Comparison of Privacy and Trust Policies in the Area of Electronic Communications : final report

de Villenfagne, Florence; Dumortier, Franck; Poullet, Yves

Publication date:
2007

Document Version
Publisher's PDF, also known as Version of record

wik-Consult/RAND Europe

CLIP/CRID/GLOCOM

Comparison of Privacy and Trust Policies in the Area of Electronic Communications

Final Report

Authors:
wik-Consult: J. Scott Marcus, Kenneth Carter
RAND Europe: Neil Robinson, Lisa Klautzer, Chris Marsden
CLIP: Joel Reidenberg, Camilla Abder, Cedric Burton, Lisa Cooms, Ezra Kover
CRID: Yves Poullet, Florence De Villenfagne, Franck Dumortier
GLOCOM: Adam Peake, Keisuke Kamimura, Tazuko Tanaka

wik-Consult GmbH
Rhoendorfer Str. 68
53604 Bad Honnef
Germany

RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom

Bad Honnef, 20 July 2007

Contents

Executive Summary

This Executive Summary provides an overview of the results of a comprehensive comparative study of arrangements that seek to support privacy and trust in electronic communications in a number of advanced countries: the United States, Japan, South Korea, Malaysia, and India. The European Commission selected these specific countries due to the fast paced nature of technological and regulatory change observed in their respective countries. The study sought to identify effective practices developed elsewhere that might be appropriate for policy makers to consider implementing for the European Union.

The objectives of the study were to compare what systems are present in each country to protect privacy and enhance trust in the realm of electronic communications. Additionally, the study reports on the effectiveness of these arrangements and the perceptions of various stakeholders of these different systems. This report thus does not claim to assert the superiority of any one approach, rather it seeks to identify the lessons that European policymakers might draw from the particular mechanisms in place in each country.

Understanding arrangements that seek to protect the privacy of individuals is exceedingly complex. Privacy protection often develops in a piecemeal fashion, not necessarily as part of a considered plan to provide for privacy and enhance trust. Arrangements within a given country have to be understood in a holistic fashion. Legal arrangements often interact with self-regulatory and co-regulatory[1] schemes in complex ways. Individual rights might be enforced by a government Data Protection Authority or equivalent, by the individual (e.g. through private suit), or by industry self-regulatory and co-regulatory arrangements. There is no single benchmark approach to the measurement of effectiveness in this realm: the effectiveness of privacy and trust arrangements can only be viewed in the context of what works best for each country, based on specific economic, social and cultural conditions. The effectiveness of these arrangements, when compared between countries or even within a single country, can be highly diverse.

This Executive Summary begins by explaining the methodology and terms. The situation in the European Union is then presented for the purposes of comparison, and the Executive Summary then describes in turn the arrangements that we identified in the United States, Japan, South Korea, Malaysia, and India. In each case, we consider (1) legal and regulatory arrangements, (2) other arrangements, (3) enforcement powers, and (4) effectiveness, in that order. This represents a „vertical" view within the context of a single system. With that background established, we go on to compare the systems, thus providing a „horizontal" view across systems; however, we do not attempt to

1 In a co-regulatory scheme, some law typically sets out a framework and objectives, but then devolves implementation to industry.

compare the effectiveness of a particular regime against some common standard. Based on our assessments of privacy and trust arrangements within each country, and our comparisons between the countries, we seek to draw conclusions on the effectiveness of each country's approach to privacy and to provide recommendations relevant to European policymakers regarding the implementation of those privacy and trust measures found to be effective elsewhere.

Methodology

WIK-Consult GmbH led a study team comprising RAND Europe; CLIP (Fordham University); CRID (Université de Namur); and GLOCOM (International University of Japan). WIK-Consult GmbH organized the data collection process. RAND Europe provided country analysis of the United States and India, and contributed network and information security expertise. CLIP (Fordham University) provided legal and regulatory expertise for the United States. CRID (Université de Namur) provided legal and regulatory expertise for Europe, and provided analysis of European arrangements. GLOCOM (International University of Japan) provided country analysis of Japan, Malaysia, and South Korea.

Following the development of a questionnaire, an extensive series of in-depth interviews were conducted by : Neil Robinson, Chris Marsden, Adam Peake and Keisuke Kamimura with representatives of the following types of stakeholder:

- Electronic Communication Service Providers
- Electronic Communication Network Providers
- Other market players (e.g. companies operating in market for privacy enhancing services)
- Lawyers and legal experts
- Government authorities
- Consumer advocacy groups

Semi-structured interviews were used as the principal research technique due to their suitability for discovering perceptions and views of stakeholders about the effectiveness of the arrangements under examination. This data could then be compared against what the various legal, regulatory and non-regulatory instruments are supposed to do, to provide an appreciation of the degree of effectiveness and contrast the reality against the perceptions of stakeholders.

The report includes comparison matrices among the countries that we studied, and also a detailed summary of the interview results.

Detailed citations for the assertions in this Executive Summary appear in the full report.

Europe

At the *regulatory level*, privacy and trust as regards electronic communications in Europe is mainly ensured by Directive 95/46/EC and Directive 2002/58/EC. These Directives rest in turn on the general bedrock of the Charter of Fundamental Rights of the European Union (Articles 7 and 8), the ECHR (Article 8), and the Council of Europe Convention number 108. It is worth noting that the ”right to respect for [one’s] private and family life, home and communications” and the „right to the protection of personal data” are viewed as fundamental and universal human rights. Comprehensive data protection legislation has been enacted in different EU countries. This legislation grants specific rights to data subjects, while imposing on the data controllers important limitations as regards data processing. While data protection authorities are playing a larger role in the enforcement of this legislation, it seems that much still remains to be done in order to achieve real awareness of these data protection provisions among both data subjects and data controllers.

In Europe, it is significant to note that the aforementioned legislative texts tend to regard *self-regulation and co-regulation schemes* as an enhancement rather than a substitute (Article 27 of Directive 95/46) means of making data protection legislative requirements more effective and legitimate. In the context of Transborder Data Flows (TBDF), self-regulation might be considered to ensure adequate data protection (see the famous Working Paper number 12 issued by the Article 29 Working Group [July 24, 1998] which has been taken as a reference by the Commission in its Safe Harbour decision [Dec. 2000/520/CE, July 26, 2000] and the opinion of the same Working Group as regards the appropriate guarantees offered by Binding Corporate Rules). This attitude is strictly in line with the European approach on the value of self- and co-regulation in general (see the inter-institutional agreement on „Better Lawmaking” concluded between the EU Parliament, the EU Council of Ministers and the EU Commission of December 16, 2003 (2003/C321/01)). Notwithstanding this positive attitude by EU authorities, self-regulatory systems (such as Online Dispute Resolution [ODR], privacy guidelines, and labelling schemes) remain rare except in a few Member States (notably the UK and the Netherlands).

Finally, *technology* might be considered as a way to enhance privacy protection. The development and adoption of PETS are encouraged by the European Union, and Data Protection Authorities have developed a proactive approach in support of these technologies.

European legal and regulatory arrangements represent a comprehensive framework for privacy and trust, coupled with substantial enforcement capabilities. Self-regulatory and co-regulatory mechanisms in Europe are much less mature at present.

The United States

The U.S. system is a complex and interwoven tapestry. The U.S. is not characterized by the kind of comprehensive privacy protection framework that exists in Europe; nonetheless, U.S. law (both at federal and at state levels) and associated regulations contain a wealth of provisions specific to privacy. These are complemented by various self-regulatory and co-regulatory schemes and measures that organizations can take on their own initiative, some of which reflect the use of technologies and/or of internal codes of conduct. These elements all contribute to the protection of the privacy of communications.

There may be advantages that come with this system, but there are also clear disadvantages. Notably, the fragmentation of the system inevitably means that there are gaps in protection, and also gaps in enforcement. Many of the laws in effect were narrowly targeted responses to specific problems that emerged at some point in time. Each has its own enforcement mechanisms, and not all mechanisms are of equal strength or effectiveness.

One of the significant criticisms levelled against the U.S. approach is that there is only limited opportunity in practice for the individual to directly launch complaints against those responsible for managing personal data transmitted over electronic communication networks. It is often the case that complaints must in effect be undertaken by organizations acting on behalf of the consumer – the Federal Trade Commission (FTC), the Federal Communications Commission (FCC), or one of the very active consumer advocacy groups such as the Electronic Privacy Information Center (EPIC) or the Electronic Frontier Foundation (EFF).

A number of specific laws address attempts by government or by private parties to intercept electronic communications, including ECPA, CALEA, and the Patriot Act. ECPA and the Telecommunications Act of 1996 oblige telecommunications service providers to respect the confidentiality of customer personal data. The CAN-SPAM deals with unsolicited commercial email messages (spam). COPPA seeks to protect personal information provided by persons under 13 years of age. These laws are complemented by a number of sector-specific laws that in part address general issues of privacy (for example, in the health and financial sectors).

COPPA contains interesting aspects of co-regulation. The FTC can recognize trade association guidelines as constituting a safe harbour with respect to the collection of information from children.

Particularly noteworthy are the state laws that require the disclosure of data security breaches that improperly reveal personal data to third parties. Where such laws require notification directly to the individual, they may facilitate the ability of the individual to take appropriate measures (for example, to avert identity theft). These laws probably

serve to reinforce the commercial incentives of service providers to invest appropriately in privacy and security.

The U.S. is also characterized by a number of measures that operate outside of the formal legal process. For example, TRUSTe and BBBOnline are labelling schemes that seek to certify and monitor privacy policies for electronic communications.

There is strong interest in the U.S. in Privacy Enhancing Technologies (PETS), but limited deployment to date. This is seen more as a future trend.

Enforcement is highly diverse. Some specific laws can be enforced only by public authorities (usually the FTC or the FCC), while others are enforced by private actions. Some laws permit both public and private enforcement.

The implications for effectiveness are again complex. Some respondents felt that the fear of government action or of private suit had great deterrent effect; however, one must question this, since in practice enforcement actions are infrequent and fines tend in most cases to be minimal. Similarly, one must question the effectiveness of enforcement by private suit – it appears that few such suits are brought, presumably due to the high costs and the uncertainty of prevailing.

Views on labelling schemes were mixed. Some saw substantial merit; others felt that the labelling schemes merely gave companies an excuse to do as they wished.

Japan

Japan does not explicitly recognize a right to privacy at a constitutional or statutory level; however, a right to „… assurance that one's private life will not be unreasonably disclosed to the public" has been recognized by the courts.

The Act on the Protection of Personal Information was enacted in 2003 as part of a comprehensive set of laws that generally establish fair information principles similar to those in effect in Europe. The Acts set forth only high level principles, but these principles have subsequently been elaborated by a series of cabinet and ministerial orders. As of March 2007, 35 such guidelines had been published in 22 industry sectors.

Unlike Europe, there is no overall Data Protection Authority. Instead, specific cases are dealt with as they occur by the ministry responsible for the corresponding sector. The Cabinet Office takes the lead in coordinating actions at the ministerial level, but there is no central authority that can exercise government-wide enforcement power.

Japanese arrangements embody many aspects of self-regulation and co-regulation. Businesses handling personal information are expected to take the initiative in pursuing the Protection of Personal Information. Industry groups and trade associations can be

designated as „Authorized Personal Information Protection Organizations" in order to promote industry-wide personal information protection.

Japanese industry makes use of labelling schemes including Privacy Mark and TRUSTe. A number of sector-specific labelling schemes are also in use, notably the Japan Accreditation Council for Healthcare Information (JACHI).

The Act on the Protection of Personal Information places primary responsibility on industry, and consequently provides for somewhat limited penalties. The Act requires organisations that hold information on 5,000 or more individuals to appropriately handle the information. Should they fail to do so, they can be required to file a report with the appropriate minister. In more serious cases, the minister may respond with either recommendations or orders.

A problem that has emerged is that some organisations holding personal data have become over-sensitive to the Act. Media stories report that organisations are sometimes reluctant to provide information that is legitimately required, such as census data or information needed to support public safety.[2]

Japan has a strong interest in the APEC Privacy Framework, and discussion of a possible implementation are ongoing; nonetheless, the general sense is that the APEC framework is not yet mature enough to implement.

These relatively new arrangements in Japan appear to be achieving useful results. A public opinion poll conducted by the Cabinet Office in 2006 showed that 80% of respondents were aware of the Act, and generally showed tangible support for the Act on the part of industry and the public.

---

2 See „JR West rejects disclosure of casualties' information to municipal authorities" (11 May, 2005) http://www2.asahi.com/special/ 050425/OSK200505110052.html: These misunderstandings about the law can be serious and in some cased quite distressing. On the morning of 26 April 2005 the derailment of a West Japan Railway Company (JR West) killed 106 passengers and the train driver. Following the accident, the railway company and hospitals receiving the injured both refused to offer the information of casualties to family members for fear they may infringe their privacy and personal information under the misunderstood law. See also „Minutes of the Quality-of-Life Council",http://www5.cao.go.jp/ seikatsu/shingikai/kojin/kojinjyouhouhogobukai-index.html: Although disclosure of personal information in emergencies is considered to be lawful even without prior consent of data subjects, this was not fully understood at that time. As mentioned, other minor cases, such as refusal to answer the national census or to provide information to law enforcement authorities have also been reported at the Committee on the Protection of Personal Information of the Quality-of-Life Council.

South Korea

The South Korean constitution explicitly recognizes a right to privacy. Nonetheless, given South Korea's unique circumstances, national security concerns loom large and sometimes take precedence over privacy concerns.

The Act on Promotion of Information and Communications Network Utilization and Information Protection (which came into effect in 2001) is the principle law relevant to privacy in electronic communications in the private sector. It is based on the eight core principles of the 1980 OECD privacy guidelines. As with most South Korean laws related to privacy, it also incorporates many aspects of industrial policy. It is administered by the Korea Information Security Agency (KISA), an agency of the Ministry of Information and Communications (MIC); however, KISA does not have full powers of investigation or enforcement. The Act represents a fairly comprehensive privacy framework for electronic communications; however, it is not applied to all sectors. The Act includes both public enforcement provisions, and a private right to action whereby an aggrieved individual can seek compensation.

Several laws deal with equivalent issues on the part of government, and also with lawful intercept (wiretaps).

Other laws and guidelines deal with more specialized issues, including consumer protection and RFIDs. The Protection of Location Information Act (2005) provides for penalties for the misuse of subscriber location information by private companies.

Moving beyond the sphere of law and regulation, the Korea Association of Information and Telecommunication (KAIT) offers two trustmarks: „i-Safe" for security and „e-Privacy" for privacy. There has been only limited take-up of these trustmarks to date, possibly reflecting limited promotion of the program.

Enforcement capabilities of Korean laws and regulations are in theory quite considerable, but it appears that they are not enforced to the limit.

A number of survey respondents felt that Korea's National Resident Registration Number is emerging as a major privacy concern in its own right. The number encapsulates many personal aspects itself (including date of birth and place of birth), but beyond that it is used for a wide range of transactions.

Malaysia

A right to privacy is not explicitly recognized in the Constitution of Malaysia. The courts have not recognized a right to privacy – in fact, in a 2001 ruling, a civil court found that a right to privacy was not even enforceable under common law, because British law at the

time of Malaysian independence (1957) had not recognized infringement of privacy as a tort.

Taken as a whole, then, privacy does not appear to enjoy strong legal protection in Malaysia. The limited laws that exist tend to address privacy concerns as an aspect of information and data security, rather than a fundamental right of the individual.

Since 1998, efforts to introduce a comprehensive Data Protection Act have been ongoing, but the Act has been stalled since 2002.

Pursuant to the Communications and Multimedia Act of 1998, all providers of publicly available ECN participate in the Communications and Multimedia Consumer Forum. The Forum developed a General Consumer Code of Practice that embodies a number of fair information practices. In principle, this could represent an important co-regulatory mechanism in support of privacy; however, in practice, the Code appears to be ineffective. The guiding principles „which could be adopted" seem to be stated in such general terms as to be effectively unenforceable.

In principle, public authorities have strong enforcement powers; however, in practice, the codes promoted by the Multimedia Act do not seem to be monitored for compliance or enforced.

India

Interest in privacy is strong among firms that provide Business Process Out-Sourcing (BPO) for foreign firms, especially for European firms. Interest is much weaker as regards the privacy rights of Indian consumers.

The Indian constitution does not explicitly recognize a right to privacy; however, the Indian Supreme Court has recognized a significant (but not unbounded) right to privacy. Nonetheless, explicit legal recognition of consumer privacy is minimal. No explicit data protection law exists at the national level, although a number of other provisions are tangentially relevant, including the Information Technology Act of 2000, and the various licensing and regulatory provisions relevant to ISPs. A number of states are considering proposed data protection laws at the state level, including Kerala and Andhra Pradesh; however, it is unclear whether these initiatives will have traction at the national level.

Privacy rights on behalf of BPO arrangements are maintained primarily as a matter of private contract, rather than through national legislation. Taken as a whole, India can consequently be viewed as a privacy *rule-taker* rather than a *rule-maker* as regards Europe and the U.S.

Comparisons

There are many dimensions on which the countries and systems studied can and should be compared. Once again, we consider (1) legal and regulatory arrangements, (2) other arrangements, (3) enforcement powers, and (4) effectiveness, in that order.

- **Legal and regulatory arrangements**: An explicit constitutional right to privacy exists in Korea, effectively exists in Europe, and by judicial interpretation exists in the United States and India. Europe and Japan have comprehensive laws, and South Korea has two moderately comprehensive laws covering public and private organisations; the other countries studied lack comprehensive laws protecting individual privacy. Countries that lack comprehensive data protection laws may nonetheless offer substantial protection of specific aspects of privacy; however, there may be gaps or asymmetries in the quality of privacy protection. All of the countries studied impose somewhat distinctive obligations on providers of publicly available ECSs and ECNs.
- **Measures other than law and regulation**: In Japan, South Korea, and Malaysia, there are elements of co-regulation driven in the first instance by legislation. Self-regulatory schemes in the U.S. and India tend to be more market driven. Privacy labelling schemes are promising, and appear in a number of the countries studied – most notably TRUSTe in the U.S. and Japan. Codes of Conduct play an important role in the U.S., and also for Business Process Out-sourcing (BPO) firms in India. A number of the countries studied place greater reliance on self-regulation and co-regulation than does Europe in general.
- **Enforcement**: Public enforcement powers are quite varied across the countries studied. In the U.S., the FTC has some direct and indirect enforcement powers, which however are not necessarily used to full effect. The FCC has enforcement powers against ECSPs and ECNPs. In Japan, power resides primarily with the minister responsible for the commercial sector in question. None of the countries studied could be said to have a fully empowered Data Protection Authority. Where privacy is enforced primarily by contract, as between BPO providers and their clients and India, contract law provides for effective enforcement. Private litigation could potentially serve as a useful alternative to enforcement by government for consumer privacy as well; however, there are significant challenges to doing so in each of the countries studied.
- **Effectiveness**: It is perhaps most difficult to compare the countries in terms of effectiveness. It is clear that comprehensive data protection legislation contributes to uniform and comprehensible protection of privacy; nonetheless, even the most fragmented systems had strengths in specific targeted areas. A number of the self-regulatory and co-regulatory arrangements in the countries studied are working well, and potentially offer useful lessons to Europe. Contractual law is another way to achieve effectiveness, and appears to be robust in India, serving as a reputational signalling mechanism.

Recommendations and observations

We have made a number of suggestions and observations to the European Commission as regards the establishment and enforcement of privacy rights. Inasmuch as our study was focused on the target countries, and not on Europe, our recommendations must necessarily be tentative. We have not attempted an impact assessment on specific initiatives. At the same time, our study of the target countries provides insight into mechanisms that seem to be effective elsewhere and that potentially could serve well here in Europe.

Our key findings are:

- **Legal protection of privacy**: The country studies represent a wide spectrum of approaches to the legal protection of privacy. There is not a single right way to achieve privacy protection. At the same time, it does appear that systems that enact comprehensive data protection laws (as is the case in Europe and in Japan) can potentially achieve more consistent and coherent privacy protection.

- **Self-regulatory and co-regulatory arrangements**: A number of the countries studied make effective use of co-regulatory and self-regulatory arrangements. Particularly instructive is the use of COPPA in the U.S., where the FTC can designate industry association guidelines as providing safe harbour to firms that collect personal data from children.

- **Trustmarks**: The use of trustmarks such as TRUSTe and BBBOnline in the U.S. and in Japan is a relatively unintrusive approach that could potentially have value in Europe. This approach merits further study in order to explore the incentives for the development of satisfactory guidelines and deployment.

- **Enforcement and deterrence**: Penalties for taking insufficient care with personal data must be sufficient to motivate proper behaviour.

- **Breach notification**: Many U.S. states require notification to authorities or to impacted individuals whenever personal information is inappropriately disclosed to third parties. The Commission has already expressed an interest in imposing such an obligation as part of the 2006 review of the European Regulatory Framework. Experience in the U.S. and in Japan generally suggests that this is a viable and productive way to motivate service providers to take greater care with personal data.

- **PETS**: Privacy Enhancing Technologies are a promising approach whose time has not yet come – but that time is approaching. Further study of PETS in Europe would appear to be appropriate

- **Liberty versus security**: Many of the countries that we studied are struggling to find the right balance between privacy and national security in a world where concerns with terrorism have been greatly heightened. There is no obvious right answer, but there is a clear danger of sacrificing privacy to a greater degree than is warranted.

- **Privacy Rights and Development Policy**: The approach of each country to privacy issues reflects the orientation of the legal and political system in that country. It also reflects the availability of resources to implement data protection – developing countries may have more important immediate domestic concerns. This does not necessarily have immediate policy implications for Europe, but implies that policymakers should interpret the needs of their constituents with these factors in mind, and should be cautious in applying lessons from other countries to Europe.

1 Introduction

This report is pursuant to a study for the European Commission: *A Comparison of Privacy and Trust Policies in Electronic Communications*, with specific reference to privacy and trust practices in the United States, Japan, Korea, Malaysia, and India. The European Commission chose these particular countries because they felt that each had experienced rapid technological and regulatory change. We have attempted to describe the main features, advantages and disadvantages of these approaches in terms of the objectives that the European Commission strives to achieve for electronic communications in Europe, including competition, the development of the internal market, and consumer rights and interests.[3]

Our country by country analysis concentrates on four key aspects of these privacy and trust practices:

- Legal and regulatory measures to enhance privacy and trust
- Other measures to enhance privacy and trust, including self-regulatory and co-regulatory arrangements, privacy-enhancing technologies, and standards
- Enforcement powers
- Effectiveness

In order to put these privacy and trust practices in proper context, we are also providing comparative background on corresponding aspects of the European system. Our intent is to enable a meaningful *comparison* of privacy and trust practices in these countries to corresponding practices in Europe, but not to necessarily provide a detailed *analysis* of European practices at the same level as those of the target countries.

The study team sees potential value in learning from best practices in other parts of the world, and in selectively borrowing and incorporating promising ideas where they are compatible with European values and where they promise a suitably favourable relationship of benefits to costs

The next section of this Introduction, Section 1.1, provides definitions, and presents the scope and the research methodology of the study. Section 1.2 provides our preliminary observations on privacy and trust practices in the countries that we studied.

As for the overall structure of the report, Chapters 2, 3, 4, 5, 6, and 7 provide detailed analysis of privacy and trust practices in Europe, the United States, Japan, Korea, Malaysia, and India, respectively. Each of these chapters consists of a discussion of (1) legal and regulatory measures, (2) self-regulatory, co-regulatory and technical ar-

---

3 Cf. Framework Directive, Article 8, including Article 8(4)(c).

rangements, (3) enforcement, and (4) effectiveness. Chapter 8 compares the countries that we studied. Chapter 9 considers a number of cross-cutting issues that are present in varying degrees in most or all of the countries that we studied – the relative merits of regulation, self-regulation, and co-regulation, and the value of a comprehensive legal framework for data protection. Chapter 10 provides recommendations and concluding observations. Annexes provide summary comparisons among the countries studied, a more detailed comparison table for each country, and a glossary. Additionally an accompanying volume contains the responses from the semi-structured interviews where the respondent permitted them to be referenced.

