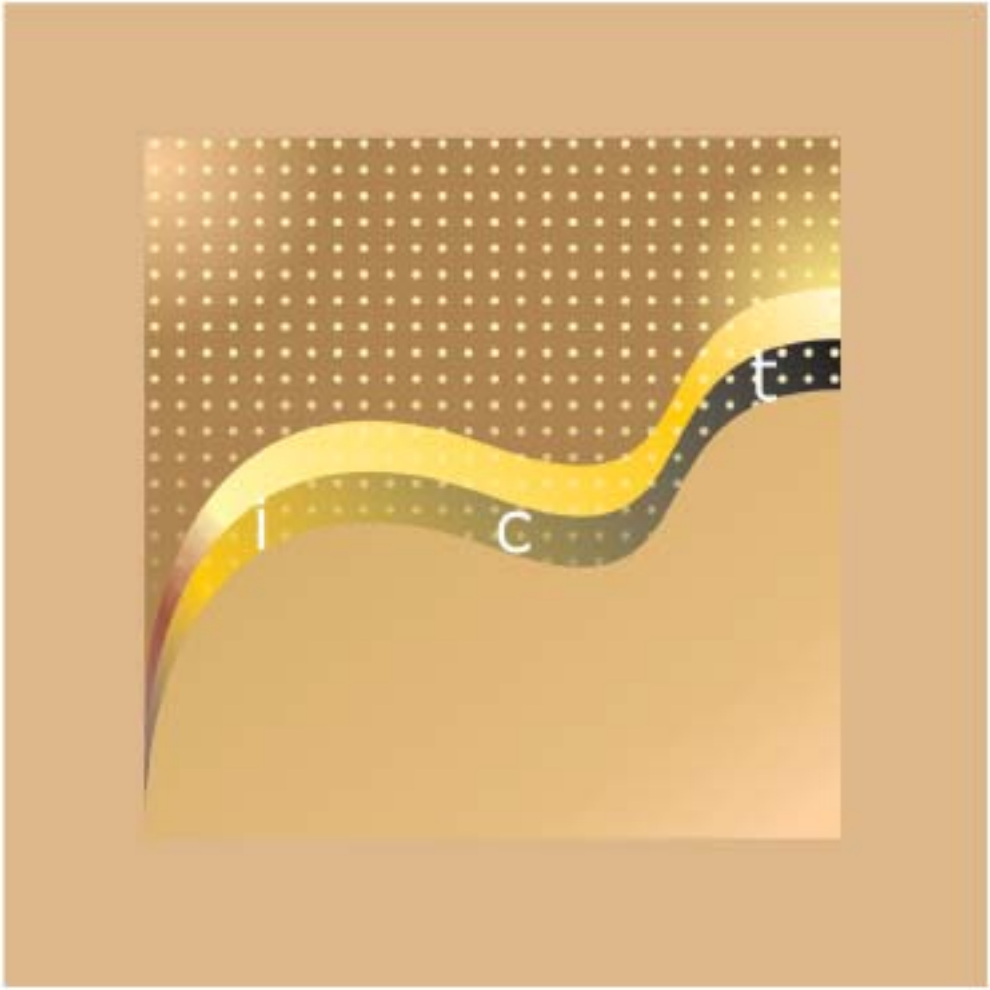
United Nations Conference on Trade and Development

E-COMMERCE AND DEVELOPMENT REPORT 2004

CHAPTER 6.



UNITED NATIONS
New York and Geneva, 2004

Chapter 6
Protecting Privacy Rights in an Online World

A. Personal data in the information economy

1. Introduction

Post-industrial economies, where information is a key asset, are also known as "information economies". An important asset of the information economy is personal data, primarily in the form of data about customers and potential customers. Indeed, during the dot.com boom, much of the value ascribed by stock markets to companies was based on the personal data they held, that is millions of registered users (read future customers), rather than on the products and services they had sold.

In information economies the task of protecting data is of paramount importance. While secure storage and transparent use are important for many categories of public information, managing personal data also involves important issues of privacy and the related need to strike a balance between privacy and the various needs to transmit personal data. The transmission of such data is fundamental for the conduct of e-business, but it needs a great deal of trust and confidence. With the growth of computing, the expanded use of the Internet and the extensive use of other technologies which facilitate the creation of data trails, privacy threats or at least the fear of them have substantially increased. Therefore, some form of legal protection of privacy is important for generating trust in e-commerce.

Various laws govern the processing of personal data, including those relating to intellectual property and consumer protection, and, most obviously, laws protecting privacy. Different jurisdictions adopt various approaches to the problem of data protection, and this poses problems of har-

Box 6.1

The need for laws protecting personal data

A recent example of this is the case of India. India has been extremely successful in developing an outsourcing industry, from basic data entry processing to more sophisticated services such as customer call centres and financial services, based on a literate workforce and a developed computer and communications infrastructure.[i] Indian businesses have attracted a wide range of Western companies, from financial services to utilities, to relocate various business processes to the sub-continent. However, concerns have recently been voiced in the European Parliament about the vulnerability of personal data being transferred under such outsourcing arrangements.[ii] Some view outsourcing as a process that effectively circumvents European regulatory safeguards. As a consequence, the Indian National Association of Software and Service Companies has recently been pressuring the Indian Government to take regulatory action to help forestall any reaction from Europe.[iii]

Another example can be found in Kenyan practice. Ms. Mugure Mugo, the founder of PrecissPatrol, a Kenyan outsourcing enterprise dealing with IT services, has already received requests from European-based clients specifically wanting to know the enterprise's policy on the collection and security of collected data.[iv] She recognizes that the fact that Kenya does not have specific data protection laws may constitute a barrier to the development of the country's e-business.

[i] See further chapter 5, "Business process outsourcing services for economic development", pp. 135-152, in UNCTAD (2003).
[ii] Bennet M (2004a).
[iii] Bennet M (2004b).
[iv] UNCTAD 2003., p. 143 et seq...

monization, especially in the case of transborder flows of data. Privacy laws governing the processing of personal data are particularly comprehensive in Europe. In European jurisdictions it is forbidden to transfer data to a jurisdiction that does not provide adequate protection. The "adequacy provision" could affect countries that do not provide such protection in their business with European countries.

Developing countries that want to participate in the information economy, and thus facilitate the free flow of information from developed to developing countries, have therefore to consider the need for laws protecting personal data.

This chapter is divided into six sections. Section A puts the question of data protection in context. Section B defines the various categories of personal data. Section C presents the privacy principles, the basis for data protection regulation. Section D deals with the regulatory approaches taken by the various jurisdictions, explaining why each jurisdiction has chosen a specific approach and the consequences of such a choice. Section E considers the question of transborder transfers of data, highlighting the interest of developing countries, and section F presents the results of a questionnaire on data protection legislation and offers some policy recommendations for developing countries.

2. Privacy of personal data as a fundamental human right

As stated in the Universal Declaration of Human Rights, privacy is a fundamental human right. Respect for privacy is viewed as a prerequisite to enable citizens to fully develop as individuals as well as to participate in society, although what is considered to constitute the concept of privacy and its boundaries may differ widely between cultures and societies. For some, the threat of interference is perceived to lie primarily in government and public administration. For others, the private sector is seen as an eqtual or even greater threat, as customer data have become an increasingly valuable asset.

