



Privacy and Social Networking in the Workplace

International Labor Group

Moderator:

Aaron J. Schindel, New York

Presenters:

Daniel Ornstein, London

Cécile Martin, Paris



How can an employer legally monitor employees' emails and internet access?

To legally implement a monitoring system, the employer must:

- Inform and consult the Works Council;
- Inform the employees on an individual basis; and
- Notify the French Data Protection Agency (CNIL).

Two types of monitoring systems:

- Individual monitoring system: Provides detailed information on internet sites visited by each workstation (can be used to ascertain sites visited and time spent on the internet by an employee). Such a system is quite burdensome for the employer, which must provide the Agency with a lot of information.
- Global monitoring system: Does not permit the employer to control the employees' activity on an individual basis (can be used for gathering statistics about internet usage). Notification to the Agency requires only a simple confirmation of compliance with the Agency's decision of 2005.



How can an employer legally monitor employees' emails and internet access?

Emails

- **The employees have a right to privacy** even in the workplace and even during working time. Employers' access to emails sent or received by their employees is restricted.
- **Before opening or reading** an employee's email, the employer needs to ensure that the employee has not identified it as "personal" (in the email subject line notably).
- **Sanctions:** fine (€45.000) + imprisonment (up to one year).
- However, the employee may not transform professional data into private data (**good faith** duty).
- To avoid uncertainty, the employer who wants to access an employee's emails designated as "personal" can seek judicial approval.



How can an employer legally monitor employees' emails and internet access?

Internet

- Internet connections made from an employee's work station during working hours are deemed to be work-related.
- **No infringement** of employee's privacy if the employer checks the employee's record of internet connections, without the employee being present.
- French Supreme Court 2008: The termination of an employee was permissible when the employer noticed, while the employee was on sick leave, that he had been accessing pornographic websites while at work.



How can an employer legally monitor employees' emails and internet access?

- The UK Legal Framework
 - Right to Privacy – Human Rights Act
 - Data Protection
 - Regulation on Investigatory Powers Act (“**RIPA**”)
 - The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations (the “**Telecommunications Regulations**”)



Right to Privacy

- Article 8: “*everyone has a right to respect for his private and family life, his home and his correspondence*”
- Extends to workplace
- Not absolute – a balancing act:
 - the employer’s own legitimate interests
 - conflicting legitimate interests of other employees (e.g., right not to be harassed)
 - no more than necessary to accomplish the objective identified
- *McGowan v Scottish Water; cf. Mills v Mid Sussex District Council*



Data Protection

- Part III of the Employment Practices Code – “Monitoring at Work”
- Non-statutory guidance
- The importance of “Impact Assessment”



The Impact Assessment – a substitute for employee consent

- Identifying clearly the **purpose(s)** behind the monitoring arrangement and the benefits it is likely to deliver;
- Identifying any likely **adverse impact** of the monitoring arrangement;
- Considering **alternatives** to monitoring or different ways in which it might be carried out;
- Taking into account the **obligations** that arise from monitoring;
- Judging whether monitoring is **justified**.



RIPA and the Telecommunication's Regulations

- RIPA regulates the “*interception of a communication in the course of transmission*”
 - Listening in on telephone conversation
 - Opening **unopened** emails
 - Criminal liability
- The Telecommunications Regulations permit interception for business use, without consent, for limited purposes, including, most importantly:
 - Compliance with practices and procedures relevant to the business (*e.g.*, misconduct, harassment, fraud, breach of confidentiality)



Is it legitimate to restrict an employee's Internet access and how should this be carried out?

- Access to Internet for **personal purposes** during working time is generally admitted as long as it is reasonable.
- Any **restriction** must be proportionate to the goal pursued → general prohibition of personal use is not possible.
- Permissible to **restrain** the type of use or prohibit access to specific websites (by name “*Facebook*” or content “*pornography*”).
- Permissible to **prohibit** certain employees' actions with regard to network security (e.g., downloading software, connecting to forums).
- **Before implementation** of restrictions, the employees must be **informed**, and the Works Council must be **consulted**.
- Restrictions are usually contained in **codes of conduct** and may lead to disciplinary measures (e.g., dismissal of an employee who spent 41 hours in one month on the Internet).



