Part III of the Code covers monitoring at work. It recommends that all employers undertake an "impact assessment" before carrying out any monitoring. This involves identifying:

- Whether monitoring is necessary.
- What form it should take to achieve the best balance between employees' rights to privacy and the employer's needs for carrying out its business.

The assessment should address:

- The benefits of monitoring for the employer.
- The adverse impact on employees.
- Whether comparable benefits can be achieved with a less intrusive method of monitoring.
- Whether more closely targeted monitoring can achieve the same benefits.
- Which less intrusive methods of monitoring are available.
- Whether the employer can comply with the further obligations required once it has acquired data as a result of the monitoring.

If monitoring is considered necessary, the employer should assess whether it is a proportionate response to the relevant business need. If disproportionate, the employer should not carry out the monitoring. If the general assessment identifies and justifies the need for monitoring and the type of monitoring, the employer should then carry out a further impact assessment specific to the type of monitoring contemplated.

When monitoring electronic communications, employers should establish a policy on their use and communicate it to employees. The policy should set out clearly:

- The circumstances in which employees can or cannot use the employer's systems for private communications.

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

- The extent and type of private use that is allowed.
- In relation to internet access, any restrictions on material that can be viewed or copied; a simple ban on “offensive material” is unlikely to be sufficiently clear for people to know what is and is not allowed.
- What alternative methods of communication can be used to ensure confidentiality, for example, suitably marked communications by internal post, rather than by e-mail.
- The purposes, method and extent of monitoring.
- How the policy is enforced and the penalties for breaching it.

An employer that carries out full impact assessments need not obtain its employees’ consent to monitor unless it obtains sensitive personal data as a result of monitoring.

Further guidance on monitoring in the Code includes the following:

- Employees should be reminded periodically that they are being monitored and told about any significant changes.
- Employees should be trained to understand the data protection principles that arise when carrying out monitoring.
- The most appropriate person must be chosen to monitor and there should be as few people as possible doing such a task.
- Employees must have the opportunity to challenge and explain a claim that they have used their electronic communications incorrectly.
- Employers must not act inconsistently with their policy. This means that if something is not permitted but they have allowed it or “turned a blind eye”, they can not then rely on the policy when an employee breaches it.

Although the Code is not legally binding, failure to comply with it is likely to be cited in any enforcement notice for non-compliance with the Act. An employer that fails to comply with an enforcement notice is guilty of a criminal offence and may be fined. However, the courts are unlikely to prevent use of the data obtained, for example as evidence in an action relating to an employee’s dismissal.

A recent European Court of Human Rights (ECHR) case (*Copland v UK C-62617/00*) clearly illustrated the dangers of not having a proper technology use policy when monitoring employees’ electronic communications. The ECHR found that an employer’s monitoring of an employee’s e-mail, telephone and internet use was in breach of her right to respect for her privacy and family life, home and correspondence (*Article 8, Human Rights Act*). Her employer claimed that it was authorised to do anything necessary or expedient for the purposes of providing higher and further education. The employee was subjected to 18 months of monitoring which covered her telephone, e-mail and internet use. Crucially, the employer had no technology use policy in force negating the employee’s expectation of privacy when using her employer’s e-mail, telephone and internet systems.

The ECHR found that as the employee had not been warned that her telephone calls would be monitored, she had a reasonable expectation of privacy in respect of not only calls made from her work telephone but also her e-mail and internet usage while at work. By monitoring the employee’s communications, the employer had breached Article 8 and was ordered to pay damages of GBP3,000 (about US$5,931) and costs of GBP6,000 (about US$11,862).

This case emphasises the need for employers who monitor employees to ensure that those employees are aware that:

- Their communications could be monitored.
- There is a good reason for such monitoring in every case.

Employees could argue that monitoring breaches:

- Article 8 of the Human Rights Act.
- The employer’s duty of trust and confidence, entitling them to resign and claim constructive dismissal.