1.1 Definitions, scope and research methodology

Section 1.1.1 provides working definitions of terms that are used throughout the report, and reflected in the Glossary. In characterizing different systems that seek to maintain privacy and trust, and in organizing this report, we make constant use of these terms. Section 1.1.2 discusses the scope of the study, while Section 1.1.3 reviews the research methodology used for this report.

1.1.1 Definitions

In the context of this report, we define privacy as „the right of the individual to determine his own destiny without hindrance, especially from government" (or „the right of the individual to information self-determination"[4]). We define trust as: „reliance on the integrity, strength, ability, surety, of a person or thing; confidence."

There are a variety of instruments that can provide, enhance or protect privacy. In our study we categorized these into legal and regulatory measures (stretching from the constitutional enshrinement of privacy to laws and statutes), and arrangements other than law and mechanisms combined with law. These latter arrangements and mechanisms include measures such as self-and co-regulatory instruments, Privacy Enhancing Technologies (PETs) and standards. Effective protection of privacy is, however, not simply restricted to the mere existence of such instruments but must take into account what means exist to enforce adherence to the law or what can promote the adherence to other arrangements. Put simply, regardless of the extent of the law or other regulatory or non-regulatory means, they cannot be effective if not enforced.

Consequently, in the context of legal and regulatory measures, researchers have to look at what enforcement measures are established including those performed by public authorities, and those empowering the individual to pursue private litigation. For other

4 See Spiros Simitis, Reviewing Privacy in an Information Society, 135 Univ. of Penn. L. Rev. 707, at 734-35 (1987) ; Alan Westin, Privacy and Freedom, at xiii (1967).

arrangements there is a need to look at the effective uptake or the mechanisms by which these are integrated into business practices e.g. the cost benefit of such models, the monitoring of such mechanisms and sanctions available (e.g. revocation of a privacy seal).

Self- and co-regulatory measures

Self-regulatory measures are instruments that are not enforced by statute, but are voluntarily adhered to. Co-regulatory measures involve some blend of government involvement and voluntary compliance. Point 22 of the joint European Parliament, European Council of Ministers and European Commission 2003 Inter-institutional agreement on Better Law-making[5] defines self-regulation as „the possibility for economic operators, the social partners, non-governmental organisation or associations to adopt amongst themselves common guidelines…(particularly codes of practice or sectoral agreements)." The same document defines co-regulation in Point 18 as „the attainment of the objectives defined by the legislative authority to parties which are recognized in the field (such as economic operators, the social partners, non governmental organisations, or associations)."

Self regulatory measures can include privacy commitments, codes of conduct, guidelines, privacy seals (such as TRUSTe or BBBOnLine), or Inter Company Agreements based on standard contractual clauses of the International Chamber of Commerce (ICC). These measures may be introduced via a SRO (self-regulatory organisation) or adopted by a single company.

The U.S. Children's Online Privacy Protection Act (COPPA) represents a good example of co-regulation. COPPA devolves the mechanism for attaining objectives laid out in the legislation to those governed by the Act, but still subject to approval by the U.S. FTC.

Technical and organisational measures

In the context of technical and organisational measures, a range of instruments can support data protection. In particular, this category includes PETs (Privacy Enhancing Technologies) such as web anonymisers, re-mailers, and disk encryption, but also privacy-management protocols such as the World Wide Web Consortium's (W3C) P3P (Platform for Privacy Preferences). PETs are a relatively new approach to the protection of personal data. They seek to empower end-users to protect their own personal data via technologies such as the masking, removal or obfuscation of electronic identifiers used on the Internet. These measures do not often address the actual treatment of personal information once acquired by another party. Additionally, technological measures to provide for the security of personal data (for example, firewalls and cryptography) can support the protection of personal data.

---

5 *Inter-institutional Agreement on Better Law-making* of 16 December 2003, 0J 31.12.2003, 2003/C 321/01

Standards

We treat standards separately from self-regulation, although they are closely linked. The most popular standard of this type is the ISO 27001: *Best Practice for an Information Security Management* standard. Although not strictly standards, other important measures include the *Control Objectives for Information Technology (COBIT*) guidance on IT management, and the *Information Technology Infrastructure Library (ITIL*) Information Security Management best practice. Such standards require organisations to take certain measures to secure personal data, and may be used to help meet responsibilities associated with providing for the security of personal data as described in the 1995 *Directive on Data Protection*. Compliance or accreditation to such standards is often combined with formalised auditing processes in order to monitor long-term compliance.

Evaluating effectiveness

Evaluating the data protection of a country is a challenging task. We did not resort to categorising measures to enhance privacy and trust in one country as „good" or „bad", but rather looked at effectiveness in the context of the country in question. Recent literature[6] suggests looking at the following aspects when evaluating the law:

- scope of the law (in particular whether it regulates both, private and public sector or not; clarity and consistency of the law;
- scope of the law's exemptions;
- remedies and sanctions provided by law;
- kind of enforcement machinery that it establishes;
- extent to which the law is able to cover circumstances brought about by future technological change.

These are useful criteria for evaluating the legal landscape. However, as noted, privacy is not only provided by law and the enforcement of the law, but can also highly depend on other arrangements such as self-regulatory instruments, the use of PETs compliance and certification to standards etc. Therefore, in order to properly evaluate the entirety of a country's approach to privacy, we also took into account criteria relevant to the self-regulatory and co-regulatory environment. Such criteria (besides of course a strong and unambiguous law, and an effective data protection authority) have been characterised as follows:

---

6 Bennett, C. J., Raab, C. D. (2006) The governance of privacy, Cambridge, Massachusetts: The MIT Press, pages 254-255.

- strong commitment by data controllers (those using personal data),
- market incentives driving self-regulatory pro-privacy initiatives,
- vigilant, concerned, and activist citizenry,
- and the application of privacy enhancing technologies.[7]

1.1.2 Scope

This study addresses privacy and trust in the realm of 'e-Communications'. As such, the report focuses on the mechanisms to enhance privacy and trust for personal information handled in the context of communications and does not explore the privacy frameworks that might apply to the processing of personal data according to the content of the data handled for communications purposes. In conducting the study, we had to decide how to deal with a number of issues that were only tangentially relevant. For example, privacy and security concerns regarding electronic databases held by private firms or by government agencies (which use data transmitted across electronic communication networks) were not squarely in the scope of this study; electronic communications were involved, but electronic communications privacy mechanisms were not central to the data protection issues. To the extent that these non-communications privacy mechanisms shed useful light on privacy arrangements for electronic communications in the target countries, the study references them; however, in order to keep the size and complexity of the study manageable, we did not attempt to provide an in-depth analysis.

Although the monitoring of communications for law enforcement or national security concerns is clearly of importance to electronic communications privacy and trust, we did not explore government surveillance because it is an EU '1st pillar' responsibility (i.e. exclusively a matter of national sovereignty). Inasmuch as government surveillance is a matter of national rather than European competence, it is not of direct relevance to the European Commission.

As has already been highlighted, the European Commission selected the countries covered in this report because they were felt to be undergoing significant technological and regulatory change.

For those countries with a federal government system (e.g. the United States and India) the report describes arrangements at the federal level, and highlights measures of particular relevance or interest where they have been implemented in specific states. This report does not seek to provide a comprehensive view of privacy measures in each state.

---

7 ibid, p 264.

We provide a brief comparative background on the situation as it exists in Europe in order to put the measures as they exist in Europe into context. It was the intent of the study to provide a meaningful comparison of privacy and trust practices across the selected countries and reference them to corresponding practices in Europe. The study does not necessarily provide a detailed analysis of European practices to the same degree of those of the target countries.

1.1.3 Research Methodology

The study consisted of substantial desk research, augmented by more than forty in-depth interviews with experts representing electronic communication service providers (ECSP), electronic communication network providers (ECNP), other market players, legal experts, government, data protection authorities, and consumer advocacy groups.

WIK-Consult GmbH led the consulting team and organized the data collection process. RAND Europe provided country analysis of the United States and India, and contributed network and information security expertise. CLIP (Fordham University) provided legal and regulatory expertise for the United States. CRID (Université de Namur) provided legal and regulatory expertise for Europe, and provided analysis of European arrangements. GLOCOM (International University of Japan) provided country analysis of Japan, Malaysia, and South Korea.

As a key part of the study, we developed a core questionnaire with questions distinguished according to type of privacy measure. This questionnaire was then adjusted to take into consideration the different perspectives of each stakeholder, and to allow us to triangulate responses per country. This process resulted in six distinct questionnaires, each targeted at a specific kind of stakeholder.

We then transformed the questionnaire into a web-survey and began contacting participants. Given the complexity of the material, in most cases we found it preferable to conduct an interview, often face to face, and then fill in the web-survey on the user's behalf. We invited interviewees to comment on their responses in order to help ensure the accuracy of the information.

In total, by 4th June 2007, we had interviewed 39 respondents. Table 1 indicates the total number of respondents, per country, per stakeholder.

Table 1. Interview respondents per country, per stakeholder

Stakeholder	Total No. of responses					
	US	Japan	S.Korea	Malaysia	India	Total
Market Players	8	1	3	3	3	18
Government Administrations	1	1	1	-	1	6
Data Protection Authorities	n/a	1	1	-	1	3
Lawyers and Legal Experts	1	1	1	1	1	5
Consumer Advocacy Groups	2	1	1	1	2	5
Privacy Service Companies	1	1	-	-	1	3
Total	13	6	7	5	9	40

1.2 Preliminary observations

The countries in question are really quite diverse in their approaches to privacy and trust in electronic communications. By way of comparison, the European Union has viewed privacy as a fundamental right, and this commitment permeates European law and European practices. It is not just that certain intrusive practices are comprehensively banned – beyond that, European Member State governments have a positive obligation to ensure privacy. Beyond this, courts have often recognized the right of the individual to determine his own destiny without hindrance, especially from government. Taken as a whole, this means that Europeans enjoy a high degree of legal protection for their privacy. Most developed countries protect privacy of electronic communications to some degree, but not with the single-mindedness that is found in Europe.

Privacy in the United States has a significantly different character. Many basic civil liberties are enshrined in the United States Constitution, but this venerable document does not specifically address electronic communications. Legal and regulatory protections are a patchwork quilt of sector-specific national laws, state laws, and enforcement powers with various agencies and with the courts. There is no over-arching privacy framework; nonetheless, complex protections exist for the privacy of the individual. Some privacy rights are enforceable only by specific government agencies; some are enforceable only by private litigation; and some are amenable both to public and to private enforcement. Given the nature of the U.S. legal system, the threat of litigation may possibly have a deterrent effect.

In Japan, a comprehensive modern legal framework has been erected in support of privacy in electronic communications. Laws generally consistent with the OECD frame-

work assure the privacy of the individual versus private industry, government, and quasi-governmental corporations. Not all of these laws have explicit enforcement mechanisms; nonetheless, they seem to be reasonably effect in the Japanese context.

The Korean Constitution is explicit in its protection of privacy: „The privacy of no citizen shall be infringed.“, and: „The privacy of correspondence of no citizen shall be infringed.“ However, despite these protections, the historic conflict with the North has put strains on these pronouncements and has led to a society where surveillance by government is not uncommon. Korea is a leading nation in terms of broadband penetration, and this experience with high-speed, always-on networks is leading to some more sophisticated legislation and also to sophisticated problems. Privacy law has effectively been extended such that the Korean courts recognize a „right of publicity“ which allows an individual to control the commercial use of his or her identity.

In India, the Supreme Court has inferred a right to privacy from more general constitutional provisions. These are more readily enforceable against government than against private firms. Even in the absence of an explicit Data Protection Act or a specific Data Protection Authority, fairly substantial protection of consumer privacy is enforceable. Aside from formal mechanisms, the Indian ICT industry tends to be supportive of privacy protection inasmuch as they recognize that respect for privacy is a prerequisite to their success in doing business with the rest of the world, and especially with Europe.

Malaysia has no explicit constitutional right to privacy. In light of Malaysia’s somewhat fragile multicultural relationships, its relatively short history since independence from colonial rule, and its experience with a Communist insurgency, recognition of free speech and of privacy has often been subordinated to national security concerns. For example, Malaysia is a signatory to the Universal Declaration of Human Rights, but restricts its application to those „fundamental liberties provided for“ in the Constitution and to provisions consistent with the Constitution. Against this historical and also cultural background, there is no strong tradition of concern for privacy and trust in society, and it wasn’t until a national IT strategy was established in the mid-1990s that legislation and regulation relating to privacy and trust in the communications sector began to be considered. These developments flowed from Prime Minster Dr. Mahathir Mohamed’s vision for Malaysia to become a fully developed country by 2020. In 1996, the National IT Council (NITC), chaired by the Prime Minster, recognized that ICT sector would not develop unless there were laws and regulations to prevent the abuse of IT and multimedia technologies. These concerns led to a series of activities in the late 1990s and early part of the next decade to develop a national information security policy framework, enact legislation to protect personal information, and promote the positive use of the Internet; nonetheless, when viewed from the standpoint of personal and civil liberties, privacy still does not enjoy strong protection in Malaysia.

What emerges, then, is a complex tapestry of law, self-regulatory and co-regulatory mechanisms, technology, and enforcement mechanisms. Some of the target countries

recognize an overall positive right to privacy of electronic communications at what is in effect a constitutional level (Europe, India, South Korea, and to some extent the United States), others at a statutory level (Japan), while still others lack an overall recognition of a positive right to privacy (Malaysia). Nonetheless, all of the target countries provide some degree of protection through specific (negative) prohibitions of various acts that would compromise individual privacy in electronic communications. Some of the target countries implement these prohibitions in a relatively comprehensive way, while others tend to use a more piecemeal, sector-specific approach. Some make more use of self-regulatory mechanisms, some less. Some of the target countries place primary reliance on government to enforce the protection of individual privacy in electronic communications, while others (notably the United States) place substantial reliance on private litigation, or the threat of private litigation, to deter behaviour that would impact individual privacy in electronic communications.

2 Review of practices in Europe

This chapter provides background on European practice, primarily to provide a base of comparison for privacy and trust in the target countries. We are not seeking to provide a full assessment of European practice, nor are we specifically collecting stakeholder input about Europe; however, we are summarizing current practice, with which we are familiar based on previous work and current research. To facilitate comparison with the other country-specific sections, the chapter is organized to first discuss law and regulatory aspects, then self-regulatory measures, and then enforcement mechanisms.

At the *regulatory level*, privacy and trust as regards electronic communications in Europe is mainly ensured by Directive 95/46/EC and Directive 2002/58/EC. These Directives rest in turn on the general bedrock of the Charter of Fundamental Rights of the European Union (Articles 7 and 8), the ECHR (Article 8), and the Council of Europe Convention number 108. It is worth noting that the ”right to respect for [one’s] private and family life, home and communications” and the „right to the protection of personal data” are viewed as fundamental and universal human rights. Comprehensive data protection legislation has been enacted in different EU countries. This legislation grants specific rights to data subjects, while imposing on the data controllers important limitations as regards data processing. While data protection authorities are playing a larger role in the enforcement of this legislation, it seems that much still remains to be done in order to achieve real awareness of these data protection provisions among both data subjects and data controllers.

In Europe, it is significant to note that the aforementioned legislative texts tend to regard *self-regulation and co-regulation schemes* as an enhancement rather than a substitute (Article 27 of Directive 95/46) means of making data protection legislative requirements more effective and legitimate. In the context of Transborder Data Flows (TBDF), self-regulation might be considered to ensure adequate data protection (see the famous Working Paper number 12 issued by the Article 29 Working Group [July 24, 1998] which has been taken as a reference by the Commission in its Safe Harbour decision [Dec. 2000/520/CE, July 26, 2000] and the opinion of the same Working Group as regards the appropriate guarantees offered by Binding Corporate Rules). This attitude is strictly in line with the European approach on the value of self- and co-regulation in general (see the inter-institutional agreement on „Better Lawmaking” concluded between the EU Parliament, the EU Council of Ministers and the EU Commission of December 16, 2003 (2003/C321/01)). Notwithstanding this positive attitude by EU authorities, self-regulatory systems (such as ODR, privacy guidelines, labelling schemes) remain rare except in a few Member States (notably the UK and the Netherlands).

Finally, technology might be considered as a way to enhance privacy protection. PETS’s development and adoption are encouraged by the European Union, and Data Protection Authorities have developed a pro-active approach in favour of these technologies.

The security of Information Systems is a fundamental obligation of the Data Controller. Article 16 of the Directive 95/46 requires the Data Controller to provide an appropriate level of security, and is complemented by additional security measures imposed by the Directive 2002/58 as regards electronic communications (particularly Articles 4 and 5). On that point, the work done by the CEN (the European Standardisation Body, which has established an expert group on Privacy and Security and delivered its first technical and organizational norms) is also relevant.

2.1 Legal and regulatory measures to enhance privacy and trust

As previously said, in the EU, the rights to Privacy and to data protection are mainly ensured through regulation. Therefore, this first section aims to explore the various aspects of applicable European legislation taken in order to reach the desired levels of privacy/data protection and trust over secure electronic communications networks and services.

Privacy and trust regulation as regards electronic communications at the European level rests on three primary pillars:

- the *ePrivacy Directive* (2002/58/EC), which is part of the regulatory framework on electronic communications implemented in 2003 ;and
- the *General Data Protection Directive* (95/46/EC), which is supplemented but not superseded by the ePrivacy Directive.
- (the *Data Retention Directive* (2006/24/EC) which will not be discussed in the present report since it has been agreed that it was beyond the scope of the study.

These Directives rest in turn on the general bedrock of the *Charter of Fundamental Rights of the European Union* (Articles 7 and 8), the *ECHR* (Article 8) and the Council of Europe Convention n°108. These general texts will not be analyzed in the present report as they go beyond the scope of the discussion related to „trust and privacy in the context of electronic communications".

In the next sections, we expose the two European Directives (Directive 95/46/EC and Directive 2002/58/EC) more in detail and analyze their input as regards trust on electronic communications networks.

2.1.1 The general Privacy Directive (95/46/EC)

Directive 95/46/EC is the reference text, at European level, on the protection of personal data. It sets up a regulatory framework which seeks to strike a balance between a high level of protection for the privacy of individuals and the free movement of personal

data within the European Union (EU). In 1995, when this regulation was adopted, the Internet was still in the early stages of its deployment. Nevertheless, the Article 29 Working party published multiple recommendations, opinions and working papers in which the group applies the principles of Directive 95/46 in the area of electronic communications and Internet.[8]

In the next sections, we explore the main concepts of Directive 95/46 and apply these to the electronic communications realm.

---

8 In particular:
- Recommendation 2/97: Report and Guidance by the International Working Group on Data Protection in Telecommunications („Budapest - Berlin Memorandum on Data Protection and Privacy on the Internet“)
- Recommendation 3/97: Anonymity on the Internet
- Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)
- Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes
- Recommendation 2/99 on the respect of privacy in the context of interception of telecommunications
- Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware
- Working Document : Processing of Personal Data on the Internet (WP16)
- Working document „Privacy on the Internet“ - An integrated EU Approach to On-line Data Protection (WP37)
- Opinion 7/2000 On the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000
- Opinion 5/2000 on The Use of Public Directories for Reverse or Multi-criteria Searching Services (Reverse Directories)
- Opinion 2/2000 concerning the general review of the telecommunications legal framework
- Opinion 1/2000 on certain data protection aspects of electronic commerce
- Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union
- Working document - First orientations of the Article 29 Working Party concerning on-line authentication services (WP60)
- Opinion 2/2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPV6
- Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites
- Opinion 2/2003 on the application of the data protection principles to the Whois directories
- Opinion 1/2003 on the storage of traffic data for billing purposes
- Working Document on on-line authentication services (WP68)
- Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.
- Opinion 5/2004 on unsolicited communications for marketing purposes under Article 13 of Directive 2002/58/EC
- Opinion 5/2005 on the use of location data with a view to providing value-added services
- Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC
- Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive
- Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC
- Opinion 2/2006 on privacy issues related to the provision of email screening services

Personal data

The Directive applies to data processed by automated means and data contained in or intended to be part of non automated filing systems (traditional paper files). The term „Personal data" is defined as *„any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"* (Art. 2(a)). Hence, to be considered as „personal data", it is not necessary that data identifies as such the data subject. The mere fact that data might be related to an identifiable or identified person is sufficient. To determine whether a person is identifiable, Recital 26 of the Directive specifies that one should consider *„the means likely reasonably to be used either by the controller or by any other person to identify the data subject"*.

The Directive also covers special categories of data which are typically referred to as sensitive data in the national data protection legislation of Member States. The Directive includes the following within its special categories of data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data related to health or sex life. These data are subject to additional restrictions.

Note that in the context of electronic communications, two types of personal data can be distinguished: *content data* (the content of a form, an e-mail, a web-page, a telephone conversation) and *user related data* (the electronic data generated when a user connects/makes use of a electronic communication service or network or connection information such as login or a password). User related data are subject to additional regulation when these constitute „traffic data" or „location data" as defined by Directive 2002/58 (see below).

Processing of personal data

The term „processing of personal data" refers to „any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction". The definition is so broad that virtually all data operations from „cradle" (collection) to „grave" (destruction) are deemed to be processing of personal data in the EU. Note however that the processing of personal data carried out solely for journalistic, artistic or literary expression purposes are exempted from the scope of the Directive if such exemptions are „necessary to reconcile the right to privacy with the rules governing freedom of expression"[9]. The term „use" is not defined in the Directive and may also cover addressing a person through e-mail, telephone, fax or otherwise.

---

9 Article 9 of Directive 95/46/EC

Data controller – data processor

The controller is the „natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data „(Article 2 (d) of Directive 95/46/EC).

A processor is a „natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (Article 2 (e) of Directive 95/46/EC).

Applying these definitions in the context of Internet and electronic communications often is a challenge. Identifying a data controller in an open network, for instance, is difficult. Such a network is characterized by numerous intervening actors, such electronic communication service providers (ECSP) and electronic communication network providers (ECNP).

In such a network, there may be multiple controllers. The traffic data and other user related data generated by the network are controlled by ECSPs and ECNPs as they decide upon the purpose and the means of the processing of these data. As for the information and content providers (like website managers), these should be considered as data controllers with respect to the processed content data (e.g. the user filling in an order form or the collection of personal data through a cookie).

E-mail traffic, for example, may also involve multiple controllers. Recital 47 of the Directive states that where a message containing personal data is transmitted by means of a telecommunication or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be deemed the person from whom the message originates, rather than the person offering the transmission services. Consequently, when an individual uses an e-mail service on the Internet, he should be considered as a controller of the personal data in the e-mail, since he determines the purpose and means of the processing. The Internet Access Provider (IAP) is also controller since it processes certain data such as the web site visited or the address of the POP/SMTP server to which the user connects, the time and duration of the connections ensured through its intermediary. The transmitter will be deemed the controller in respect of the processing of additional personal data necessary for the operation of the service. Finally, once the data is received or intercepted, the receiver or interceptor will become the controller.

In the context of common platform used by multiple companies, the qualification of the platform manager might be difficult insofar the platform might offer only secure communications services like encryption, time stamping without having access to the message itself. In that case, certain doubts have been raised against their qualification as Data controllers.

These examples tend to demonstrate that it is often complex to apply the legal definitions of the Directive 95/46/EC in the context of open networks such as the internet.

Territorial Scope of application

The basic principle as regards the territorial scope of the Directive 95/46 is enacted by its article. 4.1. The Directive is applicable if and only if „*the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*". So, the criterion to determinate the geographical scope of the Directive is the physical link between the activities of the data processor and the EU territory, where the real activities of the data processor effectively are taking place[10]. Thus, only the activities located in Europe are regulated under Directive 95/46, even where data are transmitted to third countries.