Privacy as a right must coexist with and be balanced against other individual rights, such as the right of expression (Article 19 of the Universal Declaration), which is the basis for free media as well as with broader societal concerns, such as the threat to national security from terrorism.[1] The potential tensions between security and privacy needs is illustrated by the recent dispute between the United States and the European Union about the disclosure of passenger data by European airlines to US law enforcement agencies.[2]

A right to privacy is generally enshrined in national legal systems at the constitutional level, although there is increasing recognition that a more rigorous and detailed legal framework is often required. The Justice Ministers of the member States of the Commonwealth, for example, recently adopted a Model Privacy Law to assist individual members in establishing such a framework.[3]

Legal recognition of the importance of privacy extends beyond human rights conventions and constitutional protections. Under the WTO-administered General Agreement on Trade in Services, for example, the general obligation to remove measures that discriminate against or restrict trade in service is subject to certain general exceptions, which include "the protection of the privacy of individuals in relation to the processing and dissemination of personal data".[4]

3. Technological progress and data protection

While privacy has always been a concern, with the growth of computing in the 1960s and 1970s, there was widespread anxiety that the capabilities of computers with regard to the processing of information would engender a new threat to privacy, as noted by a report commissioned by the UK Government in 1975:

> "The speed of computers, their capacity to store, combine, retrieve and transfer data, their flexibility, and the low unit cost of the work which they can do have the following practical implications for privacy:
>
> (1) they facilitate the maintenance of extensive record systems and the retention of data on those systems;
>
> (2) they can make data easily and quickly accessible from many distant points;
>
> (3) they make it possible for data to be transferred quickly from one information system to another;

Box 6.2

Article 12 of the Universal Declaration of Human Rights

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"

(4) they make it possible for data to be combined in ways which might not otherwise be practicable"[5]

In response to these perceived threats, Governments and international organizations began to consider the need for a regulatory regime tailored specifically to address computer-derived threats to privacy. Within Europe, such regulation became known as "data protection" legislation. Data protection laws do not map neatly onto a privacy framework, but rather represent a range of differing interests. A broad distinction has to be made between "interests that relate to the quality of (personal) information and information systems", such as accessibility and reliability, and "interests pertaining to the condition of persons as data subjects[6] and to the quality of society generally", such as privacy, autonomy and democracy.[7] As a consequence of this broad range of interests, data protection laws cannot be seen as simply a subset of privacy law, but rather as a distinct but overlapping topic, also addressing data security issues.

More recently, as individuals, businesses, organizations and public authorities carry out an ever wider range of activities across the Internet, concern has again arisen about the potential threats to privacy from this online environment. This concern relates to personal data being made available on the Internet, and the monitoring of an individual's Internet-based activities.

In the first scenario, whether or not an individual uses the Internet, data collected from him/her may subsequently and increasingly be processed and made available on the Internet. A national telephone directory, for example, once placed on a server connected to the Internet becomes available to the world, thus resulting in potential exposure of a qualitatively different nature from that arising from the publication of the traditional physical directory. This qualitative shift can also be seen in respect of personal data contained in public registers, personal data that relate to our lives as citizens. For example, eligible voters in an area are traditionally listed in registers available for inspection from public offices. This information is now available on CD-ROM or the Internet. As a result, there has been a huge surge in demand for it from marketing companies, which regard "public" personal data as a valuable resource. In such situations, the Internet is basically a new medium within which personal data can be used and abused. The nature of the Internet facilitates the unfettered transmission of data around the world, with the potential to circumvent national regulations. In this respect, the concerns expressed with regard to the Internet echo those expressed in the early days of computing.

The second category of threat concerns the ability to obtain personal data arising from the online activities of data subjects when using an Internet-based service, such as e-mail,[8] the Web, Usenet or P2P applications. One aspect of this threat stems from the current insecurity of the Internet as a communications mechanism. Data subjects are generally not fully aware of the risks associated with disclosing personal information over the Internet. A second component relates to personal data arising from the monitoring of a data subject's Internet transmissions and connections, such as the websites visited and hypertext links followed. The collection of such information, particularly over time, can enable a detailed profile of an individual's preferences to be constructed.

In addition to the Internet, other technologies have a potential to pose privacy threats. For example, mobile phones and fixed lines may allow the identification and the location of the person who is calling. An Australian writer who has extensively written on new technologies identified as PITs (privacy-invasive technologies) calls this trend data-trail intensification (through identified phones, stored-value cards and intelligent transportation systems).[9]

With the expanded and extensive use of computing, the Internet and other technologies, the fear of privacy threats has substantially increased. According to a *Wall Street Journal*/NBC poll, 29 per cent of Americans ranked the loss of privacy as their primary concern for the 21st century.[10] According to the study entitled "The new e-government equation: Ease, engagement, privacy and protection", conducted by Hart-Teeter Research, more than 60 per cent of Americans who use the Internet are interested in using e-government, but they express concern that dealing with government over the Internet may compromise their privacy.[11] To react to these perceived fears, there is a strong need to build trust and confidence. Leaving aside the technological ways to do so, through data security mechanisms such as encryption, this chapter will focus on the legal ways to protect privacy, thus generating trust in e-business.

B. Categories of personal data

1. Definition

Before analysing the information privacy principles, which constitute the point of departure for data protection regulation, it is important to gain an understanding of what such principles are designed to protect -in other words, what is considered to be "personal data".

The concept of personal data is very broad and difficult to pinpoint. Personal data encompass any and all data that relate to an individual and that could be used, either directly or indirectly, to identify him or her. This includes information such as a name and birth date, which would permit direct identification of an individual, but may also include information such as a telephone number or a job title, which could be used, indirectly, to identify an individual.[12] In some jurisdictions, protection is extended to legal persons, such as companies and trade unions, as well as individual natural persons.

The types of personal data collected can be grouped into three general categories: consensual, non-consensual and sensitive data. These categories are outlined and explained below. It should be noted that while only certain data will constitute sensitive data, virtually all data can be categorized as either consensual or non-consensual data.

2. Consensual data

Consensual data are data that are obtained directly from an individual, with the individual's knowledge as to why it is being collected, and by whom, and with the individual's consent for its use, whether express or implied. For these to be truly "consensual data" the consent itself should be specific to the purpose provided, freely given and informed. Often, individuals provide these data when performing tasks such as filling out an application form, subscribing to a service or entering into a contract. They are data that an individual allows to be collected and used for certain specified purposes. In some instances, consent is implied from the fact that the individual has provided the data in order to enter into or fulfil a contract after having been informed accordingly. Under other circumstances, the data subject's consent can be implied from the fact that the person giving such consent has not objected to any purpose or further transfer after having been informed of them and given the opportunity to object to the processing. This implied consent procedure is termed an "opt-out" procedure. Under an "opt-out" procedure, the data may be used for the purposes specified, unless the individual indicates that he/she does not agree with this. However, implied consent may not be appropriate in many circumstances, and explicit consent should be obtained. One clear circumstance is where the data are of a sensitive nature, a category of personal data that is addressed below. Here the data should be obtained via an "opt-in". Under an "opt-in" procedure, the data may be used for the reasons given only where the individual affirmatively indicates this is acceptable. This is the standard for consent to use of sensitive data in many countries, notably the European Union (EU) member States.

3. Non-consensual data

Non-consensual data are data obtained without the knowledge or consent of the individual. These data may be consensual data reorganized according to certain criteria, such as geographical location, gender or income level, and then sold in the form of marketing lists to various companies or organizations. Non-consensual data may also be data collected as part of a transaction, such as what items were bought or what service was ordered, the price range of the items or service, the styles or options, and any other data that may be part of the transaction. Non-consensual data are often

combined with data from various sources to compile a more complete profile of the data subject.

A consumer may consent to the collection of personal data for specific purposes, and yet considerable amounts of valuable data may be collected through the transaction process. For example, data about the style of clothing bought, the colours, sizes, brands, general price range of each item, and payment method are all collected as part of the transaction. These data is collected without the express consent and perhaps without the knowledge of the consumer, and allow the online retailer to create a marketing profile of the consumer. This profile can then be used in-house, or sold to marketing agencies or manufacturers.

Trace data are unique to the online environment. Although non-consensual data, they are usually obtained directly from the individual but without the individual's knowledge. Trace data are data that are obtained by tracking an individual's use of Internet-based services. The data, depending on how they are collected, may include information on what websites were visited, which pages were viewed and how long an individual spent on a certain page of a website. The data collected will include information such as the IP address the consumer is using, the programs his/her computer is running, other sites visited, hypertext links clicked on, the computer's time zone, and possibly the e-mail address of the person using the computer.

Trace data are often collected through the use of "cookies", which are unique identifiers that web servers will place on an individual's computer. In essence, a cookie is a serial number for a computer that allows the web server to retrieve records regarding that computer from the web server's databases. Cookies will often be used by a website to recognize a certain computer or user, allowing automatic log-in, or to facilitate a faster consumer transaction by identifying the user and automatically charging a purchase to the consumer's credit card information already on file with the website, such as Amazon's "1-Click" transaction service. However, trace data may also be collected through the use of other technologies called "web bugs" and "spyware". Like cookies, these data-gathering tools operate in the background, without the user's explicit knowledge. A web bug is a graphic placed on a web page, or even in an e-mail message, that is designed to gather information on visitors to a website or on the individual(s) who read the e-mail. Web bugs are generally invisible, as they are added to web pages as part of the elements of the site and are usually only 1 pixel-by-1 pixel in size. Spyware is generally software that is automatically installed on an individual's computer system. It is usually designed to collect information without the user's knowledge and permission and, if so configured, to forward the information about software being used and the browsing and purchasing habits of the user to a specified data collection facility.