Is it legitimate to restrict an employee's Internet access and how should this be carried out?

- Lawful to restrict access – discretion of employer
- Blocking certain sites permissible
- However, where there is not automatic blocking and employees can access sites:
 - Have a clear policy based on an impact assessment – regularly audit
 - Ensure employees aware of policy with regular reminders (pop-ups when internet is accessed)
 - Be wary of distinctions between policy and practice



To what extent is an employer liable for things done by employees on the Internet?

- **Civil liability** → employer is liable for the wrongful acts of his employees while they are under his control (*i.e.*, misuse of Internet during working time).
- Court of Appeal 2006: Employer was liable for the actions of an employee who had created a website during his work time that infringed the rights of another existing website. Since the code of conduct allowed the employees to consult websites unrelated to professional activity, the employer had provided the employee with the means to commit the offense.
- **Criminal liability** in case the employer is considered as a co-perpetrator or accomplice.
- **Exemption** from liability if it is proven that the employee acted outside the scope of his mission and without any authorization.



To what extent is an employer liable for things done by employees on the Internet?

- Generally, an employer is liable for all things done by an employee *“in the course of employment”*
 - No vicarious liability for activities not expected of employee and outside the scope of normal duties; e.g., defamation, breach of confidence, breach of copyright
- BUT, the test in discrimination/harassment cases is wider – onus on employer to show *“that it took such steps as were reasonably practicable to prevent the employee from doing the discriminatory act”* – even where the acts were outside the normal scope of the employee’s duties

Can an employer restrict/prevent an employee from using social networking sites either in the course of or even outside of employment?



- Employees have a **Right to privacy** and **Freedom of speech**.
- Employers may **restrict**, in employment contracts / staff handbooks, the use of social networks for legitimate grounds (e.g., confidential information or trade secrets).
- **Abuse** of freedom of speech could be considered as a fault (e.g., when blogs contain insulting or excessive words tending to disrupt or destabilize the company's functioning).
- Court of Appeal 2006: The court ordered a former employee to delete from her blog the slanderous and defamatory words she had posted and pay damages to her former employer.
- **Blogs can also be an issue for employees:** In January 2010, several French headhunter agencies adopted a code of conduct in which they agreed to select candidates based on their professional skills only and not on their private life.

Can an employer restrict/prevent an employee from using social networking sites either in the course of or even outside of employment?



- Yes, within course of employment
- Employer can issue policies about the use of social networking sites outside the course of employment, and sanction employees for breaches of the policy
- Advisable to act as defence to vicarious liability
- Employer free to consider the content of public social networking sites when recruiting and in the course of employment – but cannot demand access to private sites



Can provisions in staff handbooks/codes of conduct enable employers to safeguard their rights in relation to misuse of new technologies?



- Employers should implement codes of conduct informing employees of **terms and conditions** of internet and email use (rights, obligations, responsibilities).
- French Supreme Court 2006: A code of conduct can be **binding and enforceable** against employees provided that information and consultation requirements have been fulfilled (Works Council, employees, labor authorities).
- **Failure** of the employee to comply with the code may preclude the employer's civil liability in case of wrongful use of new technologies.
- Generally, existing codes only provide for **general guidelines** regarding use of emails and Internet and do not address social networking.

Can provisions in staff handbooks/codes of conduct enable employers to safeguard their rights in relation to misuse of new technologies?



- New media: increased opportunities for stupidity and damage
- Policies can be introduced to handbooks without consent
- Areas for policies:
 - References on social networks
 - Breaches of confidentiality
 - Harassment/Discrimination
 - Defamation
 - Bringing company into disrepute



Privacy and Social Networking in the Workplace

International Labor Group

Moderator:

Aaron J. Schindel, New York

Presenters:

Daniel Ornstein, London

Cécile Martin, Paris