Only one exception[11] is foreseen by the Directive: „The Directive is applicable when the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State,…". In those cases, the Data controller located outside of the European Community has the obligation to designate a representative established in the territory of that Member State. This article deals with cases of remote usage of automated processing apart from controllers outside of EU (cookies, spyware, etc.), and intends to impose the obligations of the Directive on processing which is under the total control of Data controllers located outside of Europe. In other words, the criterion to be applied is the functional control of the equipment. The provision refers precisely to cases where a data processor located outside of Europe has or takes full control of the equipment located in Europe and collects data without voluntary authorization or without conscious transmission by the terminal equipment possessor. Cookies or spyware are examples of such remote data collection, but once could also envision applications that permit outsiders to data files without authorization of the data possessors.

Data protection principles

Without entering into details, in order to process personal data in a fair and lawful manner, the controller has to clearly define the purpose of the processing. The controller has also to ensure that the data are adequate, relevant and not excessive in relation to the purpose for which they are collected. The processing must be based on a legitimate ground (unambiguous consent, performance of a contract, compliance with a legal obligation, in pursuance of legitimate interests of the controller etc.) and the individual has the right of access to and the rectification or erasure of his personal data. The individual has at least to be informed about the identity of the controller and his representative if

---

10 Establishment does not mean necessarily where the data processing occurs About the meaning of this criterion and the explanation of this choice by the European Directive, see .L.A.BYGRAEVE, « Determining applicable law pursuant to European Data Protection Legislation », in *E-Commerce Law and practice in Europe,* C.WALDEN and J.HÖRNLE (eds), Woodhead Publishing Limited, Cambridge, 2001, p. 4 and ff. and from the same author, *Data Protection: Approaching its Rationale,Logic and Limits,* Doctoral thesis, Oslo, 1999 published by Kluwer Law international, 2000.

11 See about the Article 4.1 c), the assertion stated by TERSTEGGE : „*This rule leads to some odd extraterritorial side effects*." („Directive95/46/EC, art. 4", in *Concise European IT Law,* (A.BULLESBACH, Y.POULLET and C.PRIENS (eds.)), Kluwer Law Int., 2006, p. 164).

any, the purpose of the processing, the recipients and about his rights and a right to access is granted to him or her with a very few of exceptions.

Another important aspect is the security of the processing which may require the controller, right from the collection on, to apply specific technical and organisational measures in order to protect the data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the data are transmitted over a network. Such measures must ensure a level of security appropriate to the risks presented and the nature of the data.

As regards sensitive data specific provisions, the Directive regulates their processing dealing in with respect to the particular risks linked with the processing of these data.

Finally, transfers of data to third countries – i.e. outside of the EU – are prohibited when those countries are not recognized as providing an adequate level of protection unless particular safeguards (contractual clauses, binding corporate rules) are set up by the controller.

2.1.2 The ePrivacy Directive (2002/58/EC)

In 1999, the European Commission launched a review of the telecommunication regulatory framework. The goals of the review were five-fold: to promote more effective competition; to react to technological and market developments; to remove unnecessary regulation and to simplify associated administrative procedures; to strengthen the internal market; and finally to protect consumers.[12]

One of the results is Directive 2002/58 on privacy and electronic communications[13], which replaces Directive 97/66[14] concerning the processing of personal data and the protection of privacy in the telecommunications sector.

Traditionally, Directive 2002/58 is being seen as a *lex specialis* vis-à-vis Directive 95/46/EC applying and detailing its rules in order to adapt them to new technology[15], mainly to the Internet. Poullet has argued[16] that Directive 2002/58 introduces, in some

---

12 *The 1999 Communications Review*, European Commission, DG INFSO, Directorate A, September 2000

13 Directive 2002/58 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector, 2002, O.J. L201

14 Directive 97/66 of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the telecommunications sector, 1998, O.J. L024/1

15 See A. De Streel, R. Queck, and P. Vernet, „Le nouveau cadre réglementaire européen des réseaux et services de communications électroniques », in Cahiers du droit européen, 2002, N°3-4, 243-314

16 Y. POULLET, « Pour une troisième génération de réglementation des données »,Conférence internationale des commissaires à la protection des données, Colloque de Montreux, 14 et 15 septembre 2005, Jusletter, Nov. 2005, p. 20-24

respects, a rupture with the traditional conception of data protection and paves the way to a third generation of data protection regulation[17] for three main reasons:

1. enlargement as regards the data protected beyond the scope of the Directive 95/46 EC;

2. enlargement as regards the actors regulated which are not necessarily Data Controllers;

3. enlargement by regulating not only the processing but also the terminal equipment.

As regards the first point, the definition of „data" in Directive 2002/58 is not exactly the same as in the Directive of '95. Indeed, the definitions of „Traffic Data" and „Localisation Data" carefully avoid using the concept of „personal data" which is the main concept of Directive 95/46. Article 2 and Recital 14 of Directive 2002/58 define localisation data by the sole reference to the terminal equipment of a user. As for traffic data, Recital 15 describes it as „any naming, numbering or addressing information provided by the sender of a communication or the user of a connection to carry out the communication". Therefore, Poullet argues that traffic and localisation data need not necessarily be personal data since a link to an identified or identifiable data subject is not required. These elements tend to demonstrate that a third generation of data protection regulation is on its way. This new generation of data protection regulation seems to safeguard to the use of data towards individuals, identified or not, identifiable or not. The cookies' example is relevant.

In the next sections, we expose the main concerns of Directive 2002/58.

Services concerned

The Directive applies to *„the processing of personal data in connection with the provision of publicly available electronic communications services[18] in public communications networks in the Community"* (Art. 3(1)). The scope of the Directive thus covers all the processing of personal data in connection with the provision of publicly available electronic communications networks, being not confined to telephony or data networks but also encompassing satellite, terrestrial and cable TV. One of the typical services covered would be the one offered by the Internet access provider.

---

17 The two first generations of data protection regulations being the Article 8 ECHR as interpreted by the case-law and the Directive 95/46/

18 The concept of „electronic communications services" is defined in Article 2(c) of Directive 2002/21 on a common framework for electronic communications networks and services as a „service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks »

On the contrary, all the processing in connection with electronic communications networks which are not available to the public remain excluded, such as for example services limited to closed-user groups or services not accessible through public communication networks, for example through intranet even if these private networks are not limited to closed-user groups like automated teller machines offered in the context of banking services.[19]

Information society services[20] are not completely excluded from the scope of the Directive. For example, the „e-commerce" Directive 2000/31 describes the service provided by different intermediaries („mere conduit", „caching", and „hosting"). „Hosting" consists of „the storage of information provided by a recipient of the service". At the Internet hosting service provider level (which hosts websites, when they are not „self-hosted" through the user-own servers), there is no transmission in a communication network of information or no „conveyance of signals on electronic communications networks". So, „hosting" is excluded from Directive 2002/21. The same reasoning could be applied to the web administrator. Nevertheless, Directive 2002/58 uses a functional approach, and we have to consider other services or activities beyond those that would be „strictly" included in Art.3(1), mentioned both in the text of the instrument as well as in the Explanatory Memorandum. There we find, for instance, reference to „unsolicited communications" or „cookies". Sending unsolicited electronic mail can be done, for instance, by a web-administrator using the data he bas collected. Cookies are placed by web administrators or cyber-marketing companies. So, these activities are covered by the Directive to the extent that is mentioned in the text, irrespective of „who" does so (the question to answer is „what" any specific actor does in order to know if his activities fall under the Directive's regulation).

Territorial scope of application[21]

In the context of recent development of Internet services and the global nature of its infrastructure, it would be nonsense to restrict the European Union protection to the European Borders. To take an example, more than 60 percent of web sites are located in U.S. It is thus crucial to envisage the protection of European Internet users surfing on web sites located in U.S.

---

19 This exclusion has been criticized by the Art. 29 Working Party underlining the fact that the distinction between public and private networks will be increasingly difficult to trace and taking into account the increasing importance of these private networks and the risks associated with their use, for example, the monitoring of the use of internet by employees within a company. Certainly if the services offered by companies to customers through their own private networks are excluded from the application of Directive 2002/58, they remain subject to the principles of Directive 95/46. Those principles require inter alia that the processing will be lawful, the data processed will be relevant and not excessive and the data subjects might exercise their rights to be informed, to access and to rectification.

20 Directive 98/4816 amends Directive 98/34 and defines „information society service:' as „any service normally for remuneration, at a distance, by electronic means and at the individual request of a recipient of services."

21 On this issue, see Yves Poullet, *„Transborder Data Flows and Extraterritoriality : The European Position",* 2006 (to be published)

So, the traffic or location data might be transmitted and processed unlawfully by telecommunications service providers established outside of the EU European Data subjects might be victims of unsolicited mails or by illicit and unfair Data collected through cookies or spyware installed on his hard disk by processors established anywhere throughout the world.

Therefore, provisions of the Directive 2002/58 target all Electronic communications services without taking into account the nationality or the establishment of their providers. In that sense, one might speak clearly about the extraterritoriality of this Directive[22].

Confidentiality of communications

The principle of the confidentiality of communications has been clearly asserted by the European Court of Human Rights (See *Klass* (ECHR), *Malone* (ECHR), etc.) and derives directly from the Article 8 ECHR which clearly asserts the secrecy of correspondence and must be interpreted as being applicable irrespective of the technical means used for the conveyance (postal card, electronic mail, etc.). Thus, this principle forbids, as is the case for a postal card, any interference, any interception or surveillance of electronic correspondence.

Article 5 of Directive 2002/58 recalls this important principle. Within the framework of the Directive, the term „communication" means any information exchanged or conveyed between communications services. The concept is thus very wide and covers any information exchanged (the e-mail message sent or received, the web page visited, etc.) This concept is clearly distinguished from the data identifying the communication (such as the sender, receiver, protocol used) and necessary for the conveyance of the message, that is following the wording used by the European Directive the „Traffic Data" which are also protected by the same principle[23]. This distinction, however, permits more exceptions as regard the obligation of confidentiality for traffic data than for communication.

Traffic data

„Traffic data" is defined as „any data processed for the purpose of the conveyance of a communication on electronic communication networks or for the billing thereof".

---

22 *„Some of the services covered by the Directive might be offered to a subscriber or a use inside the European Union from a provider located outside the Community, for example as Internet access provider, In that case, the text states clearly that the European Directive is applicable. The criterion fixed by the Directive is not the same as the criterion of establishment retained by the General Directive and will thus permit an extraterritorial effect of this Directive."* (Y.POULLET, „Directive 2002/58/EC, art. 4", in *Concise European IT Law,* (A.BULLESBACH, Y.POULLET and C.PRIENS (eds.)), Kluwer Law Int., 2006, p. 164).

23 Art. 5(1) of Directive 2002/58 foresees that interception or surveillance of communications and the related traffic data is prohibited, except when legally required in accordance with Art. 15(1)

Traffic data are those data needed by the protocols to carry out the proper transmission from the sender to the recipient. Traffic data consists partly of information supplied by the sender (e.g. email address of the recipient, URL) and partly of technical information generated automatically during the processing of an electronic communication (e.g. IP address).

Directive 2002/58 foresees that interception or surveillance of communications and the related traffic data is prohibited, except when legally authorised in accordance with Art.15(1).

The principle is that traffic data must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. These obligations are without prejudice to Art. 15(1), as well as Art.6 (2) (billing purposes), Art.6 (3) (marketing of electronic communications services or for the provision of value added services), and Art.6 (5) (customer enquires, fraud detection, and so on).

The concept of „data processed for billing purposes" represents those data that are routinely kept for the unique purpose of billing. On the one hand, in the case of an access using a „pay per call" communication line (modem on an analogue phone line or Terminal Adaptor on a numeric [ISDN] line) the originating telecommunication operator typically needs to collect the date and the time of the communication, its duration, the number called, and of course the calling number of his subscriber. On the other hand, if the subscriber uses a DSL connection, the billing of this kind of Internet access appears to usually be a flat fee with a maximum number of Megabytes of traffic per month. If so, it is no longer necessary to record each connection to the Internet, but it may still be necessary to count the volume of traffic, in which case it will also be necessary to identify the subscriber of the fixed line on which the DSL connection has been activated. Those data are collected by the historical telecommunication operator for billing purposes. In addition, there is the Internet service provider (possibly a different firm) that offers Internet access by providing a unique IP address and the function of routing IP packets on the Internet.

Security

Article 4 of Directive 2002/58 imposes additional security obligation on the provider of publicly available electronic communications services due to the specificity of the risks linked with the use of networks. It reads as follows.

„1. The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

2. In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved."

The concept of „security" is quite broad. It means, under Art. 17(1) of Directive 95/46, protection „against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing". So, for example, the risk of wiretapping by unauthorised third parties during the use of the services requires appropriate safeguards like the use of cryptography or secured lines (e.g. in case of the electronic transmission of credit card numbers). The possibility of intrusion within the provider's information system in order to collect all its customers' addresses or to manipulate certain data imposes the necessity to install firewalls and other security measures. The sending of „worms" through the information systems of a communication service provider or the creation of a mirror site in order to lead astray certain communication are other specific risks linked with the use of communication services. The obligation is not limited to technical measures but encompasses also organizational measures which might be the appointment of a data security manager competent to ensure the compliance of the functioning of the service with all Directive provisions. In order to ensure such security, cooperation with the provider of the network might be desirable. Consequently, the operator of a network might be asked to intervene, if an intrusion is detected, to automatically block any access to the information system of the service provider.

The second sentence of para.1 of Article 4 recalls the criteria developed by Art. 17 of Directive 95/46 to appreciate the level of security to be taken into account by the service provider. Thus, considering the potential risks linked with the nature of the service as regards both the probability of its occurrence and the harm that would result (an electronic communication service in the healthcare sector needs more security measures than a network permitting access to movies), attention will have to be paid both to the state of the art, that is, in particular the standards developed by such standardisation institutes as ISO, and the cost of implementing the security measures. The more significant the risk, the higher the security level that must be achieved considering the cost of the implementing measures.

As regards the kind of measures, emphasis should be placed on the importance of self-regulation in this realm: the development of standards, auditing methods, regimes for the approval of information systems, and so forth (see section 1.3 below)

Finally, recital 20 of Directive 2002/58 recalls the obligation of the electronic communications service provider to adapt continuously the level of security taking into account the evolution of the state of the art.

In addition, the lack of network security and the proliferation of opportunities for illicit actions make it necessary for the providers of electronic communication services to be obligated to issue warnings concerning their use. Paragraph 2 of Article 4 answers this need.

In case of a „particular" security risk (for example, the unexpected appearance of a worm, the discovery of certain failures in the security of its information system or the multiplication of attacks by hackers, the provider of the communication service has the duty to provide information about the existence of these risks. If no action against the risk is available to the service provider, it must alert the subscribers to the possible ways of avoiding or mitigating the risk including the costs of these remedies. For example, it will advise about using certain anti-spam or anti-spyware software.

Cookies and spyware

The question of cookies and spyware is addressed in the Directive, both in the Recitals (24 and 25) and „implicitly" in Art. 5. Indeed the Directive aims at being technologicalIy neutral and therefore speaks of „technical storage of information" or „access to information stored in terminal equipment". After having stressed that terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private spheres of users requiring protection under the European Convention for Human Rights, the EU Directive recitaIs recognise that cookies may be a legitimate and useful tool for example in verifying the identity of users engaged in online transactions. In this sense, Art.5(3) limits the use of technical storage or access to information stored in terminal equipment for sole purpose of carrying out or facilitating the transmission of a communication over an electronic communication network or to facilitate the provision of information society services. Article 5(3) conditions the use of cookies to the provision of clear and precise information in accordance with Directive 95/46 about the purposes of the cookies, spyware or similar devices so as to ensure that users are made fully aware of the information being placed on the terminal that they are using. Finally, Art.5(3) restricts the use of cookies to the possibility for the users to refuse to have a cookie, spyware or similar device stored on their terminal equipment. However, the article implicitly admits that in the event that one refuses to accept a cookie used for a legitimate purpose, access to specific web site content may be refused.

Unsolicited Communications

Article13 of Directive 2002/58 deals with the question of unsolicited communications. The idea is to provide safeguards for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, fax machines, emails or SMS messages.

The regime which applies to these types of communications depends on the means used to send the communication to the person targeted.

If communication means such as automated calling systems, e-mail, facsimile machines are used, then Art. 13 (1), (2) and (5) of Directive 2002/58 apply (see below)

If other forms of communications means such as person-to-person voice telephony calls are used, then Art. 13 (3) and (5) will apply (see below).

Moreover, Article 7 of the e-commerce Directive 2000/31 will apply if the unsolicited communication is provided within the frame of an „information society service" that is to say a service normally provided for remuneration at a distance by electronic means at the individual request of a recipient of services. According to this provision, Member States which permit unsolicited commercial communications by electronic mail should ensure that such a commercial communication by a service established on their territory is clearly identified as soon as the communication is received by the recipient. It also provides that Member States ensure that service providers undertaking unsolicited commercial communications by electronic mail consult regularly and respect opt-out registers in which natural persons not wishing to receive such communications can register themselves.

Article 13 (1) of Directive 2002/58 establishes the regime of opt-in whereby in principle the use of automated calling machines, fax machines and e-mails for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. Indeed, it is believed that these forms of unsolicited commercial communications may, on the one hand, be relatively cheap and easy to send and, on the other, may impose burden and/or cost on the recipient. Moreover in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such reasons it is considered justified to require that prior explicit consent of the recipient is obtained before such communication are addressed to them.

However, Art. 13(2) softens the regime for unsolicited electronic communications sent within the framework of existing customer relationships. Indeed, it is believed that within the context of existing customer relationships it is reasonable to allow the use of electronic contact details for the offering of similar products or services, but only by the same company that has obtained the contact details according to Directive 95/46. When the contact details are obtained, the customer must be informed of their future use for direct marketing purposes in a clear and distinct manner and given the possibility to refuse such use free of charge.

For all other forms of unsolicited commercial communications by telecommunications means such as person-to-person voice telephony calls, Art. 13(4) enables Member States to choose between an opt-in or opt-out regime. The idea is that since these forms of direct marketing are more costly for the sender and impose no financial cost on

the receiver, this may justify the maintenance of a system giving subscribers and users the possibility to indicate that they do not wish to receive such calls (opt-out).

In all cases, Art. 13(4) prohibits the sending of electronic mail for purposes of direct marketing which disguise or conceal the identity of the sender on whose behalf the communication is made, or without a valid address to which the recipient may send a request that such communications cease. Indeed, to ensure the effective enforcement of the rules on unsolicited commercial communications, it is important to prevent the use of false identities or false return addresses.

Terminal equipment

Terminal equipment is regulated indirectly by various articles but directly by article 14 of the Directive. So, certain provisions requires that the terminal equipment will be equipped by certain functionalities in order to ensure data protection (for example, the user must have the right with user-friendly system to block the sending to the receiver of his/her telephone number or to block the arrival of any cookie or spyware. As regards Art.14 two concerns have taken into consideration.

On the one hand, it is an important objective of the European Community to create a single and competitive market for telecommunications services as well as for terminal equipment. The Directive therefore stresses that Member States – when implementing the provisions of the Directive – should ensure that no requirements for specific technical features are imposed on terminal equipment or other electronic communication equipment if such requirements could prevent this equipment from being placed on the single market or from circulating there. Requirements which do not influence the introduction in the market or the free circulation in the Community can be imposed without infringing the Directive.

On the other hand, the Directive acknowledges that technology may be compatible or incompatible with the right of users to protect the use of their data. Therefore the implementation of the Directive may not be entirely technology neutral. Member states may – where necessary- adopt measures which ensure that terminal equipment is compatible with the right of the users under the Directive. Indeed, measures which require privacy-enhancing features in terminal equipment (e.g., a simple means to eliminate calling line identification according to art. 8) may be vital for the successful implementation of the Directive.

Finally, the implementation of the Directive has to be reconciled with the requirements of European standardization of terminal equipment. According to Recital 46, *„. It may […] be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected. The adoption of such measures in accordance with*

Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity will ensure that the introduction of technical features of electronic communication equipment including software for data protection purposes is harmonised in order to be compatible with the implementation of the internal market." This means that if Member States adopt such measures, they have to take into account the R & TTE Directive[24] as well as the Council Decision[25] of 1986 on standardization in this field, in order to prevent divergent national requirements with regard to technical specifications.

More recently as regards the new threats linked with the development of RFID systems, the Article 29 Working Group has pointed out the necessity for terminal equipment producers to implement in the design of their systems the means to ensure the full respect of the privacy requirements by the companies who would like to use their systems.

According to the Group, *„manufacturers of RFID technology and standardization bodies are responsible for ensuring that data protection/privacy compliant RFID technology is order to ensure that such standards are widely followed in practical applications. In particular RFID privacy compliant standards must be available to ensure that data controllers processing personal data through RFID technology have the necessary tools to implement the requirements contained in the data protection Directive.".* This principle has been repeated in other opinions and might be seen as a way to extend the data protection obligations beyond its traditional scope: the terminal equipment manufacturers are clearly considered as liable if their system allows certain privacy threats even if these threats are not caused by themselves.

2.2 Arrangements other than law and regulation

The aim of this section is to examine the existence of self regulatory measures undertaken by different stakeholders – ECSPs, ECNPs, content providers, software providers, marketing associations – who aim to enhance the end user trust in on line activity. This entails security of networks, equipment, services and on line electronic commerce practices as well as measures aimed to secure the privacy of information transfer over the networks using different types of services.

Section 1.2.1 deals with self/co-regulation in general and codes of conduct, Section 1.2.2 addresses the topic of technical measures and section 1.3.3 covers the concerns related to standardization.

---

24 Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

25 COUNCIL DECISION of 22 December 1986 on standardization in the field of information technology and telecommunications (87/95/EEC)

2.2.1 Self/Co-Regulation mechanisms and Codes of Conduct

2.2.1.1 The general European position as regards Self/Co-Regulation

In 2003, an *Inter-institutional Agreement on Better Law-making* concluded between the EU Parliament, the EU Council of Ministers and the EU Commission[26] recalls the importance of alternative regulation mechanisms for a better regulation. This Agreement contains the overall principle regarding alternative regulation mechanisms (Point 16), the limits of their use (Point 17) and precise definitions of what is meant by 'co-regulation' (Point 18) and 'self-regulation (Point 22).

As regards the role of the legislative action, Point 16 of the Agreement enunciates that *„The three Institutions recall the Community's obligation to legislate only where it is necessary, in accordance with the Protocol on the application of the principles of subsidiarity and proportionality. They recognise the need to use, in suitable cases or where the Treaty does not specifically require the use of a legal instrument, alternative regulation mechanisms."*

The text clearly asserts the double „subsidiarity" of the legislative approach. The first one has been asserted as a fundamental principle of the European Union and does mean that the European Union institutions may only act on matters that might not be more adequately ruled at another lower level (read *local* level). Apart from that, the combination of the subsidiarity and proportionality principles leads the European Agreement to an additional point of view. It imposes not to legislate when other means to achieve the public objectives might be met by other ways, particularly self-regulation, or to legislate only to the extent necessary to fix the public objectives, leaving to the private sector the decision as regards the right way for reaching them. In this last case we are speaking about co-regulation.

These principles enacted, the Agreement imposes certain limits to these alternative modes of regulation. Point 17 details these limits. We briefly mention them here:

- the use of co-regulation or self-regulation must always be *consistent with Community law*
- it must *meet the criteria of transparency (in particular the publicising of agreements) and representativeness of the parties involved*.
- It must *represent added value for the general interest.*

---

26 *Inter-institutional Agreement on Better Law-making* of 16 December 2003, 0J 31.12.2003, 2003/C 321/01

Again, as in 1998[27], the criteria of legal validity of a norm are present in the principle focussing on alternative regulation mechanisms[28].

The text requires the representativeness of the parties involved and the transparency of the procedures followed within the self- or co-regulatory process (legitimacy criterion).

The principle of „added value" is repeated. The mechanisms may be used on the basis of criteria defined in the legislative Act[29]. The idea is again to fight against the rigidity of legislative solutions. There is a need for supple mechanism for ensuring a continuous adaptation to the problems and sectors concerned. These must be encouraged. The European Commission ensures the conformity also through mechanisms of notification and even control[30] (conformity criterion).

Finally, the main added value of alternative regulation mechanisms relies on more adapted, rapid and efficient enforcement mechanisms, such as label, accreditation, standardization or ADR or ODR[31] mechanisms[32] (effectiveness criterion).