4. Sensitive data

Sensitive data are data considered by policy makers and legislators to reveal fundamental aspects of our private lives, and therefore require a higher level of protection to prevent privacy infringements. This may include requirements for data controllers[13] to obtain explicit rather than implied consent, enhance the security measures implemented and further limit the types of processing that may be carried out. Such enhanced protection is deemed necessary because discriminatory use of the data could substantially infringe an individual's privacy.

What is considered "sensitive" may obviously vary significantly between jurisdictions, reflecting different cultures. In the United Nations' "Guidelines for the Regulation of Computerized Personal Data Files", for example, Principle 5 prohibits the processing of certain types of data: "data likely to give rise to unlawful or arbitrary discrimination, including information on racial and ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled".[14]

Under European Union law, personal data used in particular contexts have also been subject to special regulatory treatment. In the telecommunications sector, for example, data relating to an individual's use of telecommunication services (e.g. number called, call duration and location data) are considered to pose increased risks to an individual's privacy and are therefore subject to additional legal protections. In the United States, financial data and data relating to a person's choice of video rental are considered sensitive enough to merit specific legislative protection.

C. Principles of good practice

There has been significant activity at an international level towards the recognition of a set of international data protection principles. In the early 1980s, the Council of Europe and the Organisation for Economic Co-operation and Development (OECD) adopted a number of measures, and the United Nations followed in 1990 with "Guidelines for the Regulation of Computerized Personal Data Files".[15]

Since most of the data protection regulation has been developed around the same fair information practices (or privacy principles), a description of such regulation should be preceded by an analysis of those principles. They set limits to processing, that is the performance of such operations as collection, handling, use and transfer of personal data that can be done manually as well as electronically, although electronic processing is generally perceived as presenting the greater risk to privacy. The principles also address the transfer of personal data to parties in places that do not have similar protection.

The privacy principles are present in the international instruments mentioned above as well as in relevant national legislation. They have also been adopted by the private sector in self-regulatory initiatives (see further below). Thus, despite the legal meaning they may assume according to the specific instruments in which they are enshrined,[16] one may consider their uniform repetition as evidence of *diuturnitas* (the practice of States), one of the basic features of general international law, the other being *opinio iuris ac necessitatis* (acts must occur out of a sense of obligation). If the second element is also present, the principles would then be binding on all States, regardless of their inclusion in national laws.

The advantage of a principles-based approach to the regulation of data protection is the avoidance of technological redundancy. The principles should therefore be as applicable to the Internet as they were to the introduction of computer technology, in other words they should be technologically neutral. It is the mechanisms by which such principles are complied with that obviously change in response to the new threats and opportunities created by the changing technological environment. These principles of good practice are set out below.

1. Collection

Collection of personal data should be done fairly and lawfully. Fair collection means that an individual should be informed, at the moment of collection, of the contemplated uses of that data (see also the transparency principle below). The lawfulness of data collection may be specified in different ways. Some jurisdictions, generally common-law-based, state that the collection of data is lawful provided that it is not in breach of any existing legal obligation governing the use of those data (e.g. confidential information). Other jurisdictions, generally civil law, restrict the concept of lawful collection further by stating that collection is only lawful where the data subject has given his/her consent or some other specified and limited criteria are met (e.g. the collection is necessary in order to perform a contract on behalf of the data subject). Consent is not generally considered meaningful unless it is freely given and the individual has been given adequate information about the nature of the processing activity, such as the purposes for which the information will be used, to whom it may be disclosed and any consequences that may result from withholding information or permission to use.

2. Proportionality

The collection of personal data should be limited to data that are adequate and relevant for the specified purpose or purposes. Since computers can hold vast amounts of data easily and relatively cheaply, there may be a tendency to collect excessive information from, or about, a data subject without a specific need. In addition, such data should be retained only for the minimum period of time needed to accomplish the purpose(s) for which the data are collected.[17] Data destruction procedures may be as important for the protection of an individual's privacy interests as the process of data collection and retention. For instance, billing data should in principle be retained only for the period during which the bill may be challenged or the payment pursued.

3. Use

There should be no disclosure, transfer or other use except those needed to achieve the purposes specified when the data were collected. Obvious exceptions to this principle may be where the

secondary use is required by law or for some other public interest, such as the investigation and detection of crime. Personal data should be used only in a manner consistent with expectations. Individuals provide data, or allow data to be collected, for a certain specific purpose. Data should be used only for that purpose, and should be further used or communicated only if this is necessary in order to accomplish the original purpose.[18]

4. Quality

Personal data that are collected and stored should be accurate and reviewed periodically to ensure that they are kept accurate and up to date. This principle is an example of where the privacy interests of the individual should overlap with those of the entity, whether public or private sector, which is processing the data.

5. Transparency

In line with the concept of "fair" collection noted above, individuals should be informed of the purpose(s) for collecting data, who will be using the data, who is in charge of protecting those data, and, if applicable, any contemplated transfers of the data and to whom.

6. Access and correction

Individuals should have the right to inquire whether their personal data are being used and the right to obtain a copy of all personal data collected and maintained that relate to them. There will be certain exemptions to the granting of such access, for example where the information would also reveal personal information provided by another party, whose privacy interests also need to be considered. Individuals should also be given the right to have inaccurate data corrected.[19]

7. Objection

Individuals should have the right to object to the processing of the personal data relating to them in certain situations, such as where serious damage or distress results, or for specified purposes, such as use for direct marketing activities.

8. Transfers/disclosure

Personal data should not be transferred to third parties unless the individual was informed that such disclosure may take place and provided that it can be ensured that the data will be given the same level of protection by the recipient as was provided by the sender. This is particularly an issue where data are transferred between jurisdictions that have different legal frameworks.

9. Security

Appropriate security measures should be implemented to protect against risks presented by the collection, use and storage of an individual's personal data, whether from accidental loss, damage or disclosure or deliberate interference. This may require the use of organizational measures, such as the appropriate screening and training of employees; technological measures, such as encryption and access controls; and physical measures, such as preventing computers from being stolen. The appropriateness of the security measures applied will depend on the nature of the data concerned (e.g. sensitive data), the purposes for which they are being used, the availability of the protection mechanisms and their cost, relative to the risks involved.

10. Accountability

Data controller compliance should be ensured through a system of enforcement, which includes the ability of a data subject to seek redress for breach of the principles in the processing of his or her personal data. The implementation of substantive rules controlling the ways in which personal information can be collected, processed and disclosed is obviously insufficient in and of itself. There is also a need for a procedural framework that ensures that such rules are complied with and that remedies are available for non-compliance.

D. Regulatory approaches

The German State of Hesse enacted the first law directed specifically at the protection of personal data in 1970. Laws in Sweden and the United States followed soon after. Throughout the rest of the 1970s most developed nations followed suit,

enacting some form of privacy or data protection legislation themselves. However, by the late 1970s the differences in the provisions of these various national laws had created the threat of obstacles to the free flow of information between countries, potentially stifling economic growth. To create more coherent and uniform laws, intergovernmental organizations such as the OECD and the Council of Europe outlined common data protection principles to be followed by member States. The principles outlined by those two organizations are the foundation for most national legislation in place today.

1. Approaches taken by international organizations

In 1980 the OECD concluded a study that culminated in the creation of the OECD Council Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data[20]. The Guidelines established eight basic "privacy principles", which apply to any information relating to an identified or identifiable natural person, cover both the public and private sectors, and encompass all types of data processing.

The Guidelines require that member countries' data protection standards provide equivalent protection. If a member country does not provide equivalent protection for certain categories of data, the Guidelines provide for the implementation of legitimate restrictions on transfers of those categories of data to that member country.

The Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[21] is similar to the OECD Guidelines in that the principles also apply to both the public and the private sector. It differs from the OECD Guidelines in that it applies only to automated data processing. They also differ in their emphasis: the Convention stresses the privacy of the individual, while the OECD Guidelines emphasize the desire to ensure the free flow of information.