US

US law generally allows monitoring of employees provided they have no reasonable expectation of

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1
privacy. Generally, this applies if companies have given employees clear notice that they will monitor public areas and technology resources.

Under federal law, an employer's monitoring of e-mails is governed primarily by the Electronic Communications Privacy Act of 1986 (*18 USC §§ 2510 et seq*) (ECPA). What an employer can monitor depends on whether the employees' messages are intercepted during transmission or are retrieved from storage on the employer's server.

The monitoring of messages as they are transmitted is subject to the ECPA's most stringent restrictions and is permitted only in limited circumstances. For employers' purposes, the exceptions most likely to apply are that:

- Prior consent is given by at least one party to the communication.
- Interception is necessary to provide the service or to protect the rights or property of the service provider.

Under the ECPA, employers can read employee communications stored on their servers regardless of whether either of these exceptions apply. The employer is therefore relatively free to monitor stored e-mails as long as any reasonable expectation of privacy has been removed (*Fraser v Nationwide Mutual Insurance Company, 352 F.3d 107 (3rd Cir 2003)*).

Similarly, if an employer notifies employees (for example, in its technology use policy) that it reserves the right to, and will in fact, monitor employees' internet use, there are few legal impediments to that monitoring. However, some states require notification prior to an employer monitoring employees' use of the company e-mail system. For instance:

- Connecticut employment law directly addresses electronic monitoring by requiring that employers engaged in electronic monitoring give employees prior notice of such monitoring (*Conn. Gen. Stat. § 31-48d (2006)*). Before engaging in electronic monitoring, an employer must conspicuously post a notice of the types of electronic monitoring in which it may engage, which may satisfy the prior written notice requirement.
- Delaware employment law explicitly requires employers to give notice before engaging in the monitoring of telephone transmissions, e-mail and internet usage (*Del. Code Ann. tit. 19, § 705 (2006)*). To satisfy the notice requirement, an employer can either:
    - provide electronic notice of monitoring once each day that an employee accesses employer-provided e-mail or internet access services;
    - give the employee a one-time notice in writing in an electronic record or other electronic form that has been acknowledged by the employee electronically or in writing.

Asia-Pacific

The law on employee monitoring varies significantly between different Asia-Pacific jurisdictions. Several have adopted a model similar to the US, where giving notice to the employee is a necessary and sufficient requirement for the employer to monitor. Others, such as Hong Kong and Japan, have adopted far-reaching guidelines supplementing the legislative framework and imposing strict requirements on data collected from employees.

Australia
Employee monitoring in Australia is regulated at both federal and state level.

Federal level. Although it is not always clear, employee monitoring is permitted by the "employee records exemption", which was introduced to the federal Privacy Act 1988 when it became applicable to the private sector. The exemption applies to data collection practices that relate directly to a current or former employment relationship and employment records (*section 7B(3), Privacy Act*). Monitoring techniques that are not proportionate to the risk addressed cannot be "directly related" to the employment relationship and are not covered by the exemption.

However, the exact scope of the exemption is unclear. For example, in a recent case in an organisation involving the disclosure by a manager of personal information about an employee's HIV/AIDS status to co-workers, the Privacy Commissioner decided that although the employer's (and the co-workers') interest was unlikely to outweigh the infringement of privacy suffered by the person in question, the disclosure was found to fall within the exemption.

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

In April 2004, the Privacy Commissioner advocated the repeal of the employee records exemption, mainly on the grounds that it would ensure (*see www.privacy.gov.au/publications/empsub.pdf*):

- Consistency across all states and territories.
- That privacy issues are not left to employment agreements, which reflect unequal bargaining positions.
- That private-sector employees enjoy substantially the same rights to privacy protection as their public-sector counterparts.

Nothing further has come of this proposal for reform to date.

Although intended for public-sector use, in response to demand for guidance on privacy best practice, the Privacy Commissioner has recommended that private-sector businesses use the Guidelines on Workplace E-mail, Web Browsing and Privacy (March 2000) (*see www.privacy.gov.au/internet/email/index_print.html*).