The analysis of the second part of point 17 highlights that the alternative regulation mechanisms may not be used in all circumstances:

They may not be applicable:

- where fundamental rights or important political options are at stake or
- in situations where the rules must be applied in a uniform fashion in all Member States.

Finally, Point 17 foresees that they must ensure swift and flexible regulation which does not affect the principles of competition or the unity of the internal market.

Points 18 and 22 of the Inter-institutional Agreement define respectively co-regulation and self-regulation.

The Agreement defines co-regulation as the mechanisms whereby a community legislative act entrusts the attainment of the objectives defined by the legislative authority to parties which are recognized in the field (such as economic operators, the social partners, non governmental organisations, or associations)".

---

27 See WP 13 described and discussed above

28 Refer on this point to Yves Poullet, Internet Governance: Some thoughts after the two WSIS, *Liber Amicorum J. Berleur, Springer Verlag*, to be published,, p.13

29 Point 18 §2 of the inter-institutional Agreement

30 *« These measures may provide, for example, for the regular supply of information by the Commission to the legislative authority on follow up to application or for a revision clause under which the Commission will report at the end of a specific period, …* » (Inter-institutional Agreement, Point 21 in fine).

31 Alternative Dispute Resolution

32 „*The competent legislative authority will define in the act the relevant measures to be taken in order to follow up its application …" (*Inter-institutional Agreement, Point 21)

This definition induces a clear partition of the responsibilities of the State, on one hand, and the private sector and other interested parties, on the other hand. The legislative authorities have to fix the essential public policy objectives, when the means, by which they are met, are fixed together by the public and the private sectors. Public and private orderings are hence not on the same level. There is a sort of hierarchy insofar the co-regulation is viewed not as a substitute to the public intervention but as a way to achieve (choice of the means) the end objectives imposed by the framework fixed by the State.

The European conception of co-regulation does envisage this mechanism not as a way to prepare future public regulation,[33] but as a tool for refining the content of regulation enacted by public bodies and actually implementing it[34].

As regards self-regulation, the Agreement stipulates in its Point 22 that „Self-regulation is defined as the possibility for economic operators, the social partners, non-governmental organisation or associations to adopt amongst themselves and for themselves common guidelines at European level (particularly codes of practice or sectoral agreements).

As a general rule, this type of voluntary initiative does not imply that the Institutions have adopted any particular stance, in particular where such initiatives are undertaken in areas which are not covered by the Treaties or in which the Union has not hitherto legislated. As one of its responsibilities, the Commission will scrutinise self-regulation practices in order to verify that they comply with the provisions of the EC Treaty."

More flexibility is thus given to the private sector insofar as initiatives may be *undertaken in areas which are not covered by the Treaties or in which the Union has not hitherto legislated.* A certain control will however be exercised thereon.

Finally, point 23 of the Agreement foresees the necessity to notify the European Parliament and the Council of self-regulation practices regarded as contributing to the attainment of the EC Treaty objectives, being compatible with its provisions, having a satisfactory representativeness of parties involved and containing commitments with added value. Publicity is made for such kind of practices.

---

33 As pointed out by the White Paper (EU Commission White Paper, „*European Governance", (COM (2001)428, final*,p.12) whose content has been used as the basis for the Inter institutional Agreement: „*the quality, relevance and effectiveness of EU policies depend on ensuring wide participation throughout the policy chain – from conception to implementation. Improved participation is likely creating more confidence in the end result and in Institutions which deliver policies*". So, the White Paper does suggest a „more effective and transparent consultation at the heart of EU policy-shaping" through multiple channels: advisory committees, hearings, on-line consultations

34 Yves Poullet," Internet Governance: Some thoughts after the two WSIS", *op.cit*., p.14

2.2.1.2 The European position as regards Privacy Codes of Conduct

a. Introduction

When considering the European position as regards Codes of Conduct one should first focus on Article 27 of the European Directive 95/46. This article explicitly encourages *the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to* [the] *Directive, taking account of the specific features of the various sectors.*

To complete the landscape, one must take account of the opinions and working documents of the Article 29 Working Party. Article 27 of the Directive determines the role of this Working Party as regards codes of conduct: draft Community Codes or amendments (including extensions) to existing Community Codes may be submitted to the Working Party in order for the Party to check whether the drafts submitted are in accordance with the provisions of the Directive. Up to now, only the FEDMA Code and the IATA Code have been adopted pursuant to this procedure.

In addition, the Article 29 Working Party also played an important role in the adoption of codes of conducts specifically created in the framework of Transborder Data Flows (the Safe Harbour Principles) and in the determination of the criteria to be respected for considering a code of conduct to meaningfully contributing to the level of data protection in a third country. This chapter will have a close look at these criteria.

Finally, the trustmark or label scheme is worth being analysed. European initiatives (notably the Joint Research Centre (JRC) e-confidence Forum initiative) are tempting to organize some coherence in the e-commerce (including a data protection dimension) trustmark systems by establishing meta-trustmarks (common European basic criteria for an adequate e-commerce trustmarking).

b. European recognition of codes of conduct

At European level, the use of codes of conducts has been legally recognized in Article 27 of European 95/46. As previously said, Member States and the Commission explicitly encourage *the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States pursuant to* [the] *Directive.* An express reference is made to the necessity to adopt codes by sector, taking account of their specific features.

The provision further puts the accent on the need for two types of codes: on one hand, national codes (new ones or the adaptation of existing ones) that can be submitted to the National data protection authority, and, on the other hand, Community Codes (new ones or the adaptation of existing ones) that can be submitted to the Article 29 Working Party. The Working Party will determine among other things, whether the drafts are in

accordance with the provisions adopted pursuant to the European Directive[35]. If a code is approved, the Commission *may ensure appropriate publicity*[36] for it.

The procedure that has to be followed by interested parties for the submission of Community Codes of Conduct, and for their subsequent evaluation has been clarified in a Working Document of the Article 29 Working Party of 10 September 1998: the so-called WP13[37]. This procedure contains acceptance criteria and criteria „de fond":

To be considered by the Working Party, the Community Code must be submitted *by any organisation representative of the sector concerned and established or active in a significant number of Member States.*[38] The draft code must also be *prepared carefully, preferably in consultation with the data subjects concerned or their representatives, and must clearly define the organisation or sector to which the code is intended to apply.*[39] Finally, a language criteria has to be respected (translation to English and French is mandatory).

To be approved by the Working Party, the submitted code of conduct must *be in accordance with the data protection directives and, where relevant, the national provisions adopted pursuant to these directives*[40]*.* It must also be of sufficient quality and internal consistency. It must provide *sufficient added value to the directives and other applicable data protection legislation*. This can be achieved when the code is well-adapted to the data protection issues in the organisation or sector at stake.

These criteria reflect the three main conditions as regards the enactment of self-regulatory or co-regulatory norms[41]: legitimacy, conformity and effectiveness.

---

35 Article 27, al. 3

36 Article 27, al.3 *in fine*

37 'Future work on codes of conduct: Working Document on the procedure for the consideration by the Working Party of Community codes of conduct', WP 13, 10 September 1998.

38 WP13, Article 2.1.

39 WP13, Article 2.2.

40 WP 13, Article 4.1.

41 The three criteria of the validity of a self-or co-regulation have been extensively developed by Yves Poullet in a essay taking into account the reflections proposed by R. SUMMERS (Y. POULLET, „How to regulate Internet?: New Paradigms for Internet Governance", in *Variations sur le droit de la société de l'information, J. Berleur et alii (ed.,) Cahier du CRID, n° 20*, p. 130 et s). These three criteria are defined as follows:

„- *The **„legitimacy"** is „source oriented and underlines the question of the authors of a norm. To what extent, might the legal system accept a norm elaborated outside of the actors designated by the Constitution or under constitutional rules? This quality of the norm means that the authorities in charge of the norm promulgation must be habilitated for doing that by the community or communities of the persons which will have to respect the rule they have enacted. This legitimacy is obvious as regards the traditional State authorities acting in conformity with the competence devoted to them by the Constitution. It is less obvious when the regulation is the expression of private actors themselves as it is the case with self-regulation, particularly when it is the fact of certain obscure associations or even of private companies able to impose their technical standards.*

- *The **„conformity"** is „content oriented" and designates the compliance of normative content vis-à-vis fundamental society values, those embedded undoubtedly in the legal texts but also beyond that those considered as ethical values to be taken into account by the legal system. Again this*

The „Legitimacy" criterion is found in the requirement of representativeness of the business association at the source of the Code of conduct and their preliminary consultation of the data subjects.

The „Conformity" criterion is met by the need to comply with the provisions of the data protection directives and the national provisions adopted pursuant to these. In addition, the principle of „added value[42]" is declared.

Finally, regarding the „Effectiveness" criterion is also embedded in the need for a Code of *sufficient quality and internal consistency*, with *added value* and compliant with the applicable Directives. It is clear that the Working Party will consider the effectiveness as a crucial point. Effective sanctions, dispute resolutions, easy access to the contact points, monitoring of the system are the key points to check.

The procedure described in WP13 has nonetheless been rarely followed. Up to now, two codes of conducts have been approved in this context: the FEDMA and the IATA[43] codes. In the present contribution we will have a closer look at the FEDMA Code.

The FEDMA Code of the Federation of European Direct Marketing has been approved by the Working Party on 13 June 2003.[44] The Opinion expressed in WP77 details that the Code is in accordance with the Directive and the national provisions implementing it at national level, and, secondly, that the code provides sufficient added-value, *in terms of being sufficiently focussed on the specific data protection questions and problems in the direct marketing sector and offering sufficiently clear solutions for the questions and*

---

criterion is quite easy to satisfy and to verify in case of traditional texts issued by governmental authorities insofar these texts must be taken in consideration of already existing rules with superior values. It seems more intricate to satisfy to this criterion when the compliance with existing legislative text is not systematically checked insofar these texts are not existing or not clearly identified. Indeed self-regulation is often a way to avoid the traditional and constitutionally foreseen regulatory methods of rule-making.

- *Finally, the „**effectiveness**" is „respect oriented". To what extent, a norm will be effectively respected by those to whom the norm is addressed? So, the question about the information about the existence of the norms, about the sanctions and the way by which they might be obtained are central for determining the effectiveness of a norm. By this criterion, one means in particular the fact for the addressees of the norm to be aware of the content of the norm but also for norms to foresee a cost for its non respect by addressees who are so stimulated to follow the rule."*

42 The „added value" principle has been enacted quite clearly by the „e-confidence forum" settled up by the DG Sanco in order to define key principles as regards the acceptability of the self-regulatory methods (code of conduct, labelling system and On Line Dispute Resolution Platforms (in brief ODR).). As regards these principles, see the e-confidence website available at : http://www.econfidence.jrc.it/default/htm. These principles and more broadly the attitude of the E.U authorities v. à v. the self-regulation have been commented by Yves Poullet in: „ Vues de Bruxelles: Un droit européen de l'Internet ?", *Le droit international de l'Internet*, Bruylant, Brussels p.165 and ff.

43 In 1997, the International Air Transport Association (IATA) submitted to the Working Party „Recommended Practice 1774 - Protection of privacy and transborder data flows of personal data used in international air transport of passengers and cargo" (RP 1174). These guidelines are recommended by IATA to its members for years. In light of directive 95/46/EC, IATA revised RP 1774 with the aim to comply with the directive and possibly contribute to free flow of personal data amongst its international members.

44 'Opinion 3/2003 on the European code of conduct of FEDMA for the use of personal data in direct marketing', WP77, 13 June 2003.

problems at stake[45]. The Code provides indeed for a clear and well-illustrated explanation of the data-protection issues in the field of direct marketing. It takes account of specific issues such as in-house suppression lists, host mailings, disclosure of lists, the sources of the data, the right to object to the processing for direct marketing purposes, preference services systems, etc. and explains clearly all the possible situations that can be encountered by Companies organising direct marketing[46].

Judging the value of a code

Privacy commitments are undertakings by individual companies while *Privacy Codes of Practice* or Codes of Conduct are laid down at more collective levels, such as within an industrial sector. In the event a firm does not respect the principles it has accepted, it must face the sanctions determined in the code. These sanctions have been determined by the association that drew up the code. Finally, *standards*[47] involve an assessment procedure for determining whether those that agree to abide by them, in fact do so. This can be achieved by delivering a certification that the actual protection conforms to the agreed privacy principles and/or the awarding of a label. More *general standards* can also be developed. They will be subject to audits or other checks[48].

The advantage of such alternative regulation mechanisms for data subjects is that they offer principles that are adapted to the particular circumstances of a company or sector, in a language that is much easier to understand than formal legislation could impose. But the great disadvantage, in turn, can be a lack of effectiveness of this form of regulation.

In the previous section we already focussed on three criteria of validity of a norm that has been applied to the validity of self-regulation and co-regulation: the legitimacy, the conformity and the effectiveness criteria.

The analysis of the Article 29 Working Party opinions can help us to refine these criteria.

The Article 29 Working Party has first determined criteria to judge the value of a code in a precise framework: the transfer of personal data to third countries.

Article 25(2) of the data protection directive (95/46/EC) requires the level of personal data protection to be assessed in the light of *all the circumstances* surrounding a data transfer operation or set of such operations. These circumstances include rules of law but reference is also made to *professional rules and security measures which are complied with in that country*. Non-legal rules have thus to be taken into account provided

---

45 WP77, p.3
46 The FEDMA Code has been annexed to the WP77
47 Regarding standards, please refer to part III of the present report
48 See Y. Poullet, „ Internet Governance: Some thoughts after the two WSIS", *op.cit*., p.14

that these rules *are complied with.* It is indeed of importance to determine when self-regulation makes a meaningful contribution to the level of personal data protection in a third country.

Article 25 of Directive 95/46 recognises thus – as Article 27 more directly does – the importance and legal value of codes of conduct.

It is in this 'transborder context' that the Article 29 Working Party has considered the role of industry self-regulation in January 1998[49] and the criteria to judge them. Its WP 7[50] is dedicated to the issue. The general criteria that are given provide for an interesting overall analysis of the way to determine the value of Privacy Codes of Practice.

Self-regulation is defined in the WP at stake as *any set of data protection rules applying to a plurality of data controllers from the same profession or industry sector, the content of which has been determined primarily by members of the industry or profession concerned*.

This concept includes confidentiality codes of conduct developed by small industry associations as well as detailed deontological codes applicable to entire professions (doctors, bankers, attorneys at law,…) and having often quasi-judicial force.

A first criterion on which the Article 29 Working Party is focussing is the **representativeness** of the associations or bodies responsible for the code. The Article 29 Working Party put forward that*, in this context, the question of whether the association or body responsible for the code represents all the operators in a sector or only a small percentage of them, is probably less important than the strength of the association in terms of its ability to, for example, impose sanctions on its members for non-compliance with the code*[51]*.* The degree to which the rules can be **enforced** is thus the point to matter about. The Article 29 Working Party nonetheless highlights that *there are several secondary reasons which render industry-wide or profession-wide codes with clearly comprehensive coverage more useful instruments of protection than those developed by small groupings of companies within sectors.* When several associations are dividing a same sector by adopting rival codes, the consumer can be confused. **Transparency** then disappears. And personal data can be less effectively protected. An example given in this regard concerns the direct marketing industry. The Article 29 Group mentions that in such kind of industry *where personal data is routinely passed between different companies of the same sector, situations can arise where the company disclosing personal data is not subject to the same data protection code as the company that receives*

---

49 Definitively, the Binding Corporate Rules, which are also promoted by the Art. 29 WG as another way for multinational companies to offer an adequate protection in the sense of article 26.2, are also a"selfregulatory" tools.

50 Working Document 7 of Working Party on the Protection of Individuals with regard to the Processing of Personal Data : *Judging industry self-regulation: when does it make a meaningful contribution to the level of data protection in a third country?*, 14 January 1998, D/5057/97 final

51 WP7, p.2

it. This is a source of considerable ambiguity as to the nature of the rules applicable, and it might also render investigation and resolution of complaints from individual data subjects extremely difficult. The solution of the e-confidence initiative[52] in this regard is to prohibit the transfer of data between companies not subject to the same code, unless additional guarantees are foreseen. We will have a closer eye on this initiative in a next section.

This being said, the opinion of the Article 29 Working Party allows us to conclude that the evaluation of a code has to be made at three levels: the source of the document (upstream), the content of the document and the effectiveness of the document (downstream).

1. Upstream : source of the document

The first conditions to check are related to the source-oriented. As already largely explained, this relates to the legitimacy of the code: the verification of the representativeness of the author of the document, its enforcement power and the transparency of the code.

2. Content of the document

The Content of the Document must be assessed to check its conformity with the applicable directives and national provisions. A check list of core principles has been drawn up by the Article 29 Working Party.[53] These principles are the purpose limitation principle[54], the data quality and proportionality principle[55], the transparency principle[56], the security principle[57], the rights of access, rectification and opposition[58], restrictions on onward transfers to other third countries[59] and additional principles to be applied to specific types of processing:

1) sensitive data[60]; 2) direct marketing[61]; and 3) automated individual decision[62]

---

52 UNICE and BEUC, e-confidence project, BEUC/X/179/2000, 22 October 2001,

53 Note the use of the same core principles when making the overall assessment of the adequate level of protection offered by a third country (WP12)

54 Data should be processed for a specific purpose and subsequently used or further communicated only insofar as this is not incompatible with the purpose of the transfer (exemptions in Article 13 of the directive are allowed).

55 Data should be accurate, kept up to date, adequate, relevant and not excessive

56 Information must be provided as to the purpose of the processing, the identity of the data controller and other information insofar as this is necessary to ensure fairness. (exemption in Articles 11(2) and 13 of the D.P. Directive 95/46).

57 Appropriate technical and organisational security measures should be taken

58 Right to obtain a copy of all data, right to rectification, right to object to the processing (exemption in Article 13 of the Directive).

59 Further transfers of the personal data from the destination third country to another third country should be permitted only where the second third country also affords an adequate level of protection (exceptions in Article 26 of the directive)

60 Where 'sensitive' categories of data are involved (those listed in article 8), additional safeguards should be in place, e.g. the explicit consent for the processing.

3. Downstream: effectiveness of the document

The Article 29 Working Party insists on the necessity to have an efficient mechanism. This effectiveness must be obtained in three situations: in achieving 1) a good level of general compliance, 2) support and help to individual data subjects and 3) appropriate redress (including compensation where appropriate[63].

The Good Level of Compliance depends typically on

- *the degree of awareness of the code's existence and of its content among members,*
- *the steps taken to ensure transparency of the code to consumers in order to allow the market forces to make an effective contribution,*
- *on the existence of a system of external verification (such as a requirement for an audit of compliance at regular intervals) and*
- *on the nature and enforcement of the sanction in cases of non-compliance*[64]

This requirement is thus directly linked to the sanctions that should be put in place. Important is here to have effective sanctions. Not simply „remedial" sanctions[65], but rather „punitive" sanctions[66]. Only the latter might have an actual effect on the future behaviour of data controllers.

Further there is a need for an Effective Support and Help provided to individual data subjects. They may not be left alone when facing a problem relating to their data. An ideal scenario would be the existence of an *impartial, independent and equipped* institutional support *with the necessary powers to investigate any complaint from a data subject.*

Finally, the existence of Appropriate Redress mechanisms must be checked. *If the self-regulatory code is shown to have been breached, a remedy should be available to the data subject.* And if the individual has suffered damage (*including psychological or moral harm*, details the Working Party), there should be appropriate compensation. As sanctions have a dual function of punishing and thus encouraging compliance, it also remedies a breach of rules. Consequently, appropriate and effective sanctions are again (as it was for the necessity of Good Compliance) a solution to comply with this

---

61 The data subject should be able to 'opt-out' from having his/her data used for such purposes at any stage.
62 The individual should have the right to know the logic involved in this decision and other measures should be taken to safeguard the individual's legitimate interest.
63 WP7, p.3
64 WP7, p.4
65 The member is required, in case of non compliance, to simply change its practices to be in line with the code.
66 The member is actually punished for its non compliance

condition. Remedies may be improved by setting up Alternative Dispute Resolution (ADR) mechanisms.

Summary of the retained criteria

By combining this view with the previously mentioned three basic criteria for the value of a norm, one can summarise the criteria to take into account as follows:

1. Upstream	LEGITIMACY	Check the **Source** - Representativeness - Enforcement power - Transparency (rival codes in same sector?)
2. Content	CONFORMITY	1. Check **conformity** with - Directives - National provisions ➔ Check existence of **core content principles** 2. Check **transparency** (language, concrete examples); 3. Check **prohibition of disclosure** to non-members except if additional safeguards
3. Downstream	EFFECTIVENESS	Check achievement of - a good level of general **compliance** o degree of awareness o transparency o system of external verification o sanctions in cases of non-compliance (punitive) - **support and help** to individual data subjects: impartial, independent and equipped appropriate **redress** (including compensation where appropriate). Including psychological harm

Relevant questions as regards the effectiveness pole

To complete the diagram, it is worth mentioning the questions related to the 3 conditions determined in the Effectiveness part. The Article 29 Working party has indeed tempted to be as concrete as possible in its opinion. It therefore has mentioned actual questions providing a good understanding of what is meant by 'good compliance', 'support and help' and 'appropriate redress. We quote them hereunder.

1. Questions related to the evaluation of a good level of compliance with the code by the members.

   - *what efforts does the representative body make to ensure that its members are aware of the code?*
   - *does the representative body require evidence from its members that it has put the provisions of the code into practice? How often?*
   - *is such evidence provided by the member company itself or does it come from an external source (such as an accredited auditor)?*
   - *does the representative body investigate alleged or suspected breaches of the code?*
   - *is compliance with the code a condition of membership of the representative body or is compliance purely „voluntary"?*
   - *where a member has been shown to breach the code, what forms of disciplinary sanction are available to the representative body (expulsion or other) ?*
   - *is it possible for an individual or company to continue working in the particular profession or industry, even after expulsion from the representative body?*
   - *is compliance with the code enforceable in other ways, for example by way of the courts or a specialist tribunal? Professional codes of ethics have legal force in some countries. It might also be possible in some circumstances to use general laws relating to fair trading practice or even competition to enforce industry codes.*

2. Questions related to the evaluation of an adequate support and help mechanism.

   - *Is there a system in place allowing for investigation of complaints from individual data subjects?*
   - *How are data subjects made aware of this system and of the decisions taken in individual cases?*
   - *Are there any costs involved for the data subject?*
   - *Who carries out the investigation? Do they have the necessary powers?*
   - *Who adjudicates on an alleged breach of the code? Are they independent and impartial?*

3. Questions related to the evaluation of an appropriate redress

   Questions of part 1 above (compliance) relating to sanctions can be appropriate. Additional questions are:

- *Is it possible to verify that a member who has been shown to contravene the code has changed his practices and put the problem right?*
- *Can individuals obtain compensation under the code, and how?*
- *Is the breach of the code equivalent to a breach of contract, or enforceable under public law (e.g. consumer protection, unfair competition), and can the competent jurisdiction award damages on this basis?*

Example of an alternative regulation mechanism: **Labelling schemes**

Interesting manners for promoting consumer confidence in electronic commerce are labelling mechanisms. Organisations (code owners) establish standards (codes of conduct) for conducting electronic commerce or, sometimes, more restrictively, for respecting one specific issue in this landscape – such as privacy – and certify that a particular subscriber meets the determined standards. When the requirements are fulfilled, the subscriber receives most commonly a trustmark seal of approval.

The 2005 report on trustmarks and web seals in the European Union[67] aimed at determining the usefulness of trustmarks as regards the contribution to a stronger consumer confidence in e-commerce. The report however did not forget other essential facets of the issue: the question whether trustmarks are commercially viable operations, the issues related to independence, monitoring and enforcement (and the management and costs of such operations); and, finally, the extent to which trustmarks benefit different types of e-merchants (major enterprises as opposed to SMEs), and to which extent they substitute (or have potential to substitute) brand recognition on the e-commerce market[68]. Before to describe the main results of this report, it must be underlined that if all the trustmarks analysed are not covering the privacy issues, most of them are dealing with these issues even if the consumer protection requirements seems more central. None is specifically addressing only the Privacy requirements.