Although the two organizations are in general agreement as to the nature of privacy principles, the OECD Guidelines are non-binding in law, whereas the Convention is an instrument of public international law, which signatory member States are obliged to implement through the adoption of national legislation reflecting the Convention's provisions. Moreover, the means by which the provisions are given effect in national law vary from State to State.

The United Nations adopted a measure addressing the human rights aspects of the use of computer technology some ten years after the OECD and Council of Europe. In 1990, the General Assembly adopted a set of “Guidelines for the Regulation of Computerized Personal Data Files”.[22] These Guidelines are divided into two sections. The first section covers "Principles concerning the minimum guarantees that should be provided in national legislations". These principles echo those put forward by both the Council of Europe Convention and the OECD Guidelines. The second section considers the “Application of the Guidelines to personal data files kept by governmental international organizations”. This requires that international organizations designate a particular supervisory authority to oversee their compliance. In addition, it includes a “humanitarian clause”, which states that "a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance".

Such a clause is intended to cover organizations such as Amnesty International, which hold large amounts of personal data of prisoners, but would be wary of sending information out to a data subject on the basis of an access request made while the person was still imprisoned.

The UN Guidelines also provide for the principle of non-discrimination, according to which sensitive data should not be compiled at all. The power to make an exception to the principles contained in the Guidelines is severely limited and a national supervisory authority should have the power to impose sanctions for non-compliance.

2. Current approaches to data protection law

The OECD and Council of Europe principles established the fundamental principles of fair information practices for the protection of personal data. However, the approaches taken by states to implement these principles into national legislation have developed along three different

lines. The conflict between these approaches is centred on methodology and scope, and not on basic privacy principles. The three basic approaches developed to implement data protection principles are comprehensive regulation, sectoral regulation and self-regulation/co-regulation.

Comprehensive or omnibus regulation

A comprehensive regulatory approach essentially builds on the Council of Europe model of *omnibus* or universal protection. This approach requires the creation of a general law promoting fair information practices. In addition to laying out rules establishing the parameters for collection, use and dissemination of personal data in both the public and private sectors, the law must provide individuals with the right to receive confirmation as to what data, if any, are maintained about them and the right to have those data rectified if they are incorrect or incomplete. The most important aspect of the comprehensive approach, from the individual/consumer's perspective, is the requirement that prior to the collection or use of any personal data, the individual must be notified of what data will be collected and how they will be used. Consent for that processing must usually be obtained. The goal is to give individuals greater control over their personal data. This is the approach taken by the European Union in Directive No. 95/46/EC of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, otherwise known as the Data Protection Directive.[23]

Supervision of the implementation and enforcement of the law on a national basis, as well as of compliance with it, is conducted by a national supervisory authority or regulator. This authority also acts as the guarantor of individual rights and must therefore be empowered to act independently of other government bodies. At a minimum the supervising body's powers must include the powers of investigation and intervention, particularly in cases of complaints from individuals, and the power to engage in legal proceedings. In some countries, such as Germany, the comprehensive regulatory approach requires each data controller to appoint an "in-house supervisor". The duty of this supervisor is to identify, monitor and analyse the purposes and practices of processing within the company, organization or association in which he or she operates. The supervisor is also legally responsible for ensuring that an individual's rights are protected, and he/she should therefore be endowed with sufficient authority to act autonomously from the rest of the organization, since the controller is directly accountable to the national oversight body, not to the organization for which he/she works.

Until recently South American countries generally did not have legislation regulating data protection, but now a number of countries from the region have been re-evaluating their legislative regimes as they pertain to the protection of personal data, partly because of the EU Data Protection Directive. As a result, some South American countries follow the comprehensive approach. On 11 November 2003 a judge in Buenos Aires issued the first injunction under the Argentine data protection law.[24]

Because of the nature of the comprehensive approach, the transfer of personal data to countries where the data are not provided the same level, or an adequate level, of protection is prohibited. This is to prevent circumvention of the law through the use of a third-party country, and to protect the rights of the individual in their personal data. For data to be transferred to a country with less than adequate protection, the individual must consent to the transfer or arrangements must be made, either via contract or some other method, to ensure that the data will receive the requisite protection (see further below).

Sectoral regulation

The sectoral approach does not opt for the use of all-encompassing legislation, and instead relies on localized legislation. The theory behind a sectoral approach is that over-regulation by the Government will stifle growth and innovation. The belief is that markets should be allowed to self-regulate, with the Government only stepping in to provide protection in areas where there is a high risk of harm if data are misused, such as the financial sector or in the case of data relating to health or children. A typical example of a country following this approach is the United States; other countries following this approach are Japan, Singapore and Barbados. It can be argued that the sectoral approach stands as its own model of data protection.

In the sectoral approach there is no national oversight agency. The general trend among countries following this approach has been to enact legislation in the public sector, protecting individuals from governmental abuse of personal data, while leaving the private sector relatively regulation free. The creation, implementation and enforcement of rules, and the imposition of sanctions for violation of those rules, are left to individual sectors or industries. Where data protection rules are imposed in a sector or implemented voluntarily, they will usually take into account some of the privacy principles outlined in the OECD Guidelines or the Council of Europe Convention, but these rules will apply only within the specific sectors where they are enacted or to the extent that they are voluntarily enforced. Various companies, especially in the United States and Canada, have publicly adhered to the Guidelines. Recently, Singapore adopted a Model Data Protection Code establishing minimum standards for the private sector.[25] However, the basic assumption in a sectoral approach is that where there is no governing legislation, regulation or code of conduct, there is no legal protection.

Generally, national legislation is enacted to provide greater protection in the financial, telecommunications and medical sectors. In addition, most professions, such as doctors, accountants, lawyers and bankers, are bound by strong confidentiality practices. The failure of many organizations in the United States to embrace meaningful self-regulation led the Federal Trade Commission, the agency responsible for oversight of undertakings' compliance with stated privacy policies as a fair trade practice, to assert the need for more comprehensive privacy regulation.

Self-/co-regulatory approach

The self-/co-regulatory approach can be considered a hybrid of the comprehensive and sectoral approaches. Like a comprehensive approach, a self-/co-regulatory approach centres on universal legislation at a national level that provides individuals with rights in their personal information, and protects these rights by regulating collection, use and transfers of personal data. The primary difference between the two approaches is the manner in which the data protection principles are implemented. Under a self-/co-regulatory approach, creation, implementation and enforcement of data protection regulations, including rules, codes of conduct and/or legislation, are left to individual industries and are overseen by a privacy/data protection agency. This agency ensures compliance with the rules and is responsible for handling complaints and resolving disputes. On top of this sectoral approach is national legislation that is applicable across the board, providing a minimum level of protection to all individuals in their personal data. Industries that do not implement their own codes or rules are then subject to the standards of this legislation. Examples of countries implementing a self-/co-regulatory approach are Australia, New Zealand, South Africa and the Republic of Korea.

The self-/co-regulatory approach, like the *omnibus* approach, typically establishes a national oversight agency that is endowed with considerable power and authority. This agency may be the main oversight body for all legislation dealing with privacy and/or data protection that encompasses both the public and private sectors. This is unlike the sectoral approach, where some areas of legislation are governed by one national body while others may govern other areas.

The result of a self-/co-regulatory approach is that individuals are assured that their personal data will receive a minimum level of nationally mandated protection, but the standards may differ between industries or sectors. The differing levels of protection among the various sectors and industries may work to restrict or complicate flows of data from one sector or industry to another. However, this approach may also permit the industry-specific codes or rules to reflect its realities or particularities. This helps avoid regulation that is excessive or unnecessary in an industry or that just does not fit and thus would be unduly costly or act as a barrier to commerce.

E. Transborder transfers of data

Transborder flows of data result from an expansion of international trade, globalization and the emergence of the information economy, and is an inevitable aspect of the use of Internet-based services. However, such transfers may result in an infringement of the privacy rights of an individual, when data are moved from a protective regime to a jurisdiction without such legal protections.

The primary goal of data protection legislation is to protect the personal data of those who live within the borders of that jurisdiction, which could be compromised if data were allowed to be transferred outside the country to a jurisdiction where the protection requirements are less onerous, in effect circumventing individual rights. To avoid this, countries that have data protection laws have adopted rules regulating transborder transfers of data. The degree of regulation will obviously vary according to the regulatory approach taken. Therefore, prior to any transborder transfer of data those seeking to transfer the data must be aware of, and understand, any laws applicable to them that govern such transfers.

