International Chamber of Commerce
The world business organization

Policy Statement

Employee privacy, data protection and human resources

Prepared by the Commission on E-Business, IT and Telecoms

I. Introduction

Businesses have always had to collect and use personal information from and about employees to comply with labour, tax and other laws, to administer benefits, to operate their businesses, and to serve their customers. This policy statement sets out the position of the International Chamber of Commerce (ICC) on the key issues relating to data protection and human resources, and provides recommendations for governments making policy in this area. While technological changes and new privacy laws have caused some re-examination of workplace privacy, the amount and scope of information about their employees that employers must process has changed very little over the years. ICC therefore urges governments to work closely with business to ensure that legislation and policy dealing with data protection in the human resources context strikes a workable balance between the legitimate interests of employers, customers, and society as a whole, and the privacy of employees.

Multinationals have to abide by the law and meet the expectations of their workers and of the marketplace in all countries in which they operate. They recognize that they must meet their data protection obligations toward employees and that those obligations do not disappear simply because the employees are networked together and their data is processed at a distant location. However, data protection obligations and individual employee rights should be balanced with the benefits of networking and enterprise-level information systems and other legal obligations and duties of employers to their customers, their shareholders, and society at large.

Regimes already established to protect personal data include, in their scope, employment-related data. Separate treatment for human resources data does not provide additional protection for individuals and can even reduce benefits to employees. The lack of clarity for both employers and employees of the many national policies and laws on workplace privacy is creating an unacceptable level of risk for business, particularly multinational business. It greatly increases companies' compliance burden without appreciably improving employees' privacy. ICC urges national governments and international organizations to recognize, as an alternative to formal legislation, solutions such as company codes of conduct/policies that protect employee data while allowing companies to utilize enterprise-level information systems designed to make business more efficient and benefit companies, employees and customers.

International Chamber of Commerce
38, Cours Albert 1er, 75008 – Paris, France
Telephone +33 1 49 53 28 28 Fax +33 1 49 53 28 59
Web site www.iccwbo.org E-mail icc@iccwbo.org

Governments, regulatory agencies and data protection authorities should coordinate closely with their international counterparts to prevent the emergence of a patchwork of different obligations. Governments should rely on industry to protect its human resource data effectively as protecting employees' personal data from misuse is vital to ensuring employee satisfaction. Governments should re-examine existing laws which have a bearing on employee privacy with a view to streamlining compliance burdens on employers and offering more flexible means for compliance. However, any government actions should first engage industry to determine the potential impact of any obligations.

ICC draws attention to the valuable work of the International Labour Organisation, which published its Code of Practice for the Protection of Workers' Personal Data in 1997.[1] This Code may be used as the starting point for further discussions between legislators, industry and employees.

II. Technological developments and new ways of working

Recent technological and business developments, such as the growth of the Internet (as well as private data networks and virtual private networks) and the deployment of enterprise resource management (ERM) information systems, allow for the development of new global business models offering the potential for organizations to offer more, and more efficient, products and services to their customers and employees. ERM information systems are designed to standardize the ways of working and decision-making throughout an enterprise. They permit the automated flow of information to all affected functions in the enterprise. Enterprise-wide communications and information systems typically entail central servers and host computers, as well as remote access by authorized persons located anywhere. The centralized nature of these systems permits the deployment of centralized and uniform controls that can facilitate compliance with corporate policies and review processes. Networking and enterprise-level information systems offer many benefits both to employees and businesses including increased efficiency and productivity, lower costs, and greater flexibility.

Enterprise-level information and communication systems can:

- Reduce the need for duplicating computer facilities in each office or plant location.
- Reduce the number of times a particular piece of data must be entered into a database and ensure greater accuracy and transparency.
- Reduce the number of software programs and database types that the company must support and that employees must learn, reducing costs and promoting efficiency.
- Increase the speed and efficiency of the processing of expenses and other employee claims and benefits.
- Speed up the delivery of data to managers and employees and give them direct access to the data they need.
- Allow centralized as well as local recruiting, and speed up the processing of applications, requests, and orders.

[1] http://www.ilo.org/public/english/protection/safework/cops/english/download/e000011.pdf

- Permit more uniform and better enforced information policies, procedures, training, controls, and security across a corporate group, facilitating compliance with, for example, data protection codes and information security policies.
- Allow knowledge, experience and opportunities to be shared widely and almost immediately within a corporate group on a global scale.