In the framework of this chapter on alternative regulation mechanisms, it seemed interesting to us to have a closer look at the results of an in-depth analysis of one type of such self-regulatory tool. In that respect, the mentioned report was interesting, although not focussing directly on data protection but more largely on e-commerce. Data protection being however a brick in the e-commerce trust building, we retained its utility.

The report leads to very interesting results. We will discuss some of them that are concerning our perspective:

---

67 Yves Poullet, Ronald de Bruin, Christophe Lazaro, Ewout Keuleers, Marjolein Viersma, *Analysis and definition of common characteristics of trustmarks and web seals in the European union,* final report, February 2005, European Contract nr B5-1000/03/000381 (DG Sanco), 104 p.

68 Trustmark Report, *op.cit.,* p. 5

- the business and consumer analysis
- the legal analysis on trustmark schemes,
- commercial-viability of trust-mark schemes models; and
- the determination of the factors that are relevant to the success of trustmark schemes (critical success factors)

By first having a closer look at the results of the *business and consumer analysis*, one can make an immediate link with the criteria brought out by our desk analysis (legitimacy, conformity and effectiveness). The conclusions and recommendations made on the basis of the on-line survey realised in the framework of the project clearly refer to key-factors already identified.

The general recommendations to increase the acceptance of a trustmark scheme were:

- necessary **compliance** of the codes of conduct with EU regulations (legitimacy), an European code of conduct model could save legal on legal expenses and increase consumer/individuals trust
- need for a money-back guarantee (appropriate redress – effectiveness)
- need for strong **enforcement power** of the code owner to take appropriate action against the code subscriber that does not respect the code (enforcement – legitimacy/effectiveness)
- adequate and several possible **sanctions** (effectiveness)
- independency of the **dispute resolution** body (appropriate redress – effectiveness)
- **transparency** of the trustmark schemes, good understanding of the benefits of the scheme for the individual (conformity/effectiveness)

In the field of consumer experience, the report further recommends:

- again, need for great **transparency** (easy search for information about the content of the code, easy understanding (global (quick look) information and detailed information), user-friendly tool, availability in the individual's language).
- **conformity / effectiveness**
- Easy identification of the companies that are certified (link from the code of conduct web site to the web sites of the subscriber companies, and link from the subscriber company (web seal with hyperlink) to the general code of conduct/trustmark website).

➔ legitimacy/effectiveness

The *legal analysis* of the trust mark schemes lead to the identification of 14 critical *must-have* criteria for a trustmark scheme[69] (and other 26 *nice-to-have* criteria). These criteria can help us to refine our criteria diagram.

The must-have criteria have been summarised as follows:

1. Legitimacy of the scheme
2. Access and clearness of the code of conduct
3. Information on trustmark scheme's functioning
4. Assessment
5. Feedback
6. Applicable law and competent jurisdiction
7. Confirmation process
8. E-platform security
9. Customer service
10. Protection of children
11. Proactive monitoring
12. Complaints procedure for solving disputes
13. Enforcement system
14. Relationship with consumers

The actual application of those 14 criteria on 9 existing trustmark schemes leads to the conclusion that no one has had a positive evaluation for each of the must-have criteria at the time of the survey performed by the project team.

A particular trend is that most of the schemes have inconsistent results to the criteria test: very high scores are obtained for some criteria while very low are obtained for others (particularly for the enforcement criteria, which is problematic). In addition, the authors note a lack of '*European sensitivity'. In particular, this concerns a lack of multilingual information, lack of articulation and co-ordination between the different trustmark schemes and a lack of reference to (and involvement in) the existing EU initiatives regarding e-confidence and consumer protection*[70].

In addition to these Business and Consumer, and legal analyses, the report also highlighted the importance of a *commercial-viability of trust-mark schemes models*. Commercial viability can indeed only increase the participation of the business world to this

69 Trustmark Report, *op.cit.,* p.8
70 Trustmark Report, *op.cit.,* p.9

kind of regulation mechanisms. This dimension should not be underestimated. The implementation of a self-regulation mechanism indeed creates important costs (legal verification, implementation, monitoring of the system, functioning of support and help service, of dispute resolution, etc.). The benefits of the confidence created by the mechanism in the business of the subscribing company should at least be of equal importance.

Finally, *critical success factors* for trust mark schemes have been identified. The report concludes on a „top 7 list" of those factors[71] from which we deduce here 6 key success factors for alternative regulation mechanisms:

- a good awareness with the players (both businesses and individuals)
- a highly elaborated and robust code of conduct;
- Effective enforcement mechanisms;
- A good stakeholder support and a high number of subscribers of the mechanism
- Trust in the organisation that operates the mechanism
- Low costs/ good cost benefits

This must of course be read together with the legitimacy, conformity and effectiveness criteria already developed before.

2.2.2 The European approach as regards PETs (Privacy enhancing technologies)

In this section we briefly expose the European position as regards PETs

a. Context

The incorporation of PETs into strategies for privacy receives some encouragement from Article 17 of Directive 95/46/EC, which requires data controllers to implement *„appropriate technical and organisational measures"* to protect personal data, especially in network transmissions. Recital 46, which augments the meaning of Article 17, highlights the requirement that these measures should be taken both at the time of the design of the processing system and at the time of the processing itself, thus indicating that security cannot simply be bolted onto data systems, but must be built into them.

---

71 Trustmark Report, op.cit., p.100. The top 7 list for trademark schemes are : 1. Awareness with business and consumers; 2. a Highly elaborated and robust code of conduct; 3. Effective enforcement mechanisms; 4. Number of trustmarks issued (leading to user-fee revenue); 5. Trust in (independent) organisation that operates the trustmark scheme; 6. Stakeholder support; 7. Low up-front and operational costs.

Since the explosion of the Internet, due to the interactive nature of the network and its large capacity, new privacy threats have surfaced. The concept of Privacy Enhancing Technologies (PETs) or at least of „Privacy Compliant technologies" aims at organising/engineering the design of information and communication systems and technologies with a view 1. to minimising the collection and use of personal data, 2. to hindering any unlawful forms of processing by, for instance, making it technically impossible for unauthorised persons to access personal data, so as to prevent the possible destruction, alteration or disclosure of these data 3. to bettering the D.S. rights (right to be informed, right to access, right to rectify, etc.).

Already in '97, the Working Group on „privacy enhancing technologies" of the Committee on „Technical and organisational aspects of data protection" of the German Federal and State Data Protection Commissioners published two working papers[72] related to the topic of PETs.

The Article 29 Working Party has also showed interest for PETs by issuing Opinion 1/98 on *„the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)",* Recommendation 1/99 *„on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware"*[73], and a Working Document on *„Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group)"*

In a strategy document[74] dating from 2004, the Working Group has declared: *„New Technologies have a crucial role in promoting economic, social and human development but, at the same time, if not properly implemented, could cause adverse impact in the framework of guarantees for Fundamental rights and data protection, enshrined in*

---

72 Available at http://ec.europa.eu/justice_home/fsj/privacy/studies/priv-enhancing_en.htm

73 Recommendation 1/99 of the Article 29 Working Group, which is concerned with the threat to privacy posed by Internet communications software and hardware, establishes the principle that such industry products should provide the necessary tools to comply with European data protection rules. According to the working party, *„a condition for legitimate processing of personal data is the requirement that the data subject is informed and thus made aware of the processing in question. Therefore, the Working Party is especially concerned about all kinds of processing operations which are presently being performed by software and hardware on the Internet without the knowledge of the person concerned and hence are „invisible" to him/her (…). Internet software and hardware products should provide the Internet users information about the data that they intend to collect, store or transmit and the purpose for which they are necessary. Internet software and hardware products should also give the capacity to the data user to easily access any data collected about him/her at any later stage (…).The configuration of hard- and software products should not, by default, allow for collecting, storing or sending of client persistent information. Internet hard- and software products should allow the data subject to freely decide about the processing of his/her personal data by offering user-friendly tools to filter (i.e. to reject or to modify) the reception, storage or sending of client persistent information following certain criteria (including profiles, the domain or the identity of the Internet server, the kind and the duration of the information being collected, stored or sent and so on). The user should be provided with clear instructions regarding the use of soft- and hardware for the implementation of these options and tools (…).Internet software and hardware products should allow the users to remove client persistent information in a simple way and without involving the sender. The user should be given clear instructions on how to do this. If the information cannot be removed, there must be a reliable way to prevent it from being transferred and read."*

74 WP29, Strategy Document adopted on 29 September 2004, W.P. 98

European Law. For that reason, the impact of new technologies on privacy has always been a prominent issue of the Working Party, as common expertise and guidance is essential in that field. Since its very early documents, there has been an ongoing interest in the relationship between emerging technologies and data protection and the Working Party has always tried to provide advice on their privacy compliant design and implementation."

The European Commission has also realised that it is necessary to take additional measures to promote the use of these technologies. This has been one of the conclusions of the first implementation report on Directive 95/46/EC adopted by the Commission on the 15th of May 2003.

According to that report, *„Technological products should be in all cases developed in compliance with the applicable data protection rules. But being in compliance is only the first step. The aim should be to have products that are not only privacy-compliant and privacy-friendly but if possible also privacy-enhancing (….). The key-issue is therefore not only how to create technologies that are really privacy-enhancing, but how to make sure that these technologies are properly identified and recognised as such by the users. Certification schemes play a crucial role and the Commission will continue to follow developments in this area. The Commission believes that such schemes should indeed be encouraged and further developed. The objective is not just better privacy practices, but also to increase transparency and therefore the trust of users and to give those investing in compliance and even enhanced protection an opportunity to demonstrate their performance in this respect and exploit this to their competitive advantage".*

b. The Commission's Communication on PETs

More recently, on 2 May 2007, the Commission has adopted a Communication[75] with the purpose of identifying the benefits of Privacy Enhancing Technologies (PETs) and laying down the Commission's objectives in this field, to be achieved by a number of specific actions supporting the development of PETs and their use by data controllers and consumers.

According to that Communication, *„The intervention of different actors in data processing and the existence of different national jurisdictions involved could make enforcement of the legal framework difficult. On the other hand, PETs could ensure that certain breaches of data protection rules, resulting in invasions of fundamental rights including privacy, could be avoided because they would become technologically more difficult to carry out. The Commission is aware of the fact that technology – although having a crucial role in privacy protection – is not sufficient in itself to secure privacy. PETs need to be applied according to a regulatory framework of enforceable data protection rules providing a number of negotiable levels of privacy protection for all individuals."*

75 This Communication is available at http://ec.europa.eu/idabc/servlets/Doc?id=28587

In this, it repeats what Alexander Dix already noted when he said that *„Technology is, however, no panacea for privacy risks in cyberspace; it cannot replace a regulatory framework or legislation, contracts or code of conduct. Rather it may only operate within such a framework. Privacy by negotiation is therefore no alternative to regulation, but a necessary additional tool"*[76].

To pursue the objective of enhancing the level of privacy and data protection in the Community by promoting the development and the use of PETs, the Commission intends to conduct various activities, involving a vast array of actors, including its own services, national authorities, industry and consumers.

These activities are enumerated in the Commission's Communication and are structured around 3 objectives:

First objective: to support the development of PETs

In the context of that first objective, the first action encouraged by the commission is to identify the need and technological requirements of PETs[77] and the second to develop PETs[78].

---

76 A. Dix, Infomediaries and Negotiated Privacy Techniques, paper presented at the conference „Computers, Freedom and Privacy" (CPF 2000), 19 April, Toronto

77 The Commission will encourage various stakeholder groups to come together and debate PETs. These groups will include in particular representatives from the ICT sector, PETs developers, data protection authorities, law enforcement bodies, technology partners including experts from relevant fields, such as eHealth or information security, consumers and civil rights associations. These stakeholders should regularly look into the evolution of technology, detect the dangers it poses to fundamental rights and data protection, and outline the technical requirements of a PETs response. This may include fine-tuning the technological measures in accordance with the different risks and the different data at stake and taking into account the need to safeguard public interests, such as public security.

78 The Commission has already addressed the need for PETs. Under the auspices of the 6th Framework Programme it sponsors the PRIME8 project tackling issues of digital identity management and privacy in the information society. The OPEN-TC9 project will allow privacy protection based on open trusted computing and the DISCREET10 project develops middleware to enforce privacy in advanced network services. In the future, under the 7th Framework Programme, the Commission intends to support other RTD projects and largescale pilot demonstrations to develop and stimulate the uptake of PETs. The aim is to provide the foundation for user-empowering privacy protection services reconciling legal and technical differences across Europe through public-private partnerships. The Commission also calls on national authorities and on the private sector to invest in the development of PETs. Such investment is key to placing European industry ahead in a sector that will grow as these technologies become increasingly required by technological standards and by consumers more aware of the need to protect their rights in cyberspace.

Second objective: to support the use of available PETs by data controllers

To reach that second objective, the Commission intends to Promote the use of PETs by industry[79], to ensure respect for appropriate standards in the protection of personal data through PETs[80] thanks to standardization[81] and coordination of national technical rules on security measures for data processing[82] and finally to the use of PETs by public authorities[83].

---

79 The Commission believes that all those involved in processing of personal data would benefit from a wider use of PETs. The ICT industry, as the primary developer and provider of PETs, has a particularly important role to play with respect to the promotion of PETs. The Commission calls on all data controllers to more widely and intensely incorporate and apply PETs in their processes. For that purpose, the Commission will organise seminars with key actors of the ICT industry, and in particular PETs developers, with the aim of analyzing their possible contribution to promoting the use of PETs among data controllers. The Commission will also conduct a study on the economic benefits of PETs and disseminate its results in order to encourage enterprises, in particular SMEs, to use them.

80 While wide-reaching promotional activity requires the active involvement of the ICT industry, as the PETs producer, respect for appropriate standards requires action beyond selfregulation or the goodwill of the actors involved. The Commission will assess the need to develop standards regarding the lawful processing of personal data with PETs through appropriate impact assessments.

81 The Commission will consider the need for respect of data protection rules to be taken intoaccount in standardisation activities. The Commission will endeavour to take account of the input of the multistakeholder debate on PETs in preparing the corresponding Commission actions and the work of the European standardisation bodies. This will be paramount, in particular, where the debate identifies appropriate data protection standards requiring the incorporation and use of certain PETs. The Commission may invite the European Standardisation Organisations (CEN, CENELEC, ETSI) to assess specific European needs, and to subsequently bring them to the international level by means of applying the current agreements between European and international standardisation organisations. Where appropriate, the ESOs should establish a specific standardisation work programme covering European needs and thus complementing the ongoing work at international level.

82 National legislation adopted pursuant to the Data Protection Directive11 gives national data protection authorities certain influence in determining precise technical requirements such as providing guidance for controllers, examining the systems put in place or issuing technical instructions. National data protection authorities could also require the incorporation and use of certain PETs where the processing of personal data involved makes them necessary. The Commission considers that this is an area where coordination of national practice could contribute positively to promoting the use of PETs. In particular the Article 29 Working Party could contribute in its role of considering the uniform application of national measures adopted under the Directive. The Commission thus calls on the Article 29 Working Party to continue its work in the field by including in its programme a permanent activity of analyzing the needs for incorporating PETs in data processing operations as an effective means of ensuring respect for data protection rules. This work should then produce guidelines for data protection authorities to implement at national level through coordinated adoption of the appropriate instruments.

83 A consistent number of processing operations involving personal data are conducted by public authorities in the exercise of their competences, both at national and at Community level. Public bodies are themselves bound to respect fundamental rights, including the right to protect personal data, and ensure respect by others, and should therefore set a clear example. As regards national authorities, the Commission notes the proliferation of eGoverment applications as a tool for enhancing effectiveness of public service. As stated in the *Commission's Communication on the Role of eGoverment for Europe's Future*, the use of PETs in eGovernment is necessary to provide trust and confidence to ensure its success. The Commission calls upon governments to ensure that data protection safeguards are embedded in eGovernment applications, including through the widest possible use of PETs in their design and implementation. As for Community institutions and bodies, the Commission itself will ensure that it complies with the requirements of Regulation (EC) 45/2001 in particular through a wider use of PETs in the implementation of ICT applications involving the processing of personal data. At the same time, the Commission calls on other EU institutions to do the same. The European Data Protection Supervisor could contribute with his advice to Community institutions and bodies on drawing up internal rules relating to the processing of personal data. When selecting new ICT applications for its own use, or when developing existing applications, the Commission will consider the possibility of introducing privacy enhancing technologies. The importance of PETs will be reflected in the Commissions' overall IT governance strategy. The Commission will also continue to raise awareness in its

Third objective: to encourage consumers to use PETs

To reach this objective, the Commission intends to raise the awareness of the users[84] and to Facilitate the consumers' informed choice by promoting Privacy Seals[85]

2.2.3 The European approach as regards Standardization

Standardization is one particular form of self-regulation. Like other self-regulatory mechanisms it is based on consensus and the resulting products – rules, guides, specifications and other tools – are essentially voluntary. They cannot be legally enforced unless they are incorporated in a legal instrument. The difference between standards and other forms of self-regulation is that standards are being produced in the framework of a recognized standardization body.

The Article 29 Working Party has always followed with great interest the developments concerning standardisation in the data protection field. In its opinion 1/2002[86] „on the CEN/ISSS Report on Privacy Standardisation in Europe"**,** the Working *Party „takes note of the work undertaken by CEN/ISSS in the field of privacy standardisation in Europe2 and, in particular, of the recently published final report*[87] *reviewing the possible role of standardisation in realising privacy and data protection in accordance with Directive 95/46/EC (…).The CEN/ISSS report and, if followed up, some of its recommendations, could also assist the Data Protection Authorities in raising the awareness of industry and citizens and promoting public debate in the field of data protection. Other recommendations could help providing practical solutions to controllers and helping them therefore to comply with the obligations arising from the data protection directive".*

---

own staff. However, the implementation of PETs in the Commissions' ICT applications depends on the availability of the corresponding products and will have to be evaluated on a case by case basis, in line with the application's development cycle.

84 A consistent strategy should be adopted to raise consumer awareness of the risks involved in processing their data and of the solutions that PETs may provide as a complement to the existing systems of remedies contained in data protection legislation. The Commission intends to launch a series of EU-wide awareness-raising activities on PETs. The main responsibility for conducting this activity falls within the realm of national data protection authorities which already have relevant experience in this area. The Commission calls on them to increase their awareness-raising activities to include information on PETs through all possible means within their reach. The Commission **also** urges the Article 29 Working Party to coordinate national practice in a coherent work plan for awareness-raising on PETs and to serve as a meeting point for the sharing of good practice already in place at national level. In particular, consumer associations and other players such as the Consumer Centres Network (ECC-Net), in its role as an EU-wide network to advise citizens on their rights as consumers, could become partners in the quest to educate consumers.

85 The take-up and use of PETs could be encouraged if the presence of these technologies in a certain product and its basic features are easily recognizable. For that purpose, the Commission intends to investigate the feasibility of an EU-wide system of privacy seals, which would also include an economic and societal impact analysis. The purpose of such privacy seals would be to ensure consumers can easily identify a certain product as ensuring or enhancing data protection rules in the processing of data, in particular by incorporating appropriate PETs.

86 Article 29 Working Group Opinion 1/2002 on the CEN/ISSS Report on Privacy Standardisation in Europe, W.P. 57, May 30, 2002.

87 Initiative on Privacy Standardisation in Europe. Final Report. CEN/ISSS Secretariat. 13.2.2002., available at http://ec.europa.eu/enterprise/ict/policy/standards/ipse_finalreport.pdf

In 2004, at the 26th International Conference of Privacy and personal data protection, held at Krakow, the final resolution emphasised the need for Data Protection Commissioners to work jointly with standardisation organisations to develop privacy related technical and organisational standards

Moreover, as already mentioned, Article 14 of the Directive 2002/58/EC states that, where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary way, of protecting personal data from the risks of unlawful processing -risks that have been created by the new technological options. The reference to the standardization process as a way to develop technical norms able to better the enforcement of the privacy requirements' respect is present in different opinions of the Art. 29 W.Group (see particularly the RFID opinion[88] already quoted)

2.3 Enforcement measures

2.3.1 Public authority

The Directives 95/46/EC and 2002/58/EC require both a data protection authority with appropriate powers to supervise the information privacy principles, and individual (no class action) rights of enforcement before judicial authorities (criminal but also commercial (through unfair competition) and civil jurisdictions) with certain facilities as regards the *onus probandi* and the taking into account of pure moral damages. The European enforcement mechanisms are therefore quite strong.

Powers of the supervisory authorities

One or more public authorities must be responsible for monitoring the application of the Directives ('supervisory authority') (Art. 28 Dir 95/46). The supervisory authorities must *„act with complete independence"*, and must have investigative powers, *„effective powers of intervention"* in processing, and powers to take court action where national legislation implementing the Directives is infringed (Art. 28(3) Dir 95/46). They must be consulted concerning legislation affecting privacy (Art. 28(2) Dir 95/46). They must be able to hear complaints concerning breaches of information privacy (Art. 24(4) Dir 95/46), but nothing is specified concerning the remedies available from a supervisory authority. In certain countries (like e.g. France or Germany) they have the possibility to deliver injunction and administrative penalties. The declaration of this W.G. dated from the 25th of Nov 2004 about the enforcement of the DP Directive provisions and national legislation by the different national DPA. Describe the different initiatives taken by each national state as regards the enforcement of its data protection legislation.

---

88 Working document on data protection issues related to RFID technology, WP 105, January 2005

On 25 November 2004[89], the Working Party adopted the declaration on enforcement which summarises the outcome of the discussions on enforcement at the subgroup level and at the plenary, and announces joint enforcement actions for 2005-2006 based on criteria contained in this document. The concept is defined by the Working Party as follows: „In a broader sense, enforcement could be understood as any action leading to better compliance, including awareness raising activities and the development of guidance. In a narrower sense, enforcement means the undertaking of investigative actions, or even solely the imposition of sanctions".

A first initiative already mentioned definitively is the „Opinion on more harmonised information Provisions", that was adopted on the same day aiming at simplifying and harmonising the requirements on companies to inform the citizens about the processing of their data. The Working Party in its opinion stressed how important it is to establish a common approach for a pragmatic solution, which should give a practical added value for the implementation of the general principles of the Directive towards developing more harmonised information provisions. The Working Party endorsed the principle that a fair processing notice does not need to be contained in a single document. Instead – so long as the sum total meets legal requirements – there could be up to three layers of information provided to citizens. The main aim of these first actions is to increase the awareness of the citizens about their rights and in the same time of the Data controllers about their duties[90].

A second initiative was the call for reinforcing the role of data protection officials nominated within the Data Controllers organizations. „A broader use of data protection officials as a substitute to notification duties, at least with regard to certain industry sectors and/or in respect of larger organisations including those in the public sector, would be useful in view of the positive findings reported by the Member States in which these data protection officials have been already introduced or have existed traditionally."[91]. The main purpose is to introduce directly at the Data controllers level a prior checking of their processing activities compliance with the Data Protection Directive requirements. In other words, the Data Protection Authorities are searching for „allies" directly incorporated within the Data controllers organisations and to develop by the cooperation between these data protection officials nominated in the same sector of activities, ex-

---

89 Declaration of the Art. 29 W.P. on enforcement adopted the 24th of November 2004, W.P. 101

90 „The Working Party is of the view that awareness raising activities, the provision of guidance and advice to both data subjects and data controllers, the promotion of codes of conduct, etc, are no doubt important means for achieving compliance. The data protection authorities agree that there can be a relationship between a low level of knowledge of their rights among data subjects and compliance. A better knowledge of rights can enhance data protection awareness in society". About the importance of this awareness for a better implementation of the Data Protection legislation, see our comments in „ Mieux sensibiliser les personnes concernées - Les rendre acteurs de leur propre protection", Proceedings of the Prague Conference organized by the Council of Europe, published notably in Droit de l'immatériel, Revue Lamy, Mai 2005, p. 47 and ff.