1. Transborder transfers of data under the comprehensive approach

The comprehensive approach is generally the most restrictive with regard to transborder transfers of data. Owing to the protective nature of the comprehensive approach, transfers are prohibited unless the country or jurisdiction to which the data are transferred offers what is considered to be "adequate" or "equivalent" protection. In that connection, certain safeguards must be in place to ensure the continued protection of personal data. Exactly who will make determinations of adequacy may vary depending on how the comprehensive system is established. In the first instance, determinations may be made by the exporting data controller, on the basis of the specific circumstances, with the national supervisory authority exercising regulatory oversight. Alternatively, the authority may issue *ex-ante* general determinations for specific jurisdictions or sectors of activity.

Determinations of adequacy are generally based on the type of data being transferred and the kind of protections that are afforded to those data: the more sensitive the data, the greater the protections required. The protections may be legal, contractual or in some other binding form, but must be sufficient to ensure the continued protection of the transferred data.

To be adequate, the protections must also be enforceable; data protection rules are only effective if they are followed in practice. It is therefore necessary to consider not just the content of rules applicable to personal data transferred to a third country, but also the procedural mechanisms in place to ensure the effectiveness of such rules. This will include considerations of economic and political stability, the viability of regulatory or judicial systems, and examination of other socio-political aspects that may result in a lack of security. Thus, the adequacy of another country's data protection rules should be determined on the basis of the content of the rules and on the basis of the means and entities used to ensure their proper application. For the time being the EU has made findings of adequacy for Argentina, Hungary, Switzerland, Canada and for those US organizations that have subscribed to the "safe harbour" arrangement.[26]

2. Transborder transfer of data under the sectoral approach

The sectoral approach is generally the most relaxed with regard to transborder transfers of data. This is due to the desire to let markets adjust themselves, with little or no governmental intervention. However, in many countries sector-specific legislation or regulations have been enacted to provide protection for certain types of personal data. The sectors traditionally regulated are the financial sector and the health sector. Thus, any transfers of data regarding financial data or health data are likely to have restrictions that must be complied with. The restrictions will generally require that notification of the transfer be provided, and possibly that consent be obtained prior to the transfer. The key aspect in a sectoral approach is not necessarily the type of data that is being protected, but the sector where the data originated. For example, financial information may be protected only if it is a regulated financial services provider that collects and uses it. The same applies to health information: it must be collected and used by a regulated healthcare institution or insurer under the sectoral legislation. Canada has adopted this solution: its legislation contains no explicit reference to international data transfers, but it requires that any transfer to any third party result in continued protection under Canadian privacy standards. This permits parties to such transfer to make protective arrangements suitable to the circumstances, thus avoiding the burdens and negative impact of overly restrictive data flows.

3. Transborder transfer of data under the self-/co-regulatory approach

The rules regarding transborder transfers of data under the self-/co-regulatory approach are similar to those under a comprehensive approach. The overarching national protection provided in this approach establishes a level of protection for all individuals. Transborder transfers of any data of any individual must meet the standards set out by national law. This level is generally on a par with that of the comprehensive approach: there must be an adequate level of protection. However, a self-/co-regulatory approach will often differ from a comprehensive approach in how determinations of adequacy are made. While there is oversight on a national level in a self-/co-regulatory approach, individual sectors are generally responsible for adopting standards and making determinations of adequacy. The result is that where a comprehensive approach will look at the level of sensitivity of data to determine what is necessary in order for protection to be considered adequate, a self-/co-regulatory approach may look at the sector where the data originated in order to determine adequacy. This is similar to a sectoral approach. For example, under a self-/co-regulatory approach financial data generated by a financial institution may receive greater protection than financial data gathered from a voluntary survey, even though it may be the same data.

The self-/co-regulatory approach differs from the sectoral approach in that the data collected via the survey are still guaranteed a level of protection prior to any transborder transfers. This is most likely not the case in a sectoral approach.

4. Issues for developing countries

The three approaches to data protection outlined above are approaches traditionally taken by industrialized countries in an effort to protect personal data yet allow for the free flow of information. While data protection legislation is generally designed to be effective domestically, restrictions on transborder transfers of data can obviously have a direct effect on other countries. This is particularly true in many developing countries, where legal infrastructures often offer little protection, if any, for personal data. This may have a detrimental effect on many developing countries, as their domestic business such as data processing and call centres may be limited owing to restrictions on transfers of data from developed countries. Depending on the approach adopted by the country where data are sought to be transferred from, there are several options for developing countries.

As discussed above, under a comprehensive approach the transborder transfers of personal data are limited to countries providing adequate protection. There are several ways, however, in which an adequate level of protection may be provided: by the country enacting similar legislation, through contractual measures, or through "safe harbour" arrangements.

As explained above, the primary focus in a determination of adequacy is whether sufficient protections are available and whether those protections are enforceable. Of course, the easiest way to verify this is to ascertain whether the country seeking to receive data has adopted similar comprehensive legislation. In such instances, a determination of adequacy is generally a relatively simple matter, and once such a determination is made restrictions on transborder transfers are either abolished or significantly minimized.[27]

However, for many developing countries a comprehensive legislative approach may be too restrictive and burdensome. An alternative option may be to enact legislation, regulations or administrative rules in a specific sector, such as the telecommunications or financial sector, that are sufficient to be considered to provide adequate protection, allowing data to be transferred to data controllers within that sector.

When enacting legislation is not feasible, transborder transfers of data may still be facilitated on an individual basis through the use of contractual measures. Organizations that wish to receive data from a country with a comprehensive approach can enter into a contract, which then obligates the organization to take proper measures to ensure the protection of the data. The Council of Europe and the European Union have both adopted model contracts designed to facilitate the transfer of personal data,[28] as well as various industry organizations, such as the International Chamber of Commerce.[29]

In some instances, arrangements may be made between countries with comprehensive legislation and countries following a sectoral approach

to allow for transborder transfers of data. These are termed "safe harbour" arrangements. A safe harbour arrangement is designed to create a workable set of rules that organizations in a country with a sectoral approach can voluntarily adhere to, and that are recognized as providing adequate protection by a country with a comprehensive approach.[30] Essentially, this involves voluntary compliance with the fair information processing principles, plus an agreed enforcement regime operated, for example, by a consumer protection body (e.g. the US Federal Trade Commission). Organizations that participate in a safe harbour arrangement are then placed on a publicly available list, which allows individuals, organizations, and other countries to know which organizations may and may not receive data transfers.

The sectoral approach to data protection has traditionally been considered to be much friendlier to developing countries. This is because such an approach generally offers fewer barriers to transborder transfers of data. However, as more countries adopt a comprehensive approach to data protection, this approach may result in the data flows to developing countries being threatened. As discussed previously, even under the sectoral approach, there are often regulated sectors that may have more restrictive protective measures, typically the financial and health sectors. For transfers from these sectors to be allowed, proper measures must be taken, such as enacting similar protection or entering into contractual obligations, much like under a comprehensive approach, only more limited in scope.

With respect to transborder transfers of data to developing countries, a self-/co-regulatory approach is similar to that of a comprehensive approach: there must be adequate protection. Therefore, the three options available under a comprehensive approach -namely, enacting legislation, contractual remedies or safe harbour arrangements are available here as well. However, where a comprehensive approach has essentially two standards, for regular data and sensitive data, a co-regulatory approach may permit variations of those standards, depending on the industry or sector. An adequate level in one sector may not be adequate in another. Thus, individual undertakings in an industry that would not meet the other country's sector standards might need to put in place contractual arrangements.

F. Survey on data protection legislation

To complement the analysis above, the UNCTAD secretariat developed a questionnaire that was circulated through a note verbale to member States. Governments were invited to complete the questionnaire and to provide UNCTAD with a copy of their national legislation on the issue of data protection.

The survey asked whether the country had adopted any regulation on privacy matters. Questions were designed to identify the approach chosen by the country while regulating data protection. Other questions looked at the various categories of data to see whether they were regulated differently (for example, computer-based records versus manual records, sensitive data versus non sensitive data). Some questions explored the manner in which privacy rights were implemented and the possibilities given to individuals to access and modify their data. Finally, a specific question inquired about the situation regarding commercial trade secrets.