State level. Two relevant acts on workplace monitoring and surveillance have recently been adopted at state level:

- The Workplace Surveillance Act 2005 (NSW) in New South Wales. This is available at *www.legislation.nsw.gov.au.*
- The Surveillance Devices (Workplace Privacy) Act 2006 (VIC) in Victoria. This is available at *www.dms.dpc.vic.gov.au.*

The main features of the New South Wales legislation are:

- Employers can monitor employees in two circumstances. These are either:
    - overtly, provided a 14-day (written or e-mailed) notice has been given to them before conducting the monitoring activities (or, in the case of a new employee, before starting work);
    - covertly, if approved by a court.
- Employers can prevent delivery of e-mails received or sent by employees provided that:
    - an e-mail or internet monitoring policy has been notified in advance to employees;
    - employees are fully aware of such policy (for example, by obtaining written acknowledgement from each employee or by introducing training courses).
- Employers cannot monitor employees when “not at work” except for those cases where the employee uses equipment or resources provided by or at the employer’s expense.
- Employers should implement measures to protect those records collected by means of non-covert monitoring activities and to avoid their unauthorised use or disclosure.

The most relevant features of the Victorian legislation are:

- Employers cannot use surveillance systems (such as listening devices or video cameras) in workplace toilets, washrooms, change rooms or nursing rooms.
- Employers must seek employees’ consent for optical surveillance of “non-private” activities and for tracking surveillance.
- Employers cannot communicate or publish material obtained through surveillance.

Employers in Victoria can disregard these prohibitions in one of the following cases:

- They have been granted a warrant or emergency authorisation.
- It is required by a federal law.
- It is required as a condition of a liquor licence.

Breaches of these prohibitions can lead to fines of up to AUS$132,144 (about US$109,045) or imprisonment of up to two years.

Hong Kong

The Personal Data (Privacy) Ordinance 1997 (Ordinance) applies to employee monitoring and allows the Privacy Commission for Personal Data to adopt guidelines (*see www.pco.org.hk/english/ordinance/ordfull.html*). In December 2004, the Privacy Commissioner adopted guidelines on employee monitoring of e-mail, internet and telephone use

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1
(*www.pco.org.hk/english/publications/files/monguide_e.pdf*). As these guidelines set out the Commissioner's opinion on the application and enforcement of the Ordinance, they should be treated as binding.

Broadly speaking, the guidelines require the employer's legitimate business interests to be balanced against employees' personal data privacy rights. To do this, an employer should:

- Assess the risks that employee monitoring seeks to manage and the intrusiveness of the proposed monitoring techniques.
- Consider alternatives to employee monitoring that may be equally effective and practical in their application, yet less intrusive.

This is similar to the UK's impact assessment (*see above, UK*).

The risk threshold is low. For example, the employer can monitor the time its employees spend web-browsing, to prevent its resources from being substantially used for private purposes that may adversely impact on productivity. In addition, the contents of e-mails sent using the employer's communications equipment can be monitored to ensure the integrity and security of confidential business information.

Once a monitoring purpose is established, employers should assess the likely adverse impact that it may have on employees' privacy. For example, when monitoring e-mails, the concern is whether the message is work-related or purely private. Monitoring e-mails that are clearly unrelated to work will likely be characterized as intrusive. As a result, the identified risk must be proportionately great (for example, there must be a reasonable suspicion of seriously improper conduct).

Employers should adopt a transparent approach to formulating and disseminating employee monitoring policies and practices. An effective way of achieving this is to implement a comprehensive written privacy policy, which should explicitly address the:

- Business purpose(s) that employee monitoring seeks to meet.
- Circumstances in which monitoring can take place.
- Manner in which monitoring can be conducted.
- Kinds of personal data that can be collected from monitoring.
- Purpose(s) for which the personal data collected can be used.