Working practices have also changed dramatically in the last twenty years. Many employees now carry out some of their duties outside the workplace, for example, at remote sites such as clients' premises, while travelling, or at home. These employees need to be able to access the appropriate information while working remotely. Also, the complex clustering of functional working groups within enterprises is not necessarily consistent with the formal legal structure of the enterprise or even the formal employment arrangements, making it necessary to route employee data to other parts of the enterprise. Further, the boundaries between employees' work and private lives are being re-drawn as employees are able to work from home or be available for work-related communications outside office hours. Finally, outsourcing of functions such as payroll, recruitment and selection means that employees' personal data may need to be transferred to third parties in the course of normal business activities.

Employees clearly benefit in this evolving environment, enjoying, for example:

- Enhanced job security and prospects by improving the overall profitability of the company.
- Access to ideas and information from throughout the company, and more opportunities for distance learning and corporate training programs.
- Closer integration of employees at a distance from headquarters or from the larger plants and offices into the resources, culture, and personnel of the organization overall, and greater awareness of opportunities within the organization.
- Opportunities to readily view human resources information about themselves and update their personal data and their benefits choices.
- Flexible working hours or telecommuting opportunities, which allow employees to respond to child or family care situations.
- Greater choice and flexibility regarding benefits options, for example, with benefits plans that can be configured by the employee and automatically communicated to third-party benefits providers, rather than relying on the intervention of HR personnel.

The ability of business to make data transfers, particularly to third countries, is an essential part of global trade. As a result of varying national restrictions on transborder data flows, some companies have delayed implementing global enterprise information systems in, or including data from, countries that limit data flows of human resources data. Companies may also be required to restrict the access of employees in some countries to the full benefits of corporate Intranets. The outstanding issues surrounding crossborder transfers of personal data, including, but not limited to, employee data, need to be resolved as soon as possible so that companies, employees and economies as a whole can maximize the potential that technology developments and new ways of working offer.

III. Specific issues in data protection and human resources

Developing codes of conduct

Governments should allow companies to develop unified and comprehensive systems for human resource data management without imposing excessive obligations. Government or regulatory agency policies, or guidance from data protection authorities, should ensure that these integrated means for handling employee data worldwide can exist without impairing business efficiency. Governments should provide clear and practical guidance for the application of corporate codes, without the need for cumbersome registration or notification procedures, and with a streamlined approval process. Country-by-country approval processes, such as those currently used in the European Union, are a barrier to business and need to be addressed urgently.

Workplace monitoring

There are several reasons for the monitoring of employees which may vary from one employer, and situation, to another, such as:

- To detect, investigate, and prevent crime, such as theft, fraud or illegal use of software or the intellectual property of the employer or a third party.
- To prevent the unauthorized or unlawful disclosure of confidential business information, for example, trade secrets.
- To comply with obligations to prevent discrimination or sexual harassment under applicable laws, and prevent or reduce company exposure to liability for the unlawful acts of employees, particularly in relation to racist or sexist communications in the workplace.
- To maintain productivity and ensure the quality of products and services, and avoid damage to the company's reputation and goodwill.
- To comply with laws and regulations, e.g., workplace safety, labour, tax and other requirements.
- To ensure the integrity of information systems and compliance with company security and data protection policies.

Workplace monitoring is becoming acceptable and commonplace in many countries, although care needs to be exercised that the practice is consistent with local cultural values and traditions. Proportionate monitoring of electronic communications can be an essential part of corporate measures to foster the "culture of security" called for by the OECD Guidelines for the Security of Information Systems and Networks[2].

ICC supports lawful and fair monitoring of employee activities and communications. Employers should provide employees with notice of their policies governing the use of electronic communications, including policies on inspection and monitoring of communications, and employees should be made aware of any policy changes. It may be appropriate to provide notice to employees, or other individuals using the company's communication infrastructure, about the general circumstances under which monitoring might take place. However, prior information to

[2] http://www.oecd.org/dataoecd/59/0/1946946.pdf

an employee about specific investigations of suspected criminal activity or alleged contravention of company policies, is clearly counterproductive and should never be required.

There is considerable uncertainty as to employers' obligations and employee rights regarding workplace monitoring within some jurisdictions, and enormous variation between jurisdictions. Ill-defined restrictions on monitoring leave employers uncertain about what is permissible. This lack of clarity creates an unacceptable level of risk and potential liability for employers, and does not assist employees in knowing what level and type of privacy in the workplace they may legitimately expect. Moreover, it fails to advance worldwide interests in safeguarding important network, information and physical infrastructures, or in protecting consumers (including vulnerable consumers like children or the elderly). In many cases it is not possible to clearly delineate an employee's professional and personal use of business equipment to distinguish what types of activities may be monitored without imposing unreasonable burdens on employers. ICC urges national governments and international organizations to work with business to clarify these issues and recognize solutions such as company codes of conduct/policies as an alternative to formal legislation. These principles should be applied to other types of monitoring and surveillance used by companies for valid business purposes, such as video surveillance, building access control systems or performance monitoring systems.