1. Results and analysis of UNCTAD survey

Responses to the questionnaire were received from the following countries: Argentina, Belarus, Bulgaria, Colombia, Croatia, Czech Republic, Denmark, Dominican Republic, Egypt, Estonia, Finland, Guatemala, Italy, Jordan, Latvia, Lebanon, Lithuania, Malta, Mexico, Monaco, Morocco, Myanmar, Pakistan, Panama, Philippines, Republic of Moldova, Romania, Russian Federation, Serbia and Montenegro, Slovenia, Suriname, Turkey, Ukraine, Uruguay and Venezuela.

Before some of the results of the survey are described, it is important to state that certain responses were vague or contradictory. Thus, the results of the survey confirm the lack of awareness regarding the various implications of data protection issues. Moreover, various countries noted that since the data protection laws were adopted recently, there is still no experience in their implementation. Also, some data protection authorities or agencies are not yet fully operational.

In all countries that answered the questionnaire, with only two exceptions, the protection of pri-

vacy is established at constitutional level. While the constitutional protection may be important, it is by no means sufficient in itself, as the implementation of the good practice principles (discussed above) is not guaranteed. Some countries stated that even though they do not have specific data protection legislation, some form of protection may be derived from other legislation. Other countries indicated that they have sectoral legislation and are in the process of drafting a more comprehensive law on data protection. The rationale stated for more comprehensive legislation is the desire to have internationally recognized standards that would facilitate international trade.

The majority of the countries that answered the questionnaire have adopted a comprehensive approach, but this result probably does not reflect the global situation as most of the countries adopting the *omnibus* approach are European or South American. In some of these countries, in addition to a general law protecting the privacy of data subjects, there are specific regulations for specific professions or services. The sectors for which in most legislation there are specific provisions are always the same: banking, lawyers, notaries, statistics, archives, health, military and police, intelligence services, taxation and scientific research. Interestingly, in some countries, besides primary *omnibus* legislation on data protection there are codes of conduct and professional practice. These codes do not in principle have binding force and therefore represent a very flexible instrument whose application could be envisaged in other fields.

The same sectors that also receive specific legislative consideration under the comprehensive approach are the only ones normally regulated according to the sectoral approach. Only two countries have adopted a sectoral approach.

Another large group of countries have chosen a self-/co-regulatory approach. Even among countries adopting a similar approach some differences are noteworthy. For instance, while in some countries it is possible to access and have corrected personal information relating to a specific sector (i.e. banking or legal), the same is not possible in other countries. Also, the remedies available to individuals to redress any infringement of data protection rules vary enormously, but this may also depend on the peculiarities of the domestic legal systems.

Finally, it should be noted that security concerns play a role in the regulation of data protection: more than one State mentioned them as an important limitation on rights to privacy.

2. Concluding remarks and policy recommendations

The right to privacy is not a new concept, and has been solidified over the years through incorporation into numerous treaties, conventions and declarations. As e-commerce has developed, so have the means to amass, exploit and retrieve greater amounts of personal information. Although this may seem a threat to our privacy, in many regards it may be viewed as beneficial. It is this paradoxical contrast between keeping personal information private, while allowing use of that information to generate business and facilitate e-government, that is at the heart of the current data protection debate. Regulation that permits individuals to control the use of their personal information may limit to some extent the information available and has a cost with regard to implementation. On the other hand, failure to provide adequate protection may allow greater use of such information, but also dissuade many consumers from utilizing Internet-based services and inhibit information flows from protective regimes to non-protective regimes.

Thus, policy makers from developing countries need to understand the implications of the different interests at stake and make an attempt to balance them.

Awareness of data protection issues should be further promoted, since, as shown by the survey, there is still some confusion about the nature, importance and implications of those issues. This could be done through efforts to educate the public on their privacy rights, to educate business about how to comply with privacy regulations and to assist companies in establishing privacy policies.

Regardless of the regulatory approach adopted to address data protection issues, every effort should be made to enact a technologically neutral regulatory framework, capable of responding to the rapidly evolving online environment.

When examining the regulatory response of developing countries to the issue of protecting personal

data, it is obviously necessary to distinguish between the policy drivers that dictate and underpin the regulatory framework and the regulatory mechanisms and tools utilized to achieve them. In terms of policy drivers, the demand for developing country Governments to address the issue of protecting personal data may primarily originate from a domestic agenda or from developments abroad.

At a domestic level, data protection will generally be focused more on concerns about the use and abuse of personal data by the public sector, rather than by the private sector. The value of an individual's data is obviously directly related to a nation's state of economic development, the sophistication of private sector activity and the purchasing power of consumers. Personal data as an asset are a particular feature of service sector economies, specifically the information economy, not agrarian or industrializing economies. Of the two broad groupings of interests represented under the concept of data protection, the interests pertaining to individuals as citizens, protected from arbitrary governmental interference or participating in the democratic process, generally drive domestic calls for data protection regulation.

The pressure for a regulatory response to protect personal data may arise from developments abroad. As noted in the introduction, developing countries may perceive a need to address issues of data protection to facilitate their participation in the global information economy, so as to ensure that an absence of protection does not constitute a barrier to the flows of data between developed and developing economies. We saw at the beginning of the chapter the example of the Indian outsourcing industry. The Indian National Association of Software and Service Companies has exerted pressure on the Indian Government to take some form of regulatory action to help forestall any reaction from Europe.[31] Moreover, after the adoption of the Data Protection Directive, the possibility of restrictions on the transfer of personal data from the EU has been an added impetus for countries such as Australia, Canada[32], Philippines[33] to put in place or at least try to work out comparable data protection schemes.

The rationale for drafting a new piece of legislation on data protection given by the Ministry of Energy, Communications and Multimedia of Malaysia reflects both domestic concerns and international developments. The legislation should promote the country as:

1. A communications and multimedia hub where the national adoption of e-based transactions is expected to be high;
2. A premier investment centre for the communications and multimedia industry;
3. A premier test-bed for applications of information and communications technologies;
4. A preferred trading partner in the communications and multimedia industry that provides international standards of personal data protection.[34]

Whether calls for data protection regulation primarily reflect domestic concerns or are a reaction to the legal situation in other countries, Governments will obviously need to consider the appropriate regulatory approach comprehensive, sectoral or self-/co-regulatory.

- The first consideration will involve the identification of the major trading partner. If the partner is, for instance, the United States, there might not be the need to adopt stringent or comprehensive regulation as in the case in which the major trading party would follow the EU approach.
- The cost of regulation will then be a critical factor. The cost associated with a comprehensive or *omnibus* approach, specifically the establishment of a dedicated regulatory authority, will generally be excessive for most developing countries, especially if borne by the private sector through licensing or notification fees. However, in terms of addressing privacy concerns vis-à-vis public sector infringements, an authority independent from government will generally be necessary in order to provide the necessary trust and assurance as regards its activities. The regulatory authority may not have an exclusively data protection remit, which mitigates the costs involved.[35]
- A sectoral regulatory response may be appropriate to address specific uses and abuses of personal data, whether driven by domestic or foreign concerns. In the telecommunications sector, many developing countries have established regulatory authorities as part of an ongoing liberaliza-

tion process within the sector.[36] Also, in the financial sector, nearly all countries maintain a distinct regulatory regime, which may address the protection of consumers of financial services, as well as the wider strategic economic aspects of the sector. These new or existing regulatory bodies may be capable of embracing data protection and privacy issues within their spectrum of duties.

- Whilst a self-regulatory or co-regulatory approach may be appealing in terms of minimizing the public costs of regulation, its success depends on a sufficiently strong and active private sector, willing and able to fund the regulatory activity. It is unlikely to be appropriate in terms of the public sector use of personal data.
- Governments of developing countries, especially those that are members of regional economic groupings, should be encouraged to establish cooperative relationships, so as to increase their capacity to deal with privacy and data protection issues.
- In addition to a regulatory approach, voluntary adherence to privacy principles should be promoted both in the private and in the public sector. This could be done through the introduction of flexible instruments such as codes of conduct or guidelines or through the promotion of trust mark initiatives.