As a general rule, employee monitoring should be conducted openly on the basis of a clear and easily accessible employee monitoring policy or technology use policy. Where there is no policy, covert monitoring can only take place if special circumstances justify its highly intrusive nature. There is a twofold test for this:

- There must be reasonable suspicion that an unlawful activity is about to be, or has been, committed.
- Convert monitoring is absolutely necessary in the circumstances to detect, or collect evidence of, that unlawful activity (that is, overt monitoring would likely prejudice the detection or the successful gathering of evidence).

Covert monitoring must be limited in scope (to target only those areas in which an unlawful activity is likely to take place) and duration.

If these requirements are not met an employer can be exposed to:

- Civil compensation claims by employees.
- Enforcement notices. Non-compliance with an enforcement notice carries a penalty of between HK$25,001 (about US$3,200) and HK$50,000 (about US$6,405) and two years' imprisonment.

In a recent complaint concerning the installation of pinhole cameras at different working locations of a government department, the Privacy Commissioner found that the dimension and extensiveness of the monitoring were disproportionate, employees had not been previously informed and other less intrusive means had not been investigated. The Commissioner ordered the immediate termination of the monitoring, the destruction of all relevant recordings, and the implementation of a more

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1
transparent privacy policy (*www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=248&casetype=O&cid=23*).

Japan
The Japanese government has also published guidelines (*www.meti.go.jp/policy/it_policy/privacy/0708english.pdf*) which supplement the Law on the Protection of Personal Information 2005. They provide that an employer should:

- Specify the purposes of monitoring and incorporate them in its employee privacy policy.
- Designate the person responsible for monitoring, and the authority of that person.
- Perform audits and confirm that monitoring is being conducted appropriately.

Privacy rights are infringed if the purpose, method and manner of monitoring, when balanced against the harm incurred by the person being monitored, exceeds the range that social convention would deem to be appropriate (*Tokyo District Court (wa) 12081 of 2000*).

Therefore, monitoring should be balanced against the employee's expectation of privacy. Where the private use of e-mail is prohibited by company rules and those rules are actually implemented, employees' expectation of privacy is low. In this case, monitoring without giving notice is usually acceptable, provided there is a rational reason to monitor and a person is clearly specified as responsible for monitoring.

However, where an employer approves or even implicitly acquiesces to the private use of e-mails, employees' expectations of privacy are higher. In this instance, unless there is a particularly important need for monitoring which overcomes that higher expectation, there is a risk that it would invade privacy rights.

New Zealand
As in the US, notification is a necessary and sufficient requirement for monitoring (*Privacy Act 1993*). If employees have been notified and the expectation of privacy has been removed, an employer can monitor them.

The covert collection of information is allowed in circumstances that involve potentially unlawful behaviour, as it is recognized that advising an employee of e-mail monitoring in relation to an investigation would probably affect the employee's future behaviour, prejudicing the purpose of the monitoring.

In a recent case, the employment court ruled that an employer had to consult affected employees and their union before implementing a biometric time-keeping system (*OCS Limited v Service and Food Workers Union Nga Ringa Tota Incorporated (Wellington, WC, 15/06, 31/8/06)*). However, in another case, the court recognised the legality of finger-scanning systems where the employment agreement provided an acceptable legal ground for the use of biometrics (*PMP Print Limited v Barnes (ERA, Auckland, AA 317-04, AEA 499-04, 28 September 2004, D King)*).

South Korea
Notice of monitoring alone, even if the employer has a legitimate reason to monitor, is insufficient. Employees must also give their express consent (*Communications Secrecy Protection Act of 1993, Act on the Promotion of Information, Communications Network Utilization and Information Protection of 2001 and Articles 17 and 18, Constitution 1948*). Monitoring e-mails without employee consent will most likely infringe the law.

Employers should:

- Clearly inform their employees of the scope of monitoring and how it is carried out.
- Advise employees to store their personal e-mails separately.
- Obtain consent before monitoring.