Recruitment and selection

Business should not be prevented from making appropriate, focused and reasonable use of pre-employment screening procedures for prospective employees, provided the prospective employees are made aware that this may happen. These searches can include fact-checking of personal details provided by an applicant and an investigation of the broad suitability of the applicant for the post being considered. Increasingly, companies are legally required to vet employees in the areas of health, childcare, teaching, finance, or privately provided security and law enforcement service provision.

Restrictions on pre-employment screening may undermine necessary security measures and prevent businesses protecting themselves from the potential of fraud, damage to reputation, or other harms to businesses, their employees or customers. These restrictions may also leave companies vulnerable to liability claims from third parties if incompletely vetted employees cause harm.

In some jurisdictions employers face potential liability if they fail to conduct thorough checks on employees who are able to access the sensitive information of customers, for example, financial information, or who deal with vulnerable citizens such as health care subjects. It is in the interest of society as a whole to make sure that employers are legally able to conduct a thorough and proper review of employees and prospective employees, in the exercise of due diligence, and, using network resources, to transfer the information to appropriate human resources personnel in the context of hiring and other decisions.

Use of business contact data

Business has a legitimate need to freely use business information that may contain limited personal information, for example, an individual's name, job title, and work contact details. This use of limited personal information for business purposes does not compromise the legitimate expectations of individuals with respect to harmful use of personal data, and is an essential part

of acceptable business practice. Governments should not include business information of this kind in the scope of privacy regimes created to protect other personal data.

Facilitating cross-border data transfers

Companies in all countries and sectors need to transfer personal data from countries that regulate the export of personal data. Companies are able to both maximize the benefits attained by centrally locating human resource data and protect this data by establishing an appropriate access plan based on their global management structure. Business, in general, closely controls the individuals that have access to sensitive internal human resource data. The level and type of access to data, rather than its physical location, should be the primary focus in determining the risks of misuse of personal data. ICC urges governments to take a non-discriminatory view of different approaches to privacy protection, for example, legislative or self-regulatory approaches, and to encourage free flows of information where personally identifiable data is protected effectively. Governments that nevertheless choose to restrict employee data flows should support the broadest set of mechanisms possible to facilitate legitimate data transfers, for example, the use by companies of informed consent, contracts, and codes of conduct/company policies.

Consent

Fair processing of employee data can often be based on the needs of the employment contract, compliance with the legal obligations of the employer, and/or the legitimate interests of the employer or a third party which override the privacy interests of the employee. However, in circumstances not covered by these grounds, for example, transborder data flows, the employer must be allowed to rely on the principle of informed, unambiguous consent. Companies routinely include disclosure and consent provisions in their documentation for new employees for a range of different reasons including benefits programmes, and network access and monitoring. Consumers routinely consent to contractual provisions that they have no opportunity to negotiate, and consent in this context is not considered invalid unless the terms are unduly burdensome or onerous. The same should hold true for employees.

Where employee consent is required or used, the legal requirements for lawful consent should not exceed the principle of informed, unambiguous consent, and should be in full agreement with national requirements regarding the expression of will in the employment context. Explicit consent, especially written consent, should be reserved for extraordinary circumstances only, where the interests of the employee are seriously at risk, such as the processing of sensitive data such as health data. Nonetheless, employees should not be permitted to prevent a company from efficiently administering health and other benefits as long as adequate safeguards to protect privacy are in place.

Sensitive data

Where it is necessary for essential business purposes, or to comply with an employer's obligations under the law, companies should be permitted to request and retain employees' sensitive data. The employer must clearly inform the employee of the purpose for which the data are processed and should obtain the employee's consent if required under local law. However, employees should not be allowed to prevent the collection of vital information that may prove essential to employers in meeting their legal obligations to their customers, to the public, and to fellow employees.

IV. Conclusion

Effectively protecting employees' personal data from misuse is vital to ensuring employee satisfaction. At the same time, the Internet and new resource management technologies have created many advantages to business and their employees in terms of cost savings, increased efficiency and productivity, enhanced benefit packages, security and convenience. Flexibility and the ability to accommodate differences in interpreting privacy in the workplace are needed to facilitate access to information, communications, and commerce on a global scale.

Document N° 373-22/112
4 December 2003 MF/dfc