Annex I

List of States that completed the questionnaire, and their laws on data protection

Argentina: Constitution, articles 18, 19, 33 and 43; Civil Code, art. 1071; Data Protection Law n. 25.3297/2000 and its Regulatory Decree n.1558/2001

Belarus: Constitution, art. 28; Law on Electronic Documents n. 357-3 of 10 January 2000; Decree of the Council of Ministers on State Programme on Informatisation n. 1819 of 27 December 2002; Presidential Decree n. 195 of 6 April 1999 amending Some Issues of Informatisation

Bulgaria: Constitution, articles 30, 32, 33, 34, in State Journal n. 56 of 13 July 1991, amended in State Journal n. 85 of 26 September 2003; Law for the Protection of Personal Data, in State Journal n. 1 of 4 January 2002; Law on Telecommunications, in State Journal n. 88 of 7 October 2003; Law for the Electronic Document and Electronic Signature, in State Journal n. 34 of 6 April 2001, amended on 29 December 2001

Colombia: Constitution, articles 15 and 20; Telecommunication Decree n. 1900 of 1990; Resolution n. 575 of 7 December 2002

Croatia: Constitution, art. 37; Law on the Protection of Personal Data

Czech Republic: Constitution, art. 3, available at http://www.psp.cz/cgi-bin/eng/docs/laws/constitution.html; Charter of Fundamental Rights and Freedoms, available at http://www.psp.cz/cgi-bin/eng/docs/laws/charter.html; Act 101 of 4 April 2000 on the Protection of Personal Data and on Amendment of Some Related Acts, available at http://www.uoou.cz/eng/101_2000.php3

Denmark: Constitution; Act on Processing of Personal Data n. 429 of 31 May 2000; Access to Public Administration Files Act n. 572 of 19 December 1985; Financial Business Act n. 453 of 10 June 2003

Dominican Republic: Constitution, art. 8; General Telecommunication Law n. 153 of 27 May 1998

Egypt: Constitution

Estonia: Constitution, available at http://www.president.ee/eng/ametitegevus/;

Personal Data Protection Act of 12 June 1996, published in State Journal I 1996, 48, 994, available at

http://www.esis.ee/ist2004/103.html

http://www.esis.ee/legislation/protection.pdf

Finland: Constitution, section 10, available at http://www.om.fi/21910.htm; Personal Data Act n. 523 of 1999; Act on the Protection of Privacy in Working Life, n. 477 of 2001; Act on the Protection of Privacy and Data Security in Telecommunications n. 565 of 1999

Guatemala: Constitution, articles 19, 22, 25 and 28

Italy: Constitution, articles 2, 14 and 15; Personal Data Protection Code, Legislative Decree n. 196 of 30 June 2003

Jordan: Constitution, articles 7, 10 and 18; Statistic Law n. 8 of 2003; Criminal Law n. 16 of 1960; Labour Law n. 8 of 1996; Telecommunication law n. 13 of 1995

Latvia: Constitution, art. 96, Personal Data Protection Law of 23 March 2000, available at http://www.dvi.gov.lv

Lebanon: No laws provided

Lithuania: Constitution, articles 22 and 25; Law on Legal Protection of Personal Data n. IX-1296 of 21 January 2003, available at

http://www3.lrs.lt/cgi-bin/preps2?Condition2=208886&Condition2

Malta: Constitution, art. 32, available at http://www.gov.mt/frame.asp?l=2&url=http://justice.gov.mt/; Data Protection Act n. XXVI of 2001

Mexico: Constitution, articles 7 and 16; Federal Law of Transparency and Access to

Public Governmental Information, published in the Official Journal on 11 June 2002, available at http://www.ifai.org.mx/transparencia/LFTAIPG.pdf;

and further regulations, available at http://www.ifai.org.mx

Monaco: Constitution, art. 22; Law on the Treatment of Nominal Information n. 1.165 of 23 December 1993 and its Regulatory Decree n. 13.327 of 12 February 1998

Morocco: Constitution, preamble and article 11; Code of Public Freedoms; Criminal Code, as amended by Law n. 07/03; Press Code

Myanmar: No laws provided

Pakistan: Constitution

Panama: Constitution, art. 29; Law n. 24 of 22 May 2002, on Credit Transactions operated by the Electronic Systems, published in the Official Journal n. 24,559 of 24 May 2002; Law n. 68 of 20 November 2003 on the Right to Privacy of Patients; Law n. 9 of 1998 on Banking

Philippines: Constitution; Bank Secrecy Law

Republic of Moldova: Constitution; Law on Access to Information, n. 982-XIV of 11 May 2000, published in the Official Journal nn. 88-90 on 28 July 2000

Romania: Constitution, art. 28; Law n. 676 of 21 November 2001 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector; Law n. 677 of 2001 on Persons' Protection regarding Processing of Personal Data and the Free Movement of those Data

Russian Federation: Constitution, articles 23 and 24; Federal Law on Information, Informatization and the Protection of Information n. 24 of 20 February 1995 as amended by Federal Law n. 15 of 10 January 2003; Federal Law n. 17 of 3 February 1996 on Banks and Banking; Federal Law n. 2124-1 of 27 December 1991 on Mass Media; Federal Law on Health Protection n. 5487-1 of 22 July 1993

Serbia and Montenegro: Constitution, articles 18 and 20

Slovenia: Constitution, art. 38; Personal Data Protection Act n. 8, published in the Official Journal n. 59/99, 57/2001 and 59/2001; Criminal Code, art. 154

Suriname: Constitution, art. 17; Personnel Act n. 195 of 1962 as amended by State Journal n. 77 of 2003 on Confidentiality Duties for Government Officials; Act on the Supervision of the Bank and Credit System n. 63 of 1986

Turkey: Constitution, articles 20, 21 and 22; Law on the Right to Information n. 4982 of 9 October 2003

Ukraine: Constitution, articles 31 and 32; Law on the Protection of Information in Automatized Systems

Uruguay: Constitution, articles 7, 28, 29, 72 and 332; Law on the Press n. 16099 of 3 January 1989; Law on Statistics n. 16616 of 20 October 1994; Decree on Financial Intermediation n. 15.322 of 17 September 1982; Law on Banking n. 16.696 of 30 March 1995; Decree on the Clinical History of Patients of 30 September 2003

Venezuela: Constitution, articles 28, 47, 48, 60 and 143; Law on Messages of Data and Electronic Signatures n. 1204 of 10 February 2001, published in the Official Journal n. 37 of 28 February 2001

Annex II

Websites of data protection authorities and other relevant websites

Australia: http://www.privacy.gov.au/

Austria: http://www.dsk.gv.at/

Belgium http://www.privacy.fgov.be/

Canada: http://www.privcom.gc.ca/

Cyprus: http://www.privireal.org/countries/cyprus.htm

Czech Rpublic: http://www.uoou.cz/

Denmark: http://www.datatilsynet.dk/

Finland: http://www.tietosuoja.fi/

France: http://www.cnil.fr/

Germany: http://www.bfd.bund.de/

Greece: http://www.dpa.gr/

Guernsey: http://www.dpcommission.gov.gg/

Hong Kong (China): http://www.pco.org.hk/

Hungary: http://abiweb.obh.hu/abi/

Iceland: http://www.personuvernd.is/tolvunefnd.nsf/pages/index.html

Ireland: http://www.dataprivacy.ie/

Isle of Man: http://www.gov.im/odps/

Italy: http://www.garanteprivacy.it/garante/navig/jsp/index.jsp

Japan: http://www.soumu.go.jp/english/index.html

Jersey: http://www.dataprotection.gov.je/

Latvia: http://www.dvi.gov.lv/

Liechtenstein: http://www.sds.llv.li/

Lithuania: http://www.ada.lt/

Luxembourg: http://www.cnpd.lu/

Malaysia: http://www.ktkm.gov.my/

Malta: http://www.dataprotection.gov.mt/page.asp?p=1368&l=1

Mexico: http://www.ifai.org.mx/

Netherlands: http://www.cbpweb.nl/

New Zealand: http://www.privacy.org.nz/

Norway: http://www.datatilsynet.no/

Poland: http://www.giodo.gov.pl/

Portugal: http://www.cnpd.pt/

Republic of Korea: http://www.kisa.or.kr/english/

Romania: http://www.avp.ro/

Slovakia: http://www.dataprotection.gov.sk/buxus/generate_page.php3?page_id=1

Spain: https://www.agpd.es/index.php

Sweden: http://www.datainspektionen.se/

Switzerland: http://www.edsb.ch/

Thailand: http://www.oic.thaigov.go.th/eng/engmain.asp

United Kingdom: http://www.informationcommissioner.gov.uk/

United States of America: Federal Trade Commission, not a data protection authority, http://www.ftc.gov/

Council of Europe: http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/

European Union: http://europa.eu.int/comm/internal_market/privacy/index_en.htm

International Chamber of Commerce:

http://www.iccwbo.org/home/statements_rules/menu_rules.asp

References and bibliography

Bennet M (2004a). EU targets offshore data, *IT Week*, 13 April 2004, available at http://www.itweek.co.uk/News/1154327.