91 Article 29 Working Party report on the obligation to notify the national supervisory authorities, the best use of exceptions and simplification and the role of the data protection officers in the European Union, adopted on 18 January 2005, W.P. 106.

changes of best practices and more appropriate and specific implementation of the data protection legislative provisions.

Enforcement means also the possibility for investigating, detecting and sanctioning the infringements in case of non compliance with the data Protection requirements. On that point, Art. 29 W.P. pleads for a reinforcement of the means of action of the national D.P.A authorities but also for synchronized national efforts in direction of specific sector of activities. „An EU wide, synchronized national enforcement actions would entail co-ordinated national ex officio investigations taking place in a certain period of time, focused at similar national processing and based on questionnaires agreed at EU level…The aim of such synchronized actions will primarily be to analyse whether and how the rules are being complied with in the sector, and, if necessary, the issuing of further recommendations…. The implementation of the recommendations issued after these investigations will be monitored and, if necessary, sanctions could be imposed according to national laws"[92].

Finally, in its recent strategy programme[93], the Art. 29 W.P. has decided to increased its cooperative efforts to support a more coherent and consistent implementation of the Data Protection Directive by launching a wide synchronized investigation on certain cases or sectors of activities. In March 2006 this resulted in the launching of a first EU wide investigation about the data protection practices in the private Healthcare Insurance sector[94].

Individual rights of enforcement

Article 22 of Directive 95/46 provides that an individual must have rights to seek a judicial remedy for any breach of the national law. In Belgium, for example, several remedies are provided by the law of 8 December 1992 „on the protection of personal data":

---

92 Declaration of the Article 29 Working Party on Enforcement, adopted on 25th November 2004, W.P.101.

93 „Co-operation among data protection authorities is highly desirable, both in their daily operations and as part of the planning of joint actions, and must be a prominent component of any strategic plan or policy. Several instruments are now in place to foster practical and efficient co-operation among European data protection authorities and are current examples of this commitment:
- The biannual workshop on complaints handling and its Internet Network for exchange of information and handling trans-national cases
- The regular and informal exchange of information among the different DPAs in the form of questions and answers relating to the law and practice in every Member State
- The recent setting up of an on-line IT experts network
- The provisions for joint work that can be found in the document on Binding Corporate Rules,
- The work on simplification of the notification of personal data processing for companies established in several Member States
- The meetings and the leadership of the group of the national authorities involved with the enforcement of Community measures relating to unsolicited commercial communications or 'spam'

Finally, there is a strong will on the part of all the Data Protection Authorities of the Working Party to promptly answer any question or to fulfil any request of co-operation received from any other such Authority of another Member State to the greatest extent possible within its powers and competences

94 See, on the initiatives to increase the effectiveness of the D.P. directive's provisions, infra Point IV.

- the court may order that the judgement shall be published in full or by excerpt in one or more newspapers (Art. 40);
- the judge may pronounce the confiscation of the carriers of personal data to which the offence relates, such as manual filing systems, magnetic discs or tapes, except for the computers or any other equipment, or order the erasure of such data (Art. 41, §1);
- the judge may pronounce the interdiction to manage any processing of personal data, directly or through an agent, for a period up to two years (Art. 41, §2);
- In case of recidivism, the judge may pronounce an imprisonment of three months to two years (Art. 41, §3)

Furthermore, the Directive provides for a right to recover compensatory damages (Art. 23), but it appears that this can be provided as either a judicial or administrative remedy. Dissuasive penalties for breach are also required (Art. 24). In Belgium, for example, penalties range between 500 and 500.000 Euro.

2.3.2 Private litigation

ADR or ODR systems even if their creation is encouraged by the European Commission and in certain cases are financed in the context of EU programme (see ECODIR and CCFORM) are still in their infancy. Till now it does not seem that any ADR has been in position to solve a litigation in the Privacy field.

2.4 Effectiveness

As no stakeholder input about Europe was collected by the research team in the context of the present study, we base our considerations as regards effectiveness of the various measures on previous work and current research.

2.4.1 Effectiveness of legal and regulatory measures

a. Effectiveness of Directive 95/46/EC

Awareness

According to the results of a 2003 Eurobarometer[95], on average, in 2003, 60% of all EU citizens were concerned to a greater or lesser degree, about the broad issue of the pro-

95 Two Eurobarometer surveys on data protection awareness in the European Union were carried out in autumn 2003. The first one polls the European Union citizens about their views on privacy (Special

tection of privacy. Nevertheless, on average, more than two-thirds of EU citizens (70%) tended to agree that awareness of personal data protection in their home country was low and only 46% tended to agree that that the level of personal data protection provided by their law was high.

It is also interesting to note that two-thirds (64%) of the EU citizens polled tended to agree that they were worried about leaving personal information on the Internet. However, one-third of those polled (34%) did not know whether their national legislation could cope with the growing number of people leaving personal information on the Internet.

On average, only 32% of EU citizens had heard of laws granting individuals access to personal data held by others and the right to correct or remove data which are inaccurate or have been obtained unlawfully. The 32% of the total poll who had heard of this right were then asked whether they had ever exercised it. Only a very small percentage had done so and the average figure across the EU was only 7% of this sample.

On average, 42% of EU citizens had heard that those collecting personal information are obliged to provide individuals with certain information such as their identity and the purpose of the data. The half of the EU citizens (49%) was aware about the right to object to the use of personal information for the purpose of direct marketing (opt-out). On average, across the European Union, 49% of citizens had heard of the need to provide agreement for someone to use their personal information and their right to oppose some uses compared with the 42% who had not heard of this.

In 2007, a „E-Communications household" survey[96] was conducted by the European Commission. In that context, all respondents were asked[97] whether they would like to be informed if their personal data was lost, stolen or altered. According to the results, 64% of respondents would like to be informed under all circumstances and 14% in case there was a risk of a financial loss. Only 12% indicate that they would not like to be informed. These data tend to confirm the results of 2003 according to which, on average, 60% of all EU citizens are concerned to a greater or lesser degree, about the issue of the protection of privacy.

Eurobarometer 196) and the second one polls the European Union companies' views about privacy (Flash Eurobarometer EB 147). These are available at: http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm#actions

96 The results of a special Eurobarometer survey conducted by TNS Opinion & Social between 17 November 2006 and 19 December 2006 to measure the attitude of European households and individuals towards fixed and mobile telephony, Internet access, TV broadcast services, bundled offers, 112 emergency call number, telephone directories, privacy and security. The survey covers the 27 EU Member States together with Candidate countries (Croatia and Turkey) and the Turkish Cypriot Community, with an average of 1.000 households interviewed per country. It follows on from the previous Eurobarometer survey that was conducted between December 2005 and January 2006.

97 The question that was asked is the following: „Companies like telecom providers collect personal data such as name, address and credit card details.In case any of your personal data was lost, stolen or altered in any way, would you like to be informed or not?"

Effectiveness

According to the results of the 2003 Eurobarometer, a clear majority of Data Controllers throughout the European Union rate the level of protection offered by their respective national data protection laws as 'medium'. Moreover, a majority of respondents believe the existing legislation on data protection is unsuited to cope with the increasing amount of personal information being exchanged.

According to that Eurobarometer, 48% of the Data controllers polled made available to data subjects when personal data is collected the information consisting in „the existence of the right to access and the right to rectify the data concerning the data subjects". Moreover, although it seems as an important requirement, only one third of companies inform data subjects of the purposes of the processing before collecting their personal data. 38% indicate that the information concerning the recipients or categories of recipients of the data is made available to data subjects. Only 37% of companies reveal the physical or electronic address of a person within the organisation directly responsible for data protection matters to data subjects when their personal data is collected. Only 37% indicate the identity of the data controller or its representative.

As for the companies' experience of access requests and complaints, a relative majority of respondents indicate that their company received less than ten access requests during the year 2002 and the vast majority of companies had not received any complaints from people whose data is being processed.

b. Effectiveness of Directive 2002/58/EC

No information yet about the effectiveness of Directive 2002/58/EC

2.4.2 Effectiveness of arrangements other than law and regulation

a. General position

The Strategic review of better regulation in the European Union[98] presented by the European Commission in November 2006[99] shows that real and substantial progress has been achieved regarding a better regulation and sets out plans for taking the process forward.

It is however remarkable that the document does not mention progress regarding self- and co-regulation. The 'regulation' part of the 2003 Inter-institutional Agreement seems

98 Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52006DC0689:EN:NOT

99 Communication from the Commission to the Council, the European Parliament, the European economic and social Committee and the Committee of the Regions; A strategic review of better regulation in the European Union, 14 November 2006, COM(2006) 689 final.

not to be part of the first high level priorities for making better regulation. The next steps are indeed oriented towards a simplification of legislation, reducing administrative burden, Impact assessments, Screening and Withdrawal of pending proposals, Transposition and application of EU Law, and Codification and Repeal[100].

b. Codes of Conduct

In practical terms the procedure foreseen for promoting European Codes of conduct, with approval from the Article 29 Working Group[101], has been rarely followed even though clearly encouraged by the European Commission. Up to now, only two codes of conduct have been approved in that context[102] and, at national level, big disparities have been noticed. If the Netherlands, Italy and United Kingdom have been proactive, in other countries only a few codes of conduct have been enacted and these in sectors already heavily regulated (health, banking and insurance)[103].

Thereby, some existent alternative regulation systems (e.g. trustmarks/labelling), though they can already help to enhance confidence in e-commerce, are still in their infancy. As regards trustmarks, clear distortions exist as regards the critical criteria they should fulfil to be actually effective.

c. PETs

As the results of a 2003 Eurobarometer[104] show, the level of awareness of citizens as regards the use of PETs was low four years ago: *„72% of EU citizens had never heard of these tools or technologies. In Greece, the figure rises to 81% while in more computer-literate Sweden the figure is only 58%. The 18% of the total poll who had heard about these tools but had never used them were then asked why. The first two most cited reasons were based upon concerns over technology. The prime reason cited by 30% of this group was that they would not know how to use them. This was the situation affecting 35% of Greeks and 34% of Germans, Spaniards and Italians in contrast to only 16% of the Irish. A second technological reason concerned the inability to install them on a computer and was quoted by 21% of the poll. Lack of concern about basic privacy issues was cited by 20% of the EU sample. Lack of conviction that this type of software would actually work was the most cited reason by Luxemburgish (24%) compared with only 12% of Austrians. Cost was not a major deterring factor and was only cited by 6% of those polled."*

---

100 Chapter IV of the Communication of 14 November 2006, *op.cit.*

101 See above the details on the procedure set down in WP13

102 See above the explanation on the FEDMA and the IATA Codes

103 Yves Poullet, „EU data protection policy : The Directive 95/46 ten years after*", Computer Law and Security Report,* Elsevier, 2006, p.5

104 See the two Eurobarometer surveys published by the Internal Market Directorate and available on europa.euintlcomm/justice_home/fsj/privacy/. The first (Special Eurobarometer 196, September 2003) focuses on the views of European citizens, the second (Flash Eurobarometer 147, September 2003), on those of businesses.

However, since 2003, the level of awareness of the citizens as regards PETs is raising year after year. Indeed, according to the results of the 2007' „E-Communications household" survey[105], 81% of respondents had installed antivirus programs while 60% had antispam software in their computer.

As for the level of awareness of companies, it was not much better in 2003 as the one of the citizens. Indeed*, „results show that a clear majority, representing 66% of respondents in the European Union, do not use any such technologies or software products to enhance privacy protection of databases. It is interesting to note that among these respondents, 28% have not even heard of such technology. The use of Privacy Enhancing Technologies is more widespread in the industry and services sectors, with respectively 35% and 36% of respondents expressing this usage. These technologies prove to be more of need to the biggest companies than the smallest (20-49 employees). In fact, the small-sized companies have a significantly lower rate of respondents who indicate that they use such technologies, at 29%. 12 percentage points separate this category from the two others mentioned above."*

As regards companies, more recent results are not yet available.

d. Conclusion

In Europe, we are still in the infancy of alternative regulation mechanisms. This, however, does not mean it is an impossible dream make true. The current actual effectiveness of self-regulation is a myth in the sense that the mechanisms need to reach maturity before being able to compete with the traditional regulation systems. These mechanisms should therefore be continuously encouraged by both the authorities and the stakeholders.

2.4.3 Effectiveness of enforcement mechanisms

According to the results of the aforementioned Euro barometer, the level of knowledge about the existence of independent data protection authorities was low across the European Union in 2003 and two-thirds (68%) of EU citizens were not aware of their existence. Furthermore as previously said, a relative majority of the companies polled indicate that their company received less than ten access requests during the year 2002 and the vast majority of companies had not received any complaints from people whose data is being processed.

---

105 The results of a special Eurobarometer survey conducted by TNS Opinion & Social between 17 November 2006 and 19 December 2006 to measure the attitude of European households and individuals towards fixed and mobile telephony, Internet access, TV broadcast services, bundled offers, 112 emergency call number, telephone directories, privacy and security. The survey covers the 27 EU Member States together with Candidate countries (Croatia and Turkey) and the Turkish Cypriot Community, with an average of 1.000 households interviewed per country. It follows on from the previous Eurobarometer survey that was conducted between December 2005 and January 2006.

Moreover, in the First report[106] on the implementation of the Data Protection Directive (95/46/EC), the European Commission reviewed the general level of compliance with data protection law in the EU and the related question of enforcement. Although national situations vary, the European Commission noted the presence of three interrelated phenomena:

- An under-resourced enforcement effort and supervisory authorities with a wide range of tasks, among which enforcement actions have a rather low priority;
- Very patchy compliance by data controllers, no doubt reluctant to undertake changes in their existing practices to comply with what may seem complex and burdensome rules, when the risks of getting caught seem low;
- An apparently low level of knowledge of their rights among data subjects, which may be at the root of the previous phenomenon.

For these reasons, the Article 29 Working Party has considered the role of enforcement in the enhancement of compliance with data protection legislation by data controllers. Enforcement is one of the various activities undertaken by national data protection authorities to ensure compliance. In its „Strategy Document", adopted on 29 September 2004(WP 98), the Working Party stated that the promotion of harmonised compliance is a strategic and permanent goal of the Working Party. It also stated that it is convinced of the necessity of moving forward in the direction of promoting better compliance with data protection laws throughout the European Union and that, in this respect; it will make a joint effort to improve the situation.

In its Working Paper n°101[107], the Article 29 Working Party expressed the view that awareness raising activities, the provision of guidance and advice to both data subjects and data controllers, the promotion of codes of conduct, etc, are no doubt important means for achieving compliance. A better knowledge of rights can enhance data protection awareness in society. Nevertheless, additionally, enforcement actions in a narrower sense, including the imposition of sanctions, are also a necessary, and often last resort, means to ensure compliance. By applying enforcement and sanctions, data protection authorities discourage non-compliance with the law and encourage those who effectively comply to continue doing so. The Article 29 Working Party believes that enforcement is an important instrument in the compliance „toolbox", and it therefore, aims to contribute to a more pro-active stance towards enforcement of data protection legislation within the European Union.

---

106 First report on the implementation of the Data Protection Directive (95/46/EC) of 15 May 2003 COM (2003) 265 final. Available at http://europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf

107 Working Party document WP 101 „Declaration of the Article 29 Working Party on Enforcement", adopted on 25 November 2004

In the same Working Paper, the Article 29 Working Party has decided to exchange best practices, discuss enforcement strategies that can be applied nationally and across countries, and to investigate possibilities for the preparation of EU wide, synchronized national enforcement actions in the Member States.

3 The United States

3.1 Summary

The U.S. is characterized by the absence of a framework approach as exists in Europe. The wealth of specific privacy provisions contained in law, implementing rules and regulations, self regulatory and co-regulatory schemes and measures that organizations take on their own initiative via the use of technologies, internal codes of conduct and other measures all contribute to a complex environment for the protection of the confidentiality of communications. Industry respondents commented that a 'vigorous' environment for privacy protection existed in the United States. Having said that, one of the significant criticisms levelled against the U.S. approach is that there is little opportunity for the individual to directly launch complaints against those responsible for managing personal data transmitted over electronic communication networks. This must be done by organizations acting on behalf of the consumer. In practice it comes down to either the Federal Trade Commission (FTC) or the Federal Communications Commission (FCC) or one of the very active consumer advocacy groups such as the Electronic Privacy Information Center (EPIC) or the Electronic Frontier Foundation (EFF) acting on behalf of the aggrieved consumer to 'guide behaviour' of organisations.

Privacy protections in the United States come from a variety of sources. Although the Federal Constitution does not contain any specific protections for privacy, rights have been derived primarily from Constitutional provisions against search and seizure and against self-incrimination.[108] By contrast, at the state level, some states such as California have explicit state constitutional rights to privacy to govern areas within state jurisdiction.[109] In the U.S. legal system, jurisdiction over the protection of personal information is divided between the federal and state governments. Under the U.S. Constitution, the interstate commerce clause[110] gives the federal government the authority to regulate economic activities, including electronic communications services that cross state lines. When federal law exists, the supremacy clause of the U.S. Constitution provides that the federal rules take precedence over state law.[111] If the federal government has not acted and the U.S. Constitution does not otherwise restrict the states, states may provide statutory protections.

On both the federal and state levels, the protection of privacy and security of electronic communications and services relies heavily on statutory and self-regulatory mechanisms. In effect, the most significant rights come from targeted statutes and implement-

---

108 U.S. Const. Amend. IV (« The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. ») ; U.S. Const. Amend. V (« No person shall … be compelled in any criminal case to be a witness against himself … . »).

109 C.A. CONST. Art. 1, §3(b)(3).

110 U.S. Const., Art. I, § 8

111 U.S. Const., Art. VI, § 2

ing regulations. The interplay between federal and state law is often complex with respect to privacy because of this approach. Where the federal government targets protections narrowly, states are free to regulate other aspects of privacy. Often with respect to privacy legislation, the federal government expressly waives the supremacy of federal rules by indicating that the federal law is a floor rather than a ceiling on protection.[112]

One cost of working with such a fragmented legal framework is that there are many gaps that may not be filled with individual bits of legislation. Rules tend to be narrowly tailored for specific activities by particular types of parties and are often the result of a high profile public controversy.[113] Hence, there are important distinctions in legislation addressing government actions and legislation addressing conduct by private parties. For consumer privacy, different laws relate to health records,[114] financial institutions,[115] data maintained by telecommunication service providers,[116] cable communications viewing patterns,[117] and even personal data associated with digital rights management („DRM").[118] This piecemeal treatment of individual privacy can lead to important anomalies: for instance, cable service providers are regulated differently from Internet service providers, and stored electronic communications receive different treatment from real-time communication services.[119]

The U.S. reactive approach is reflected in the response to the problem of email spam. The U.S. CAN-SPAM Act sought to reduce spam, as has the European ePrivacy Directive, but both have had mixed results.[120] In its nature, spam is an international problem that cannot be solved in a single country or region. A notable difference between the U.S. and the European Union's approach to spam is the use in the U.S. of more liberal opt-out provisions, in contrast with European opt-in arrangements.[121] The U.S. framework relies heavily on industry and technological solutions to reduce the level of spam.

The recent proliferation of data security breach notification laws at the state level and litigation related to spyware, adware and DRM technologies reflect deepening concerns

---

112 See e.g. Fair Credit Reporting Act, 15 U.S.C. 1681t ; Financial Services Modernization Act, 15 U.S.C. 6807

113 *See e.g.* Video Privacy Protection Act, 18 U.S.C. 2710. *See also* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 47 HASTINGS L. J. 877 (2003).

114 Health Insurance Portability and Accountability Act («HIPPA »), 45 C.F.R. §§ 160-64.

115 Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422 ; Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et. seq. ; Gramm-Leach Bliley Act, 15 U.S.C. §§ 6801-6809.

116 Telecommunications Act of 1996, 47 U.S.C. § 222.

117 Cable Communications Policy Act of 1984, 47 U.S.C. §551.

118 Digital Millenium Copyright Act, 17 U.S.C. §1201.

119 *See* infra.

120 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701, et. seq. ; Council Directive 2002/58, art. 13, 2002 (EC) (addresses « unsolicited communications. »).

121 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701, et. seq. ; Council Directive 2002/58, art. 13, 2002 (EC) (addresses « unsolicited communications. »).

over privacy and trust in electronic communications with respect to industry.[122] This concern is heightened by the problems of applying targeted laws to new situations and is compounded because the fragmented approach translates to a complex set of enforcement mechanisms with varying degrees of strength. Some statutory measures include specific penalties and both private and public enforcement.[123] Others do not include penalties and do not create any specific enforcement capabilities.[124] At the same time, legal measures unrelated to privacy, like the statutory prohibitions on „unfair and deceptive trade practices" can be applied by enforcement agencies to protect privacy.[125] For example, in the case of „unfair and deceptive practices," the Federal Trade Commission has enforcement authority and has pursued claims against online service providers who do not follow their publicly disclosed privacy policies.[126] The U.S. places an important emphasis on this means of enforcing privacy policies.

At the same time that concerns arise with respect to industry, the controversies over the legality of newly disclosed telecommunications surveillance by the U.S. government show that privacy and trust are also undergoing great strains with respect to the public sector. The legal standards for law enforcement access to personal information varies across the different statutes. In Europe, lawful intercept is a particularly significant area and a matter of national rather than European competence. Data retention (of traffic and location data, but not content), however, has been addressed at the European level. In the U.S., laws such as ECPA and CALEA treat call-identifying information differently from content. In any case, the topic of lawful intercept affects the trust that users have in electronic network and service providers, especially in light of recent developments with respect to the application of CALEA to Internet services.[127]

Taken as a whole, the U.S. has been less willing than Europe to impose regulations regarding privacy on electronic communications. The U.S., as in many other areas, places greater reliance on market forces and on self-regulation than on conventional regulation.

3.2 Legal and regulatory measures to enhance privacy and trust

In the U.S. system, legal measures protecting electronic communications privacy are usually not designed specifically to enhance public trust in electronic communications. Rights against interception of communications by third-parties, for example, target privacy and confidentiality rather than trustworthiness itself. Trust-building is, however, an important secondary effect.

---

122 *See e.g.* Video Privacy Protection Act, 18 U.S.C. 2710. *See also* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 47 HASTINGS L. J. 877 (2003).
123 *See* Fair Credit Reporting Act, 15 U.S.C. §§ 1681 et. seq.
124 *See* Gramm-Leach Bliley Act, 15 U.S.C. §§ 6801-6809.
125 Federal Trade Commission Act, 15 USC § 45(a).
126 Federal Trade Commission Act, 15 U.S.C. §§ 41-58.
127 Communications Assistance for Law Enforcement Act of 1994, Pub. L. No 103-414.

By contrast, non-privacy related statutes related to data transmissions can strive to improve public trust. The most notable statutes of this type are the state data breach notification laws.[128] These statutes do not impose substantive privacy standards, but rather require public notification of data security breaches. The objective is to inform consumers when their personal information has been improperly released so that consumers can be more vigilant against identity theft. One of the goals is to improve public trust in the treatment of personal information by providing transparency to those companies that breach trust.

Because of the fragmented nature of U.S. regulation and the complexity of data practices, the actual legal obligations for privacy that apply vary according to each of the different actors: communications service providers, network providers and manufacturers/software producers.

