MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Comparing the U.S. and EU Approach to Employee Privacy

February 2008
by Ann Bevitt, Miriam Wugmeister

Related Practices:

- Employment and Labor
- Privacy and Data Security

PDF Version

The U.S. approach to employee privacy stands in sharp contrast to that of the European Union The EU Member States adopted an omnibus data protection directive (the 'Directive') regulating the collection and use of personal data across all sectors of the economy. The U.S. federal and state privacy laws, on the other hand, address specific instances of abuse or perceived market failures, or protect particularly sensitive information, such as health or financial information, and groups in need of special protection, such as children.

This fundamental difference in approach to privacy between the U.S. and the EU is reflected in the contrasting levels of regulation of two basic aspects of the employment relationship: the conducting of background checks prior to employment and the monitoring of employees in the workplace. Whereas employers conducting background checks in the U.S. are subject to some regulation, employers in the EU are more restricted, both in terms of what can and cannot be covered and also how the information obtained can be used. Similarly, employees in the U.S. have a diminished expectation of privacy at the workplace and lawful monitoring of employees' electronic communications over employer-provided facilities is seen as a legitimate function of responsible management. Failure to investigate these activities may even, in some cases, expose the employer to liability to injured third parties. In contrast, in the EU, employees' expectation of privacy at the workplace is generally high, and employees are viewed as being in need of protection from their employer's interference with their privacy.

U.S. – Employee Background Checks

The Fair Credit Reporting Act ("FCRA") is the primary federal law governing the use of background checks. One of the main aims of the FCRA is to protect consumers by seeking to ensure that consumer reporting agencies provide fair and accurate information about the 'credit worthiness, credit standing, credit capacity, character, and general reputation of consumers,' as well as to protect a 'consumer's right to privacy.'

The FCRA mainly regulates consumer credit reporting agencies, but also imposes obligations on employers that seek to obtain consumer reports from such agencies relating to security credit, insurance or other benefits, as well as employment. However, if an employer performs its own background checks in-house, the FCRA does not generally apply, although employers must still comply with certain other federal and state laws, which may impose more stringent notice requirements.

As a general principle, the FCRA applies to any background check report prepared by an agency for employment-related purposes. Under the FCRA, employers that procure a background check report for employment purposes must give applicants "clear and conspicuous" written notice of this and obtain the applicant's written consent before requesting such a report from the agency. This notice must be a stand alone document, rather than part of another document. An agency may provide a

background check for employment purposes only if the employer has certified that the employer:

1. has provided the required notice to the applicant;
2. has obtained the applicant's authorisation to procure the report;
3. will comply with the FCRA's requirements prior to taking adverse action based in whole or in part on the report; and
4. will not use the information from the report in violation of any equal employment opportunity law or regulation.

EU – Background Checks

Employers who use background checks in the EU to assess and verify the qualifications of applicants must comply with the local laws applicable in the Member State(s) where they operate. As well as national Data Protection Acts ("DP Acts"), based on the Directive, many Member States have enacted regulations on background checks, in particular with respect to the collection of criminal records. Local labour and employment laws impose additional obligations or restraints. Accordingly, local differences may necessitate modifications to the background check process from one Member State to another.

France – Background Checks

Under French law, employers may only seek personal data from job applicants to the extent there is a direct and necessary connection between the background check and the contemplated employment relationship. French employers have to file a registration with, and obtain prior approval from, the French DP Act (the "CNIL") to collect the data sought on any background check forms used.

Background checks into financial transactions or credit payment histories are generally not permissible, irrespective of any consent obtained from the applicant. Only in situations where an employer recruits for a specific job that necessitates the collection of this particular type of information, and with the applicant's prior consent, may credit information be sought and then only to a limited degree.

Background checks for the purpose of verifying the applicant's civil court records, criminal conviction records, legal proceedings or judgments are only permitted for certain positions and roles in sectors such as banking, auditing or defense. Typically, applicants are asked to apply for and produce a "certificate of good standing" giving details of any conviction recorded in central records or stating that there is no such conviction.