Bennet M (2004b). India mulls EU safeguards, vunet.com, 26 February 2004, available at http://www.vnunet.com/print/1153077.

Blume P (2002). *Protection of Informational Privacy*, Copenhagen, DJOF Publishing.

Bygrave L (2002). *Data Protection Law: Approaching its Rationale, Logic and Limits*, Dordrecht, Kluwer.

Cate F H (1998). Privacy in the information age, Washington D. C., Brooking Institution Press.

Clarke R (2001). Introducing PITs and PETs: Technologies affecting privacy. *Privacy Law & Policy Reporter* 181-188, http://www.anu.edu.au/people/Roger.Clarke/DV/PITsPETs.htm.

Hatcher S (2001). Changing the social meaning of privacy in cyberspace. *Harvard Journal of Law and Technology*, 15:149.

Korea Information Security Agency, (KISA), (2002). Korea Personal Information Protection Annual Report, available at http://www.cyberprivacy.or.kr/english/main.html.

Kuner C (2003). *European Data Privacy Law and Online Business*, Oxford University Press.

Litman J (2000). Information Privacy/Information Property, Symposium on Cyberspace and Privacy: A New Legal Paradigm? *Stanford Law Review*, 52 :1283-1313.

Marlin-Bennett R (2004). *Knowledge Power: Intellectual Property, Information and Privacy*, Connecticut, Lynne Rienner Publishers.

Michael J (1994). *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology* (in association with UNESCO), New Hampshire, Dartmouth.

Privacy and Human Rights (2003). Threats to Privacy, available at http://www.privacyinternational.org/survey/phr2003/threats.htm.

Raul A (2001). *Privacy and the Digital State: Balancing Public Information and Personal Privacy*, Dordrecht, Kluwer.

Reidenberg J (2001). E-commerce and transatlantic privacy. *Houston Law Review*, 38: 717-749.

Ribeiro J (2004). India poised to tighten data protection law, 25 June 2004, available at http://www.computerweekly.com/Article130076.htm.

Solove D (2004). *The Digital Person: Technology and Privacy in the Information Age*, New York University Press.

Tang R (2004). A view from Asia: Laying the foundations for a consolidated approach towards privacy to meet the challenges ahead, 4th IAPP Privacy and Data Security Summit and Expo, 19 February 2004, available at http://www.pco.org.hk/english/files/infocentre/speech_20040219.pdf.

UNCTAD (2003). *E-Commerce and Development Report*. United Nations publication. Sales no. UNCTAD/SDTE/ECB/3, New York and Geneva.

Walden I (2003). Data protection. In: *Computer Law* (eds. Reed and Angel), (5th edition), Oxford University Press, pp.417-454.

Walker K (2002). The costs of privacy. *Harvard Journal of Law and Public Policy*, 25 (3): 87.

Notes

1. Privacy and Human Rights (2003). See http://www.privacyinternational.org/survey/phr2003/threats.htm.
2. See Article 29 Data Protection Working Party Opinion 2/2004, "on the adequate protection of personal data contained in the PNR of air passengers to be transferred to the United States' Bureau of Customs and Border Protection (US CBP)" (10019/04/EN), available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp87_en.pdf.
   For an update on the situation see http://www.eurunion.org/news/press/2004/20040079.htm.
3. See www.commonwealth.org.
4. Article XIV(c)(ii).
5. UK White Paper, "Computers and Privacy" (Cmnd 6353), 1975, at 6.
6. In many laws, an individual to whom data relate is generally referred to as the "data subject". "Individual" and "data subject" are used interchangeably.
7. See Bygrave L (2002).
8. One may think of a recent form of unsolicited contact, used as marketing technique, which directly affects individuals' privacy –namely, spam.
9. Clarke R (2001).
10. "Your best defense against big brother, you", *Wall Street Journal*, 24 January 2000.
11. New e-government study finds ease, engagement, privacy and protection are top priorities, available at http://www.accenture.com/xd/xd.asp?it=enweb&xd=_dyn\dynamicpressrelease_602.xml.
12. The question of the protection of databases, which has traditionally received separate consideration by legislators, is outside the scope of this chapter.
13. In many laws, the entity processing personal data is referred to as a "data controller", "data user" or "data processor". These terms are used interchangeably.
14. General Assembly Resolution A/RES/45/95, 14 December 1990.
15. See subsection: D. 1 below.
16. I.e. binding if contained in an international treaty, and soft law with the value of a mere recommendation if contained in a General Assembly resolution.
17. For an application of the principle see the 2002 annual report prepared by the Korean Information Security Agency (KISA) on the state of personal information in the country: the mother of an elementary school student lodged a complaint because one of the websites she was using for her children's education required parents to provide excessive information on the children as part of the mandatory information, (Korea Information Security Agency, 2002, p. 45).
18. A classic example is a travel agent that communicates certain personal data of their client to make and confirm an airline or hotel reservation for that client. If data are to be used or communicated for a different purpose, the individual must be notified and such use must be lawful.
19. To give an example of a possible violation of this principle, one could imagine an organization keeping a list of undischarged bankrupts that does not seek information on persons discharging themselves from bankruptcy. See Walden (2003).
20. Available at http://www1.oecd.org/publications/e-book/9302011E.PDF.
21. Available at http://conventions.coe.int/treaty/en/Treaties/Html/108.htm.
22. General Assembly Resolution A/RES/45/95. Already in 1989 the General Assembly had adopted some draft guidelines (General Assembly Resolution A/RES/44/132, 15 December 1989), which were then submitted to

the Special Rapporteur of the Commission on Human Rights, Mr. Louis Joined, for a new version which incorporated the comments received by States and by other organizations.

23 Published in the *Official Journal*, L 281, 31.11.1995, available in 11 different languages at: http://europa.eu.int/comm/internal_market/en/dataprot/law/index.htm.

24. See www.protecciondedatos.com.ar/resolucionspam.htm.

25. The Singapore National Trust Council is aiming to have all TrustSg merchants full comply with the guidelines of the code by the end of 2004. See http://www.trustsg.org.sg.

26. See subsection E. 4 below.

27. See, for example, Commission Decision of 30/06/2003 on the adequate protection of personal data in Argentina (OJ L 168, 5.7.2003).

28. The Council of Europe model terms are available at http://www.coe.int/T/E/Legal_affairs/Legal_co-operation/Data_protection/Documents/Publications/1ModelContract.asp#TopOfPage. The European Union model terms are available at http://europa.eu.int/comm/internal_market/privacy/modelcontracts_en.htm.

29. "Model clauses for use in contracts involving transborder data flows", available at http://www.iccwbo.org/home/statements_rules/rules/1998/

30. An example of a safe harbour arrangement is the agreement between the United States and the EU, which is available at http://www.export.gov/safeharbor.

31. See the introduction to this chapter.

32. See the online article of the Privacy Commissioner of Canada, Ms. Jennifer Stoddart, explaining the reasons for the adoption of the Personal Information Protection and Electronic Documents Act, (PIPEDA), available at http://www.privcom.gc.ca/speech/2004/vs/vs_sp-d_040331_e.asp.

33. See the concerns expressed by the the co-chair of the security subcommitteee of the Philippine Information Technology and Electronic Commerce Council (ITECC), Mr. Dela Cruz, available at http://itmatters.com.ph/news/news_04162003c.html.

34. Available at http://www.ktkm.gov.my/.

35. In South Africa, for example, privacy issues are considered by the Human Rights Commission, while in Thailand the Office of the Official Information Commission has responsibility for all aspects of public sector use of, and access to, information.

36. See, for instance, the case of Pakistan: one of the stated functions of the Licensing Enforcement Directorate in the Telecommunications Authority is to "protect consumer rights and ensure privacy of the customers". See http://www.pta.gov.pk/ledirectorate/what.htm.