This report identifies the key statutes and their coverage for these actors as follows:

- Electronics Communication Privacy Act (« ECPA »)

This statute has three key parts - wiretapping, stored communications and pen register provisions - that affect the privacy of electronic communications. The wiretap provisions apply to service providers and network providers.[129] The main goal of these provisions is to protect the confidentiality of electronic communications while in transit by prohibiting the interception of the contents of any wire, electronic or oral communications.[130] This part of ECPA seeks to assure private individuals of the confidentiality of their communications and specifically protects private communications from government surveillance without a court order. It also prevents third parties from accessing communications without consent, and electronic communication providers from acting outside of the ordinary course of business.[131]

The stored communications provisions address service providers and protect the confidentiality of communications which are stored in an electronic format.[132] These provisions prohibit the acquisition of the contents of communications after transmission while they are in storage. The focus of these provisions is to secure the privacy of electronic messages and recordings against intrusions principally from the government. In general, for state actors to access stored communications, they must obtain a court order, or the approval of a grand jury. However, in the case of public security matters, provid-

---

128 *See e.g.* DE. CODE ANN. Tit. 6, § 12B-102 (2005); CAL. CIV. CODE § 1798.82 (2003) ; N.Y. GEN. BUS. LAW § 899-aa (McKinney 2005) ; 815 ILL. COMP. STAT. 530-12 (2006) ; UTAH CODE ANN. § 13-44-102 (2007).
129 18 U.S.C. §§ 2510-2522.
130 18 U.S.C. § 2510.
131 18 U.S.C. § 2511(2)(a).
132 18 U.S.C. §§ 2701-2711.

ers must comply with a request for information made by designated officers of the FBI.[133]

Lastly, the pen register provisions, apply principally to network providers, and prohibit the use of a pen register or trap and trace device to record dialling and routing information of electronic communications.[134] This seeks to assure the confidentiality of parties to a communication because state actors must obtain a court order in order to have a pen register or a trap and trace device installed by a provider, and private actors may only use such a device pursuant to an exception. These few exceptions include when the device is used by a communication service in the ordinary course of its business, or when there is consent by one of the party's to the communication.[135] The private party exception is critical for some services such as calling line identification.

The level of confidentiality and trust assured by ECPA is reduced by the USA PATRIOT Act.[136] The USA PATRIOT Act lowered the thresholds for obtaining legal access by law enforcement to electronic communications. This has allowed law enforcement to more efficiently and effectively to search the records of individuals purportedly involved in terrorist or other clandestine intelligence activities. In addition, law enforcement is given a layer of protection from public scrutiny, because in the context of « national security letters », recipients may not disclose that law enforcement is seeking or has obtained the information. There is, however, evidence of systemic abuse of the procedural safeguards by law enforcement and, for citizens, the lowered thresholds authorized by the USA PATRIOT Act – a lowered level of authority, and evidentiary standard – have led to the extensive use of NSLs, which appear to seriously undermine an individual's security in their acts.[137]

- Telecommunications Act of 1996

The Telecommunications Act of 1996 tries to protect the privacy of subscribers' personal information associated with telecommunications services such as call detail information and billing data because network providers have special access to sensitive personal information.[138] The requirements apply to „telecommunications carriers," i.e. network providers. The statute covers the use of customers' proprietary network information („CPNI") that is defined as „information that relates to the quantity, technical configuration, type destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and … information contained in the bills pertaining to telephone exchange service

---

133 18 U.S.C. § 2709(a).
134 18 U.S.C. §§ 3121-3127.
135 18 U.S.C. § 3121.
136 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (« USA-PATRIOT ») Act of 2001, Pub. L. No. 107-56.
137 *See* A Review of the Federal Bureau of Investigation's Use of National Security Letters (Dep't of Justice March 9, 2007), http://www.usdoj.gov/oig/new.htm.
138 Telecommunications Act of 1996, 47 U.S.C. §§ 101, et. seq.

or telephone toll service received by a customer of a carrier."[139] The law requires customer approval for the disclosure of CPNI. While the FCC tried through implementing regulations to make the „approval" an opt-in, a federal court of appeals rejected that approach and the FCC shifted to an „opt-out".[140] Subscriber information that is necessary to provide a bill to the customer or to protect the rights and property of the carrier are exempt from the limitations imposed by the statute. Similarly, information necessary for public safety emergency services such as 911 calls are exempt.

This modest protection for CPNI strives to protect privacy and enhance trust for telecommunications transaction data.

- Telephone Records and Privacy Protection Act of 2006 (« TRPPA »)

The TRPPA was enacted in response to the HP spy scandal and criminalized the fraudulent acquisition or unauthorized disclosure of telephone subscribers' phone records.[141] The statute applies to telecommunication service providers, but does not apply to law enforcement agents acting with lawful authorization to conduct investigative, protective or intelligence activities. TRPPA prohibits „pre-texting," the activity „whereby a data broker or other person represents that they are an authorized consumer and convinces an agent of the telephone company to release the data," and prohibits selling, transferring or purchasing confidential telephone records. By re-enforcing the confidentiality of telephone records, TRPPA seeks to promote the privacy of subscriber records. Recent regulations issued by the Federal Communications Commission also require that telecommunication service providers protect access to customer records with passwords and that breaches be notified to the customer as wells as law enforcement.[142]

- Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (« CAN-SPAM Act »)

The CAN-SPAM Act seeks to promote trust and privacy in electronic messaging and applies essentially to communications service providers to protect users and internet service providers from unsolicited commercial email messages known as spam.[143] Because ISPs' systems were overloaded with spam and users were frustrated by an inundation of unsolicited and unwanted messages, the statute strives to protect the integrity of email as a useful means of communications. The CAN-SPAM Act regulates the senders of unsolicited commercial email and establishes national standards for the

---

139 47 U.S.C. § 222(h)(1).
140 *See U.S. West v. Fed. Commc'n Comm'n*, 182 F.3d 1224 (CA10 1999).
141 Telephone Records and Privacy Protection Act of 2006 („TRPPA"), 18 U.S.C. § 1, et. seq., 109 Pub. L. No. 476. *See also*, H.P Before a Skeptical Congress, N.Y. TIMES, Sept. 29, 2006, at C1.
142 See Final Order 07-22, FTC Docket 96-115 (April 2, 2007) (regulations issued under Telecommunications Act of 1996)
143 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM), 15 U.S.C. §§ 7701, et. seq.

identification of unsolicited commercial messages.[144] Specifically, the statute bans false or misleading header information, prohibits deceptive subject lines, requires that recipients have an opt-out to future messages, and requires that commercial email be identified as an advertisement including a valid physical postal address for the sender.[145] Rather than regulating the messages themselves, this approach regulates the transparency of commercial email and facilitates technology-based filtering of spam messages by service providers and users. The statute does not regulate spam sent from other countries.

- State Data Breach Notification Laws

At the state level, a large number of statutes have recently been enacted that require organizations processing personal information to issue notifications if personal information on clients has been lost or improperly released to third-parties.[146] Among the actors in electronic communications, the notification obligations apply principally to communications service providers and content providers that own or license personal information.[147] These obligations vary according to the specific states. Some require notification directly to affected individuals once data has been improperly released, others only require notice if there is a sufficient risk of identity theft resulting from the improper disclosure. Some states require notice to a government agency. Essentially, the goal of these statutes is to enhance trust in electronic communications. By imposing an obligation of notification, the statutes create transparency in the management of personal information databases. Transparency increases the sense of control of the data subject.

Moreover, the notification requirement enhances the security of personal information databases by the procedures adopted by organizations. Organizations do not want the adverse publicity and loss of trust that results from a data breach notification. In addition, they do not want to incur the cost of notification and potential liability. As a result, business entities must focus more carefully on information security. However, at present, a major recent survey shows that companies are largely ignoring compliance with these laws. [148]

- Computer Assistance for Law Enforcement Act (« CALEA »)

CALEA is designed to allow the government to monitor communications for law enforcement purposes rather than to protect privacy.[149] The statute was enacted to respond to the concern that digital and wireless communications made it more difficult for law enforcement agencies to execute authorized electronic surveillance activities.

---

144 15 U.S.C § 7703.
145 15 U.S.C § 7703.
146 *See* DE. CODE ANN. Tit. 6, § 12B-102 (2005); CAL. CIV. CODE § 1798.82 (2003) ; N.Y. GEN. BUS. LAW § 899-aa (McKinney 2005) ; 815 ILL. COMP. STAT. 530-12 (2006) ; UTAH CODE ANN. § 13-44-102 (2007).
147 See N.Y. Gen. Bus. L. 899-aa(2)
148 Robert Westervelt, Survey: *Companies disregard data security breach risks*, ComputerWeekly.com, May 25, 2007 (« 46% of those surveyed said their businesses didn't implement encryption solutions on portable devices even after suffering a data breach. »)
149 Communications Assistance for Law Enforcement Act of 1994 (CALEA), 18 U.S.C. §§ 101, et. seq.

CALEA requires that telecommunications carriers ensure that law enforcement can intercept all wire and electronic communications and access call-identifying information at a location other than the carrier's premises.[150] The statute thus applies to network providers and to equipment manufacturers. More recently, the FCC ruled that facilities-based broadband internet access and interconnected VoIP providers are covered by CALEA.[151] Notably absent from the ambit of CALEA are information service providers such as email messaging services and private networks.

From a privacy perspective, CALEA reduces trust in electronic communications. By facilitating the government's capability to intercept communications, CALEA reduces the privacy of electronic communications users even though the underlying authority to intercept communications remains unchanged by CALEA. Nevertheless, from a national security and law enforcement perspective, CALEA can enhance trust in electronic communications. Since technological developments made wiretapping difficult for law enforcement agencies, CALEA preserves law enforcement's ability to conduct electronic surveillance of criminal activities in the electronic communication sector. In other words, this statue is designed to prevent criminals from using advanced electronic communications as a means to escape detection.

- Children's Online Privacy Protection Act (COPPA)

COPPA prohibits the collection, use or disclosure of personal information over the Internet from persons under the age of 13 without verifiable parental consent in order to protect young children from the risks associated with using the Internet.[152] The Act is directed at the operators of Internet sites and services intended for those children.[153] The operator of such a website is required to provide notice to parents of the collection of personal information, the purposes for the data collection and the statute allows parents to access the stored information and refuse future use of their children's personal information.[154] COPPA also prohibits websites from requiring the release of children's information as a condition to participation in an online activity.

COPPA contains a particularly interesting feature that links statutory protections with self-regulation. COPPA provides for a safe harbour that authorizes the Federal Trade Commission to approve trade association guidelines for the collection of information from children.[155] To obtain approval, the self-regulatory guidelines must comply with the protections afforded by COPPA and must be published for public comment. Once ap-

---

150 18 U.S.C. § 103(a).

151 *Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, RM-10865 (2006).

152 Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501-06. *See generally* Implementing the Children's Online Privacy Protection Act – A Report to Congress (Fed. Trade Comm'n, Feb. 2007), www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

153 15 U.S.C. § 6502.

154 15 U.S.C. § 6502.

155 15 U.S.C. § 6503(a).

proved, website operators that follow the guidelines are „deemed" to be in compliance with the statutory requirements and will not be liable for violations.[156]

From a privacy perspective, these protections address content providers offering services over the Internet to children. COPPA goes to great lengths to protect the personal information of minors who will be unaware of the implications of disclosure, yet does so with a flexible mechanism that promotes industry self-regulation.

3.3 Arrangements other than law and regulation

3.3.1 Self and co-regulation

The Direct Marketing Association (DMA) self regulatory Code of Conduct governs the activities of transmission of electronic messages by its members. Other codes of conduct exist for other sectors. The two main labelling schemes highlighted by a number of respondents are TRUSTe and BBBOnline.

TRUSTe is an independent, non-profit organisation enabling trust based on privacy for personal information on the internet. It was funded by The Electronic Frontier Foundation (EFF) and the CommerceNet Consortium. TRUSTe was established to certify and monitor web site privacy and email policies, monitor practices, and resolve consumer privacy problems. Currently there are 2940 websites participating. The fee for a TRUSTe seal varies between $599-25,000. It is a global system, but appears to have achieved greatest acceptance in the U.S. and in Japan.

The seal is Safe Harbour certified, and has a specific kid's seal. TRUSTe is different from BBOnLine in that TRUSTe does not require opt-in.

The steps towards acquisition of the TRUSTe seal are: the completion of the online application (including a self assessment the submission of the privacy policy for review), web site audit and review to make sure the website is in compliance with TRUSTe standards, the awarding of the TRUSTe's seals for display on your web site, and the ongoing monitoring and dispute resolution (websites are automatically and manually reviewed and TRUSTe performs surprise checks). TRUSTe also facilitates alternative dispute resolutions in case consumer complaints are filed. If a website fails the review an escalated investigation is conduct; depending on the severity of the breach, the investigation can lead to an on-site compliance review by a CPA firm, or the revocation of the site's trust mark license. To date, however, TRUSTe has only revoked 1 trust mark from all its participating web sites.[157] Extreme violations could in principle be referred to the appropriate law authority (e.g. in the U.S.: attorney general's office, Federal Trade

---

156 15 U.S.C. § 6503(b).
157 See TRUSTe Fact Sheet, http://www.truste.org/about/fact_sheet.php (visited June 17, 2007)

Commission, Consumer Protection Agency); however, this appears to rarely happen in practice.

Better Business Bureau's OnLine Privacy programme (BBBOnLine Privacy program) was developed to support business websites in addressing key concern of online shoppers in respect to the use of their personal data. Currently 714 web sites are covered by the BBBOnLine Privacy seal, and (depending on total annual sales) fees range from $200-7,000. The seal is available for companies based in the U.S., Canada and Japan, and is Safe Harbour certified. The steps towards the BBBOnLine Privacy Seal are: adoption and posting of an online privacy policy; completion of a business application and the Privacy Profile. These documents and the website are then reviewed by BBBOnLine to ensure compliance with program requirements.

If a company initially fails to meet the standards BBBOnLine indicates which changes have to be adopted within 60 days to guarantee compliance and awards the seal after adoption of these changes. The initial awarding of the seal is followed by annual reviews and in case of complaints, surprise checks.

BBB also awards a specific Kid's Privacy seal which was developed to help companies comply with COPPA (Children's Online Privacy Protection Act).

The use of Binding Corporate Rules (BCRs) and Inter Company Agreements (ICAs) has been referenced a number of times by industry stakeholders and knowledgeable observers. BCRs take the idea of a model contract forward and seeks to make them usable with a multinational company that transfers data outside the EU. They are set up as an alternative to the EU Safe Harbour regime to allow the transfer of personal data outside the EEA. This is a relatively new method where a multinational organisation can have the adequacy of their procedures assessed in the context of the EU Directive by an 'entry point data protection authority'. The assessment would reflect the multinational organisation's policies, procedures, training and any other aspects of business activities that affect how it deals with privacy and personal information. The process is lengthy, and can take up to two years to obtain approval (and according to some take six to nine months to set up within an organisation).[158] They have yet to be proven as a viable alternative; for example one interview respondent noted that so far in the UK only two multi-national companies have had their BCRs approved. Nonetheless, there is great interest in this approach. Following approval by the 'entry point data protection authority' the business is then allowed to transfer data outside the EEA. For U.S. organisations, their European HQ (if applicable) would be appointed as lead data protection authority for the business. The relevant data protection authority then distributes documentation to each regulator where the company operates requesting approval. The process of obtaining this approval was seen by the industry stakeholders whom we consulted as the equivalent to a full „privacy audit" inasmuch as there are a number of steps that

158 Binding Corporate Rules ; Transferring data out of the EEA http://www.marketingimprovement.com/hotnews/freestanding/bcr.html

must be taken, including co-ordination with the relevant authorities, establishment of internal appropriate codes of conduct matching the negotiated requirements, and verification, all as part of the regular internal organisation audit cycle.

Additionally telecommunications providers use Inter Company Agreements based on standard contractual clauses from the International Chamber of Commerce (ICC) to signify whether a company entity has adequate measures. This is signed by entities in the organisation and indicates which systems are transferring data to the United States and how this data is dealt with and managed.

Although it was the view from industry experts and some market players interviewed that companies will only take action when the law requires them to do, a number felt that the increasing visibility of privacy issues meant that they had to be seen to be doing more. Customers of telecommunications companies both in the Business to Business (B2B) and the Business to Consumer (B2C) domain were asking more and more questions regarding how the company protects personally sensitive information and the growth of media concern (particularly for Identity Theft and security breaches) was driving some, but not all companies to take these measures more seriously. This groundswell manifested itself in the creation of internal globally acceptable codes of conduct (covering internal controls and ethics across the organisation), the establishment in the bigger companies of the role of Chief Privacy Officer (no longer an obscure job title in the Fortune 500 companies) and other measures such as inclusion of privacy concerns in the annual audit process. The codes of conduct covered practices governing the management of privacy information for consumers and employees and in some cases were applicable across the organization's operations globally. These were monitored via internal controls, self-assessments, internal audits and (in the case of organisations participating in trans-border data flows with the EU, for example) via the previously mentioned ICAs and eventually BCRs.

Additionally, the FTC has indicated publicly that in respect to certain areas e.g. spyware, industry must lead in the implementation of self-regulatory regimes and the development of new technologies.[159]

3.3.2 PETS

Among our survey respondents, there was broad agreement that PETs are a useful development. However the overriding view was that the time for this technology had not yet come. The benefits of developing technology that provides for the better protection of personal data transmitted over electronic communications networks instead of taking a 'security-centric', reactive approach which is driven by either media or consumer concern (e.g. with regard to identity theft) or legal requirements has not yet been made

---

159 Remarks of Deborah Platt Majoras, Chairman, Federal Trade Commission, to the Anti-Spyware Coalition, February 9, 2006 available at : http://www.ftc.gov/speeches/majoras/060209cdtspyware.pdf

clear. One respondent commented that it would be better if businesses could find ways of marketing products and services without the use of personally identifiable information.

A majority of respondents felt that the market for PETs was not visible enough. The business case was viewed as being insufficient to drive implementation of PETs in the private or public sectors. The Platform for Privacy Preferences (P3P) does not appear to be widely used – only one respondent had implemented it. Although open standards present in some PETs were thought to reduce barriers, one respondent felt that the use of security measures still presented a barrier as use of open standard-based PETs was not widespread.

Suggestions as to how to make their market more visible focused on elaborating how PETs might be useful in a risk based approach to the management of information assets.

Respondents indicated that the market for information security products and services was quite active. The use of such technology is dependent upon the size of company. Many respondents indicated the difficulty of conducting a Return on Investment (RoI) calculation for technologies that enhance privacy and trust. One respondent commented that the smaller the organisation, the less clear the RoI.

3.3.3 Standardization

Awareness of ISO 17799 and 27001 is high but only in larger companies and perhaps only those that have to trade internationally (particularly with Europe). However, even in larger companies not all of the organization is accredited.

Efforts to develop privacy-protective standards for web sites such as the Platform for Privacy Preferences (P3P) have been unsuccessful. Industry development tends to be slow and adoption is very limited.

3.4 Enforcement measures

Legal mechanisms provide two types of enforcement powers against private enterprises. Where the law creates private rights of action to remedy legal violations, individuals may sue private enterprises for transgressing the corresponding privacy rights. However, the value of these enforcement powers is often undermined by two critical factors. First, courts may be reluctant to award damages for data privacy offences in the absence of monetary harm; and second, the cost of litigation is frequently significant,

particularly compared to any possible recoveries.[160] This is supported by the views of consumer advocacy groups, most notably EPIC which recognises that whilst the law may provide for redress by a citizen against a private enterprise, it is often difficult for individual citizens to act on this in a meaningful manner.

Where the law creates civil and punitive remedies, public agencies may also enforce the corresponding violations. The most relevant public agencies are government prosecutors, the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC). Each of these public agencies, however, has discretion regarding the pursuit of an action against a private enterprise for the violation of statutory privacy rights. Thus, violations may go without any redress for victims. For example, the FTC only pursues a small fraction of violations each year. During the last 5 years, the FTC brought only 11 actions for impermissible collection of personal information on the Internet from children.[161] The action against the social networking site Xanga.com for illegally collecting information from 1, 700,000 children resulted in a fine of U.S.$1m. While this was the largest civil penalty ever obtained under the COPPA, it represented less than $ 0.60 per child victim. Similarly, there had been 10 law enforcement actions pursued by the FTC against the distribution of spyware in the last two years.

3.4.1 Public authority

With respect to public enforcement, these key statutes may provide for civil and criminal penalties as follows:

- ECPA

For unlawful interceptions of electronic communications by third-parties, ECPA provides civil and criminal penalties that may be enforced by government prosecutors.[162] Similarly, the provisions protecting stored electronic communications may be enforced by government prosecutors. Lastly, for unlawful use of a pen register or trap and trace device to record traffic information, government prosecutors may bring criminal charges.

- Telecommunications Act of 1996

The law authorizes the FCC to enforce the privacy provisions of the statute through civil fines.[163]

---

160 *See* Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies*, 54 HASTINGS L. J. 877, at 896-97 (2006).

161 *See* Fed. Trade Comm'n Report to Congress on Implementing the Children's Online Privacy Protection Act, 16 (Feb. 2007), www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf.

162 18 U.S.C. § 2520.

163 47 U.S.C. §§ 401-16.

- TRPPA

The law provides for criminal penalties and authorizes public prosecution. Penalties are increased if the TRPPA is violated in conjunction with other illegal activity.[164]

- CAN-SPAM Act

The statute provides for civil fines and imprisonment for violations.[165] The law authorizes the FTC and state enforcement agencies to bring civil claims and authorizes the U.S. Department of Justice to bring criminal proceedings against violators.[166] As of May 2006, the FTC reports delays of more than a year in investigation of CAN-SPAM Act complaints, and the rate of compliance for unsolicited email is estimated at less than 0.5% in 2006.

- CALEA

The law and its implementing regulations are enforced by the U.S. Department of Justice.[167] If a telecommunications carrier has not complied with the equipment requirements of CALEA, the carrier will be unable to comply with a court-ordered surveillance order. Civil penalties for failure to respect a court surveillance order may reach $10,000 per day. Telecommunications carriers may, however, avail themselves of the safe harbour provisions in CALEA. If a carrier complies with industry standards or publicly available technical requirements, then the carrier cannot be liable for technical obstacles to compliance with a particular surveillance order.

- Data Breach Notification Laws

Under state data breach notification laws, the state attorney general would typically be authorized to file a civil action against offenders. For example, the California statutes provide that the California Attorney General may bring a civil suit on behalf of its citizens in the event of a data breach.[168]

- Children's Online Privacy Protection Act (COPPA)

The FTC may bring an action for violations of COPPA under its authority to take enforcement actions against „unfair and deceptive practices."[169] State attorneys general may take enforcement actions against violations of COPPA.[170] Civil damages and injunctive relief are available.

---

164 18 U.S.C. § 1039.
165 15 U.S.C. § 7706.
166 15 U.S.C § 7703.
167 *Communications Assistance for Law Enforcement Act and Broadband Access and Services, Second Report and Order and Memorandum Opinion and Order*, ET Docket No. 04-295, RM-10865 (2006).
168 CAL. CIV. CODE §§ 1798.80 -1798.84.
169 15 U.S.C. § 6505. *See* Federal Trade Comm'n Act, 15 U.S.C. 41 et seq.
170 Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6504(a)(1).

3.4.2 Private litigation

With respect to private rights of action, key statutes offer the following enforcement options:

- ECPA

In the case of unlawful interception of communications by third-parties, ECPA provides civil relief (including preliminary, equitable and declaratory relief) plus reasonable attorney's fees and costs to any person whose rights under the statute are violated.[171] An important caveat is that one party to the communication may consent to the interception and disclosure of the contents of the communication even if the other party is unaware.[172] For unlawful acquisition of stored communications, ECPA provides civil penalties and permits any aggrieved person to bring a civil claim in federal court. [173] For the collection of traffic information through the unlawful use of a pen register or trap and trace device, there is no private damage claim — only a criminal action. In the context of a criminal proceeding brought against a defendant that is based in part on information collected in violation of ECPA, the defendant may have the information suppressed from consideration in the trial.

- Telecommunications Act of 1996

The statute does not provide for private rights of action against the unlawful disclosure of CPNI, and courts have rejected private law suits to enforce the statute.[174] Thus, only public enforcement possibilities exist through the Federal Communications Commission or through state utility commissions.

- CAN-SPAM Act

This law does not provide any private right of action for recipients of email sent in violation of the statute. However, the CAN-SPAM Act does create a private right of action for Internet service providers whose systems are used by spammers in violation of CAN-SPAM.