France – Notice Requirements

Prior to the collection of data by means of a background check, an applicant will need to be fully informed regarding the data collection. Any forms the employer uses in the context of a background check need to provide the applicant with information on:

- the purposes for which the data are used;
- the likely recipients of the data;
- whether the data will be transferred to the U.S. (which is not considered as providing adequate protection for personal data);
- whether answering questions is mandatory;
- whether there could be consequences if the applicant does not provide the information; and
- the applicant's right to access and correct the data once collected.

Access and Correction

Every applicant must be able to access his/her personal data that have been collected in the recruitment process. The applicant must receive adequate information about how he or she can exercise his/her access right in order to be able to obtain any information upon request, including any recruitment test which the applicant took. This access right applies to information given by the applicant or third parties. The CNIL recommends providing this information in writing.

U.S. - Employee Monitoring

The Electronic Communications Privacy Act of 1986 ("ECPA") prohibits the interception of wire, oral, and electronic communication, including e-mails. Under ECPA, employers providing an e-mail account to an employee may intercept employee e-mails with the consent of one party to the communication, as part of the provision of the service or, to a lesser extent, for the protection of the rights or property of the service provider.

ECPA distinguishes between messages in storage, and messages in the process of transmission. Interceptions of messages in storage are subject to Title II of the ECPA, also known as the Stored Communications Act ("SCA"), which protects the privacy of communications while those communications are in electronic storage. The SCA makes it generally unlawful for anyone to access, intentionally and without authorisation, a facility through which an electronic communications service is provided (or intentionally to exceed an authorisation to access that facility). Furthermore the SCA makes it unlawful to obtain, alter, or prevent authorised access to a wire or electronic communication while it is in electronic storage. However, and importantly for employees, the SCA has a strong "service provider" exception, according to which anyone may access stored communications, and thereby obtain, alter, or prevent authorised access to those communications, if such conduct is authorised by the service provider. In the case of a communications service, such as an employee e-mail account, employers can persuasively argue that they are service providers and, therefore, are entitled to retrieve and review the employee's communications for any purpose. The courts generally have agreed with this interpretation of the SCA.

While U.S. employers generally may review stored e-mails, they should still specifically reserve the right to monitor employees' e-mail communications and should also reserve the right to monitor Internet use through a policy or other notice to employees. Disputes over Internet and computer use monitoring have arisen in a variety of contexts, and usually have required courts to inquire into the employee's expectation of privacy in his or her use of the employer's network. For example, one court was asked to determine whether an employee was wrongfully discharged, in violation of his right of privacy, when his employer read employee e-mails after declaring that those communications would not be intercepted or used as the basis for termination or reprimand. Regardless of the employer's privacy assurances, the court found that no privacy right had been violated.

EU – Employee Monitoring

When monitoring employees in the Member States, employers have to grapple with DP Acts, telecommunications regulations, labour laws, constitutional provisions, criminal laws and collective bargaining agreements. The Article 29 Working Party, which is a representative group of the EU Member State Data Protection Authorities ("DPAs"), adopted a working paper on the surveillance of electronic communications in the workplace (WP55). According to this document emphasis should be on the prevention of the misuse of company resources with means other than monitoring. Monitoring should generally be avoided unless there is a specific and important business need. Although the Working Party guidance is non-binding, the DPAs take note of it when applying the applicable national laws. In 2002, the Working Party issued further guidance condemning covert monitoring (WP118). Once an employer decides to monitor employees, the Working Party suggests that it follow these seven basic principles to ensure that the monitoring is done properly and in accordance with employees' right to privacy:

- *Necessity*. Prior to monitoring, an employer must assess whether the monitoring in all its forms is absolutely necessary for the specified purpose;
- *Finality*. Data collected through the monitoring activity must respond to a "specified, explicit and legitimate" purpose (for example, the security of the system) and cannot be processed for a different purpose;
- *Transparency*. Monitoring should be transparent. The employer must provide clear and comprehensive notice to employees about the monitoring;
- *Legitimacy*. Employers may monitor employees only to safeguard their legitimate interests, while not violating the employees' fundamental rights;
- *Proportionality*. Personal data processed in connection with any monitoring must be adequate, relevant, and not excessive with regard to the purpose for which they are processed;
- *Accuracy and retention of data*. Personal data must be updated and retained only for the period deemed necessary for the purpose to be achieved, which generally is no longer than three months; and
- *Security*. The employer must implement all appropriate technical and organisational measures to ensure that any personal data are protected from alteration, unauthorised access, and misuse.