Failure to do this can result in criminal penalties including imprisonment and/or fines.

Taiwan
Although there is a constitutional right to privacy (*Article 12, Constitution 1946*) and detailed data privacy legislation, the clearest statement of employee privacy law is found in district court case law

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1
from 2003 adopting the reasonable expectation test. Under this test, an employer can only monitor employees' emails if they do not have a reasonable expectation of the privacy of their work e-mails (for example, where employees have been provided with a clear e-mail monitoring policy).

The Impact of Employee Monitoring

Monitoring employees is now standard practice, but the reasons for monitoring can vary greatly. Some employers monitor to protect employees who work in hazardous environments, to ensure that safe working practices are being followed. Others may be under legal or regulatory obligations to monitor, for example, in the financial services sector. Most employers, however, primarily monitor to check on their employees' performance, either to detect misconduct or to ensure compliance with specific company policies and procedures. The monitoring of employees' electronic communications is no different from any other form of monitoring. However, because of the technological ease with which such monitoring can be undertaken, it is easy to overlook the consequences it can have.

While the advantages to the employer of monitoring may be obvious, the adverse impact on employees may be less apparent. If employees are permitted to use telephones, email and the internet for personal use, it may be difficult for an employer to draw a distinction between work-related and private information and activity, and limit monitoring to the former. Although employees may expect and accept the monitoring of their work, the monitoring of their private information and activity is likely to be much less welcome.

An employer's failure to consider the adverse impact of monitoring on employees can interfere with, or ultimately destroy, working relationships. It can also breach legal requirements, and may even amount to a criminal offence. For example, in 2005 the former CEO and five other executives of a Finnish company were given fines or up to ten months' suspended sentences for illegally keeping logs on e-mails and telephone numbers dialled by employees, in an effort to identify who had leaked information about management disputes to mass media.

Even where employers can justify monitoring employees' electronic communications, it is still advisable for them to strike a balance between the legitimate need to run their businesses in the best way they see fit and respect for their employees' private information and activities. Such monitoring also places a burden on the employer, because, having obtained information through monitoring, the company must handle the information appropriately. The statutory requirements regarding the storage, access, use, retention and deletion of the information obtained through the monitoring of employees' electronic communications can be onerous and may even put some employers off undertaking such monitoring.

Ensuring Compliance: Some Tips

There are a number of general steps that employers can take to ensure compliance across their operations:

- **Notify employees of any anticipated intention to monitor**. This can be done by implementing and disseminating a technology use policy. This overcomes any employee expectation of privacy in using the employer's e-mail or accessing the internet while at work. If a half-way approach is taken (for example, by allowing employees limited personal use of IT equipment), set this out clearly.
- **State the reasons for the monitoring**. Include in any e-mail or internet use policy a statement of the reasons for monitoring (for example, to ensure compliance with company policies or the proper functioning of the computer systems, or to monitor performance).
- **Ensure that monitoring is proportional**. Be clear about the reasons for monitoring. In principle, monitoring should be limited to the extent necessary to achieve a certain legitimate aim. If it can be carried out on a less intrusive basis (for example, monitoring only the number of e-mails sent or amount of time spent on the internet) then this should be used. Ensure that local laws can be complied with once the personal data has been collected (*see below*).

Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=4731412c-ca8e-4daa-8530-149caf8e90a1

- **Comply with local laws**. Provisions vary dramatically between jurisdictions. Do not ignore local laws and adopt, for example, a US approach across jurisdictions.
- **Ensure there is a legal basis for the monitoring**. As well as complying with any notice requirements, remember that many jurisdictions require a legal basis for monitoring. Verify whether there are any applicable exceptions for employee monitoring.
- **Conduct training**. Once a policy is implemented, conduct training sessions to raise employees' awareness of monitoring and its purposes.
- **Undertake regular audits**. Conduct audits at least annually to ensure that policies are current, applicable and being followed.

© 1996-2007 Morrison & Foerster LLP. All rights reserved.