France-Employee Monitoring

France has yet to enact specific legislation on employee monitoring, so general labour, civil, and criminal provisions, as well as the French DP Act, apply.

In October 2005, the CNIL adopted guidance to help employers solve some practical issues related to the detection of employees' activities at the workplace. Any employee monitoring in France must take into due consideration the transparency and proportionality of the monitoring and must be performed in compliance with collective bargaining agreements. Moreover, consultation with the Works Council is an indispensable condition for employee monitoring. According to Article L. 432-2-1 of the Labour Code, *"the Works Committee must be informed and consulted prior to any significant introduction of new technologies, when the technologies are likely to affect … the employees' working conditions—especially when the decisions concern means and technology allowing the control of the employees' activities."* To safeguard appropriately its legitimacy, monitoring should be mentioned in technology use policies, or internal rules (règlement d'ordre intérieur). The establishment of these rules is subject to consultation with Works Councils and employees.

In accordance with the DP Act, employers must also register their monitoring of employee Internet use with the CNIL. There is an exception to the obligation to register where the employer appoints a "correspondant informatique et libertés," an internal data protection officer ("DPO"). However, transfers of data outside the EU and, thus, any monitoring involving transfers to the U.S., are subject to authorisation and must always be registered with the CNIL, irrespective of the appointment of a DPO. Additionally, the stored data generally cannot be retained for more than six months.

In the leading Cour de Cassation (the French Supreme Court) case, *Nikon,* the Court stated that "*the employee has the right, even during working hours and at his workplace to the respect of his privacy; this includes in particular the confidentiality of his correspondence; the employer cannot, without infringing this fundamental liberty, examine the personal messages sent or received by the employee on a computer tool placed at his disposal for work, and this even in the case of the employer having prohibited a non-professional use of the computer."*

In summary, employee e-mail monitoring is generally lawful in France if it fulfils the following conditions:

- *Reasonableness.* Monitoring must be "reasonable," meaning that the employee's fundamental rights and freedoms must be balanced against the need to protect the employer's interests;
- *Personal Communications.* Particular caution should be exercised with respect to an e-mail that is marked "private" or "personal";
- *Legal Basis.* There must be a legal basis;
- *Notice*. The employer must inform the employee about the fact that it stores communications on its servers, retention periods, etc., and the conditions under which the employee may access the stored content;
- *Consultation with the Works Council*. Employers must consult with the Works Council prior to monitoring;
- *Registration with the CNIL*. If the employer monitors communications on a global basis (without identifying individual users), no specific notification of the monitoring is required. However, if the monitoring identifies users, it has to be registered with the CNIL;

Unlawful monitoring may subject employers to civil and criminal sanctions. In particular, unlawful interception of employee communications may constitute "breach of the confidentiality of personal correspondence," and may result in imprisonment of up to one year and fines of €35,000 (approximately US$51,000). Also, if a court decides that the monitoring were indeed unlawful, the employer cannot base any action, such as dismissal, on evidence obtained unlawfully.

Conclusion

Despite the difference in approaches, both the EU and the U.S. recognise the need for employee privacy. However, the degree to which they recognise that need differs. In the U.S., collecting personal information about employees is generally seen as a legitimate activity, provided that it is carried out for non-discriminating, legitimate business purposes. Alternatively EU employers generally have to justify why they need to collect personal data from their employees. Certain data may not be collected at all, and some monitoring activities are prohibited as a matter of law.

There are a number of reasons why the EU approach differs from that of the U.S., many of them historical. For example, the extent to which employers may be held liable for their employees' activities is often statutorily limited in the EU, and, therefore, employee monitoring is not as necessary to reduce liability as it is in the U.S. Accordingly, for organisations operating under both legal regimens, a two-fold approach is warranted - companies operating in the EU must restrict their data collection and monitoring activities in accordance with the local laws of the Member States where they operate, while they may engage in more extensive data collection and monitoring in the U.S.