- TRPPA

There is no private enforcement for the anti-pretexting rights created by this statute. Even though the law does not create any explicit data privacy rights or enforcement remedies, it may still be possible to police data practices through the creative use of existing legislation. For example, the principal federal consumer protection law, the Federal Trade Commission Act, prohibits „unfair and deceptive trade practices", and the Federal Trade Commission has enforcement powers under the statute. Although the

---

171 18 U.S.C. §§ 2520-21.
172 *Id*. at § 2511(2)(c).
173 *Id*. at § 2701(b) and § 2710(c).
174 *See Conboy v. AT&T Universal Card Servs. Corp.*, 84 F. Supp. 2d 492 (S.D.N.Y., 2000).

statute does not create privacy rights, the FTC interprets deviations by companies from their publicly noticed privacy policies as „unfair and deceptive", and has brought actions against a few companies for their data practices.[175]

- Data Breach Notification Laws

State data breach notification laws may include private enforcement remedies. For example, California was the first state to enact data breach notification laws, and as such many other states model their laws under this state's model. Under California law if an organization fails to encrypt personal information, such as a name, social security or driver's license number, or financial account or access information, and fails to notify the person of a data breach, then the organization may face civil liability for any actual damages and attorney fees.[176] Injured parties seeking monetary damages and/or an injunction are permitted to file private civil actions in California.

Respondents indicated that they felt that although a very complex and superficially effective set of laws exist for the protection of personal data transmitted over electronic communications networks, in actual fact there is a perception by privacy advocates that there is an absence of meaningful oversight or enforcement for the consumer.

3.5 Effectiveness

3.5.1 Effectiveness of legal and regulatory measures

One respondent compared the efficacy of different approaches in Europe and the United States. In Europe, there is a large amount of legislation and it can be said that data protection and privacy are highly regulated by law. However, this may not necessarily mean that organizations abide by such extensive legislation. Indeed, because of the black and white nature of the law, the respondent felt that it is more likely that organizations play lip-service to the law, knowing that the capacity for enforcement is limited. By comparison, in the United States, where private litigation seems to be the preferred method of managing privacy and data protection, organizations may be more willing to 'keep to the rules' due to the deterrent effect of large legal battles (fostered in part by the extensive market for company legal services). It is not clear that the effectiveness of private litigation as a constraint on behaviour is really as great as this respondent felt. In practice, individuals face great obstacles to litigating privacy violations and suits are infrequent.[177]

---

175 *See e.g. In re GeoCities*, F.T.C. Docket 98-23051 (Aug. 13, 1998).
176 CAL. CIV. CODE §§ 1798.80 -1798.84.
177 See Joel R. Reidenberg, Privacy Wrongs in Search of Remedies, 47 Hastings L. J. 877 (2003).

Although data protection and privacy law is split across sectors, the culture of the United States in terms private litigation means that if companies do not abide by these instruments there is a perceived capacity to deal with the matter via fines and injunctions.

There have been 26 law enforcement actions since 1997 against companies and individuals engaging in deceptive and unfair practices relating to the distribution of spam, 8 of which were in the last fiscal year.. In total, according to its Annual Report, the FTC has launched 89 law enforcement actions against 241 companies and individuals engaging in deceptive and unfair practices related to spam and in particular the failure to properly label pornographic messages.[178]

The FTC currently has some 3.5 m records in its Consumer Sentinel database covering fraud and identity theft.[179]

The FTC's investigative action generally comes from analysis of trends in its consumer sentinel database, media stories and cases brought to its attention by other organisations (e.g. EPIC).

With respect to privacy policies, the perception of one respondent was that fines for rulings awarded under the FTC regulations can run into the millions of dollars. This perception is not, however, supported by actual FTC privacy case settlements. To the contrary, there have only been 19 true privacy cases that the FTC concluded on „unfair and deceptive practices" over the last 8 years. None of these cases went to court. All were settlements. Of the settlements, only three included any financial redress and, of those, only one involved a fine. When the internet service provider „Vision 1" sold the personal information of almost one million consumers in breach of its privacy promises, the company settled with the FTC by relinquishing the U.S. $9,101.63 in fees it made from renting the consumer information.[180] Similarly, when Gateway Learning, despite a pledge to keep information private, rented customer information, the company settled with the FTC by disgorging the U.S.$4,608 it earned.[181] The only case to include payment of a civil penalty involved ChoicePoint. As a result of data breaches at ChoicePoint, more than 160,000 people were acknowledged by ChoicePoint to have suffered the compromise of their personal information and at least 800 individuals were victims of identity theft as a result of the ChoicePoint breach. The company agreed to pay U.S.$10 million in civil penalties as well as U.S.$5 million in consumer redress.[182] The remaining 16

---

178 Federal Trade Commission (2007) The FTC in 2007: A Champion for Consumers and Competition, p 31, available at: http://www.ftc.gov/os/2007/04/ChairmansReport2007.pdf

179 ibid

180 Agreement Containing Consent Order, In the Matter of Vision I Properties, LLC FTC File No. 0423160 (Mar. 10, 2005), available at http://www.ftc.gov/os/caselist/0423068/050310agree0423068.pdf.

181 Agreement Containing Consent Order, *In re Gateway Learning Corp.*, File No. 042-3047, available at http:// www.ftc.gov/os/caselist/0423047/040707agree0423047.pdf.

182 Stipulation, *U.S. v. ChoicePoint Inc.*, Civ. No. 1-06-CV-0198 9 (Jan. 26, 2006), available at http://ftc.gov/os/caselist/choicepoint/0523069stip.pdf. *See also*, ChoicePoint settles with 43 states, D.C. over data breach, Assoc. Press, May 31, 2007, available at http://www.siliconvalley.com/news/ci_6029567 (ChoicePoint agrees to specific security measures as a settlement with state Attorneys General.)

cases brought by the FTC only resulted in promises of practices changes by the companies. In other words, the claims about the FTC's powerful enforcement role may reflect perception more than reality.

FTC enforcement may be more vigorous where clear statutory rights exist to protect children. Even so, in the last seven years, the FTC has only brought 12 cases under the Children's Online Privacy Protection Act. These cases typically involve the illegal collection of personal information from children under the age of 13 where the web sites knew that the users were young children. However, unlike the „unfair and deceptive practices" settlements, each of these child-victim cases included civil penalties. The median penalty was $35,000 and the largest penalty of U.S. $1 million was assessed against Xanga.com for violating the privacy of 1.7 million children (i.e. a penalty amount that was less than U.S.$ 0.60 per victim)[183]

Public enforcement by any of the authorities faces a number of important obstacles. The Federal Trade Commission is one of the lead agencies for consumer protection. Yet the budget appropriation for the agency to pursue both its consumer protection mission and its anti-trust enforcement mission in 2008 is only U.S.$24m. In 2007 there were 92 staff working on consumer issues out of a total of 569. The number of staff working on these issues has increased, but they are responsible for all consumer protection matters and not just privacy. In addition, Congress is threatening the FTC with a loss of funding in the FY2008 appropriation because the FTC has, on the rare occasions as noted above, fined companies for privacy violations.[184] Typically, instead of prosecution, the FTC runs a number of awareness and public education campaigns, including the OnGuard online campaign (a website with 3.5m visitors since September 2005) and the distribution of identity theft training kits. The FTC exhorts industry to implement self-regulatory regimes, particularly in the area of spam, spy-ware and malicious code.

Industry representatives recognize that the work of government agencies is characterised by limited funding.

A number of sector specific legal measures with their accompanying implementation rules require the creation of privacy notices or following other measures. These include instruments in the healthcare industry (the Health Insurance Portability Accountability Act) and the financial area (Title V of the Gramm-Leach Bliley Act) Although not concerned with telecommunications, the privacy notice requirements contained within such legislation are relevant as they require companies to address privacy measures (e.g. establishment of privacy policies) and the privacy notices are often available through organizational web sites.

---

183 See FTC Privacy Initiatives Children's Privacy Enforcement, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html (visited June 12, 2007)

184 See U.S. Congress, H.Rep. 110-207 on H.R. 2829 Financial Services and General Government Appropriations Bill of 2008, pp. 60-61, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_reports&docid=f:hr207.110.pdf

3.5.2 Effectiveness of Arrangements other than law and regulation

Unsurprisingly, there are divergent views about the effectiveness of self-regulatory instruments. Respondents' interpretations of the effectiveness of these instruments varied from the view that they were generally useful, to the view that privacy labels in particular gave companies an excuse not to bother with protecting customers' privacy. Self regulatory measures would need to be backed up by strong legislation. Some respondents' views indicate that self-regulatory measures are having some effect in the absence of black and white law, given the size of the country, the size of the e-Commerce market and other contributing factors. However, the experience of weak implementation of self-regulatory approaches like the US-EU Safe Harbour[185] indicate that such measures are unlikely to work effectively without the backing of legal sanctions.

Codes of practice based on sector distinctions do exist. One such example is the Direct Marketing Association Code of Conduct for Members („DMA"). However, upon a breach of this code, the only form of action available to the DMA is removal of the offending member from the Association. There is no evidence that the DMA has ever expelled a member for violating consumer privacy. Similarly, a recent analysis by a prominent computer security expert of web sites certified by TRUSTe reports that the TRUSTe sites are more than twice as likely to be untrustworthy.[186]

The market for self-regulatory instruments is thought to be worth around US$400-US$500m, largely dominated by Secure Sockets Layer (SSL) digital certificates provided by Verisign. TRUSTe is also present but its use is dominated by one online service provider. However, at least two of the respondents considered that lawyers and litigation could be considered as part of the self-regulatory regime; therefore the market could be as much as US$1bn. If the creation of the role of Chief Privacy Officer (perhaps US$150,000 per role) is included, then the market for self-regulatory instruments is clearly above US$1bn.

When considering the size of the market, it is important to make a distinction between the size of the market implied by the number of e-commerce sites using privacy labels (in which case it is very low) and the volume of e-commerce sales (in which case it is high). What this means is that the market for privacy labels is significant amongst those sites that account for the most e-Commerce sales.

There are different views as to whether self-regulatory instruments provide an added value for those companies implementing them. One respondent felt that the presence of a code of conduct or privacy seal would not make a difference to a consumer, but another indicated that a magic conversion rate of 15% existed (an estimate of the in-

---

185 See Jan Dhont, Maria Veronica Perez Asinari, Yves Poullet, Joel R. Reidenberg & Lee A. Bygrave, Safe Harbor Decision Implementation Study, Eur. Comm'n Internal Market DG Contract No. PRS/2003/A0-7002/E/27 (19 April 2004)

186 See Ben Edelman, Certifications and Site Trustworthiness, http://www.benedelman.org/news/092506-1.html (Sept. 25, 2006)

creased value to a consumer, based on a study completed for a large ISP). The benefits also flow through to Alternative Dispute Resolution mechanisms and thus to increased trust.

A question over the participation in self-regulatory systems, particularly labelling schemes was also raised. One respondent commented that in some cases a large company with a significant brand name would see no added value for the participation in a labelling scheme because the company was more well known that the label itself. This did not prevent the organisation from participating, apparently because the organisation felt that doing so was a way of showing leadership in its industry sector.

So in this respect, labels could be seen as more useful to small and medium sized organisations that can trade off the trust that the label represents. However, these companies are of course the ones more likely, because of their size and limited resource, to have difficulties in maintaining compliance with labelling schemes.

Awareness of certain standards which may help to protect Personal Information and Sensitive Personal Information is relatively high amongst the market. In particular, the ISO standard No 27001 (*Information technology -- Security techniques -- Information security management systems -- Requirements*) is very widely cited. However, despite awareness of this popular set of best practice being high, a limited number of companies are undertaking accreditation, presumably due to the costs of accreditation and the perceived lack of sufficient of benefit. Often, a large company undertakes accreditation only for certain parts of the organization.

As to labelling schemes, there are different views on the effectiveness of these instruments. Organizations like EPIC that work on behalf of the consumer consider that they provide no real benefit and simply act as another way, like privacy policies, for companies to do what they want. Recent research suggests that consumers will pay more for products when privacy policies are clearly disclosed.[187] However, no data is available to indicate whether the existence of a policy means that the companies are actually implementing those policies to protect consumer information.

Privacy policies of the sort that appear on websites are seen by some as providing an excuse, indicating to the prospective consumer the approach of the organisation towards the management of personal information but not giving the consumer any recourse. These are seen by consumer groups as not giving consumers the ability to make meaningful choices as to privacy policies or representations. The same concern was levelled against the Platform for Privacy Preferences (P3P), in that it was simply a way to get consumers to consent to disclosing their data, whereas what is needed are techniques that ‘minimise or eliminate the collection of personally identifiable information’.

---

187 The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study (June 2007) http://weis2007.econinfosec.org/papers/57.pdf

Another criticism described when discussing whether arrangements to enhance privacy and trust are effective is the issue of metrics. Specifically, respondents were concerned about the lack of robust data to make informed cost / benefit assessments. One commercial organisation interviewed had not undertaken any quantitative assessments but instead relied upon quantitative data from subject matter experts. Another indicated that no formal cost/benefit was done but that the organisation tried to do as best it could regardless of the amount of investment required because of the high profile of the organisation. The lack of common data was a recurring theme across many stakeholders from government and industry. The views of EPIC were that the downstream costs of the misuse of personal data can only increase over time and therefore investment in technologies to reduce these costs will be well spent. Even large multinational market players such as IBM and Verizon had not undertaken any formal cost/benefit due to lack of data. The question of how much is privacy worth and 'how much privacy is enough' will continue to perplex industry and academia for some time.

The difficulty of translating benefits to the end user was cited – the previously cited absence of useful security metrics meant that it was very difficult for companies to follow the investment into measures like PETs into better privacy for customers.

3.5.3 Effectiveness of enforcement measures

Fines and sanctions are seen as being important to enforce legal rights. Industry views these fines to be appropriate and to provide a useful level of deterrent. Those groups acting on behalf of consumers feel that they do not represent enough of a deterrent – a company would be prepared to accept the fines as they are not sufficient to match the scope of the of the benefit to the company of violating privacy. More than one respondent indicated that companies focus on the legal and public relations aspects of the protection of personally sensitive information, and not enough on 'building in' privacy protection.

The lack of sufficient recourse to private redress was cited by many respondents as being an example of one of the inefficiencies in the enforcement of the law. Some respondents agreed that it was difficult for an individual to obtain quick and easy help. The fact that it is typically the FTC that pursues cases on behalf of the consumer (and even then mostly via the use of a statute not explicitly intended to cover breaches of privacy), and the limited ability in practice for consumers to pursue their own claims, support the view of some respondents that organisations may not be under sufficient pressure to maintain individual privacy. Instead, consumers are forced to rely upon trust that organisations will comply with the relevant laws and adhere to their own self imposed privacy practices and codes of conduct. In some circumstances, the organisations take this responsibility very seriously, and particularly where doing so is seen to be of direct value (for example, where it is important for the organisation to be viewed as being trusted or competent in a sensitive area such as healthcare or financial data).

However, in other cases, and especially with smaller organisations (where funding for privacy programmes is likely to be extremely limited), the organisation may be less fastidious in its privacy practices, and the aggrieved consumer may be left to rely upon a federal agency to pursue a claim on his or her behalf.

The TRUSTe labelling scheme was seen to be the most effective, allowing the consumer to simply review the compliance of a site. Similarly, BBBOnline has been actively promoting its privacy seal under a general campaign of consumer awareness. Although awareness of the TRUSTe seal is high. some privacy experts doubt the effectiveness of TRUSTe enforcement; since its inception in 1997, TRUSTe investigated 2951 complaints, yet only one company has ever been terminated from the programme.

4 Japan

The concept of privacy gained legal definition and popular currency in Japan in the late 1950s and early 1960s, largely as a result of a privacy lawsuit brought in 1961 by the politician Hachiro Arita against the well-known author Yukio Mishima. In 1964, the Tokyo District Court, ruling on the case, gave the first recognition of privacy as a right protected by Japanese law. According to the Court, that right consisted of „the legal right and assurance that one's private life will not be unreasonably disclosed to the public". Article 13 of the 1946 Constitution, referring to the right to pursue „happiness", is regarded as the constitutional basis for the protection of privacy.

In 1981, the Administrative Management Agency's Research Committee on the Protection of Privacy recommended the passage of a national data protection law based on fair information principles. Seven years later, in 1988, the Diet passed the Act for the Protection of Computer-Processed Personal Data Held by Administrative Organs, which set out rules for the handling of personal data in the national public sector.

Some individual laws were passed during the 1980s and 1990s that included provisions protecting certain types of personal data handled by the private sector (such as financial and credit data, and employee data), though many of these laws did not include punitive provisions for mishandling of data. Aside from these sector-specific legal provisions, the Japanese Government's primary focus remained on fostering industry self-regulation.

To this end, the Government sponsored influential best-practice guidelines for the private sector, such as the Ministry of International Trade and Industry's influential 1989 Guidelines for the Protection of Computer-Processed Personal Data in the Private Sector, the 1987 Guidelines on the Protection of Personal Data for Financial Institutions of the Center for Financial Industry Information Systems (FISC), approved by the Ministry of Finance. The Ministry of Posts and Telecommunications (MPT) produced additional, sector-specific guidelines. These guidelines were all modelled on the OECD Guidelines.

Between 1989 and 1999, a number of organizations associated with Government ministries also issued guidelines and formulated other compliance measures. Foremost among these was the Japan Information Processing Development Corporation (JIPDEC). JIPDEC established the „System for Granting Marks of Confidence for Privacy and Personal Data Protection," through which businesses may become certified as compliant with a set of personal data handling guidelines based on JIS (Japan Industrial Standard) Q15001 of 1999. Certified businesses may use the JIPDEC Privacy Mark (similar to a privacy seal) on letterheads, advertising, websites and other forms of publicity. In addition to JIPDEC, the Electronic Commerce Promotion Council (ECOM) was active in formulating and publishing guidelines. The group's members include some of Japan's largest companies, as well as major multinationals. ECOM issued Guidelines Concerning the Protection of Personal Data in Electronic Commerce in the Private Sector in 1998, and followed up with a Personal Data Protection Guide in 2002.

In 1999, a Basic Resident Registers Act was passed requiring all Japanese citizens and resident aliens to register basic personal information in a new computerized nationwide Resident Registry Network System known as Juki-Net. Juki-Net's implementation has been controversial. The system met with strong resistance from many citizens, and some local governments refused to connect to the network. While largely accepted and operational today, some local governments still refuse to connect to the system over concerns for security of personal information.

While the national Government emphasized self-regulation, a body of data protection law covering the private sector as a whole did develop during the 1990s at the local level through the passage of local data protection ordinances. These ordinances varied in their scope and coverage, with some limited to the municipal public sector or to computer data processing, and others drafted in „omnibus" form – covering all sectors and types of processing unless specifically excluded.

On May 30, 2003, the Japanese Diet ratified the „Act on the Protection of Personal Information". A good part of the impetus on this legislation came from the need to comply with the European Union's restrictions on the export of personal information from Europe arising from the Data Protection Directive of 1995. With the passage of this Act, and its coming into effect in April 2005, the government accomplished its objective of supporting the exchange of information by establishing a rather broad framework with one piece of legislation covering all sectors of the economy.

In its sections applying to the private sector, the Act protects *individuals* by regulating the use of *personal information* in *personal information databases* by private sector businesses (known as *entities handling personal information*). Therefore, the Act enumerates several fair information principles. The Act also provides that the Ministry responsible for each industry sector will draft working „Guidelines" and then work with the relevant industry association to formulate standards for practical application. These Guidelines are often vague enough to leave the Ministries latitude to respond on a case-by-case basis.

Unlike many European countries, there is no data protection or privacy commissioner providing central oversight. Allowing Ministries to respond as cases occur in industries under their purview has created a fragmented sectoral approach to the implementation of data and privacy protection.

However, given the very broad scope of the Act, situations will arise in which the application of its provisions to a specific industry sector or type of information will be unclear. Given the „hybrid" nature of the Act, it is highly likely that the Government will move to formulate sector- or information-specific regulations or even additional sector- or information-specific laws. Further rulemaking is likely to affect personal information handling in the telecommunications, personal credit, health and employment contexts – areas in which supplementary data protection rulemaking is common worldwide.

4.1 Measures to enhance privacy and trust

Privacy is not defined as such in the Japanese legal environment although historically a number of court decisions were made in order to protect the nature of privacy. Personal information had been subject to regulation in some areas, such as telecommunications, but it took the introduction of the Act on the Protection of Personal Information in 2003 for the protection of personal information to be respected across all industry sectors and the nation.

The following subsections describe the legal environment on the protection of privacy and personal information.

4.1.1 Constitutional clauses on privacy and personal information protection

Privacy as a self-determination right is construed by a number of articles in the Constitution of Japan, such as Articles 13[188], 19[189], 21 (2)[190], 23[191], 31[192], 33[193], 35[194] and 38 (1)[195]. This aspect of privacy is not restricted to the privacy of information. However, there is no statutory provision of privacy in Japan, and currently no rule-making is in order to legislate privacy.

In practice, Article 13 of the Constitution (right to pursue happiness), provisions on defamation or contempt in the Criminal Law and provisions on tort in the Civil Law are referred to in order to consider cases of privacy infringement.

Although recent legislation on the protection of personal information in both public and private sectors deal with the protection of „personal information", the scope of these acts do not extend to privacy as such. Of course privacy will be ensured in the course of the protection of personal information.

As part of Article 21, the Constitution of Japan also guarantees the secrecy of communication. The article states, „Freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed. (2) No censorship shall be

---

188 Article 13 articulates that all of the people shall be respected as individuals. Their right to life, liberty, and the pursuit of happiness shall be the supreme consideration in legislation unless it does not interfere with the public welfare.

189 Article 19 guarantees that freedom of thought and conscience shall not be violated.

190 Article 21 (2) stipulates that no censorship shall be maintained, nor shall the secrecy of any means of communication be violated.

191 Article 23 articulates that academic freedom is guaranteed.

192 Article 31 stipulates that no person shall be deprived of life or liberty, nor shall any other criminal penalty be imposed, except according to procedure established by law.

193 Article 33 articulates that no person shall be apprehended except upon warrant issued by a competent judicial officer.

194 Article 35 stipulates that the right of all persons to be secure in their homes, papers and effects against entries, searches and seizures shall not be impaired except upon warrant issued for adequate cause.

195 Article 38 (1) stipulates that no person shall be compelled to testify against himself.

maintained, nor shall the secrecy of any means of communication be violated.“ However, this constitutional clause is not considered to provide an overall basis for protecting privacy in general because the secrecy of communication is to be imposed on the government not private entities.

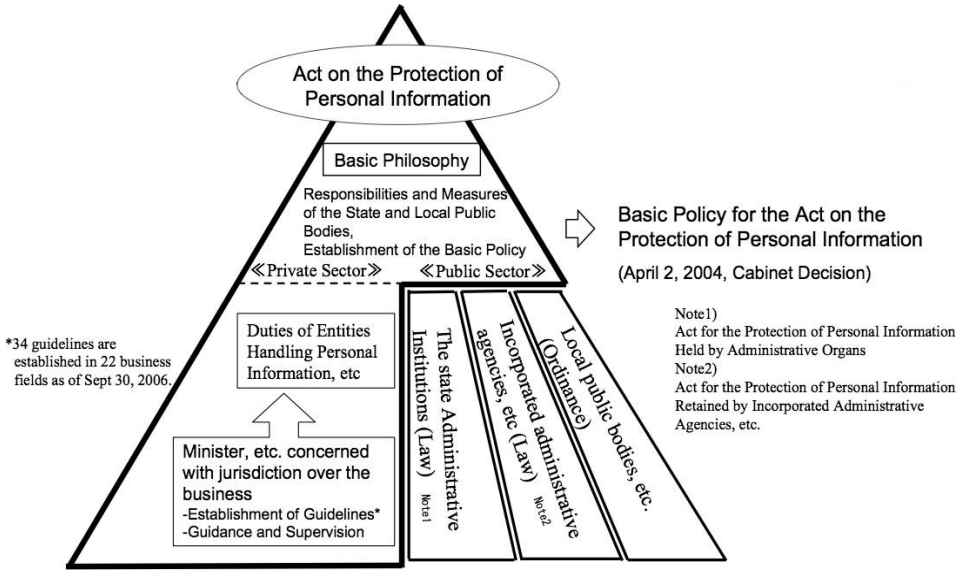
4.1.2 Legislation on the Protection of Personal Information

The recent legislation on the protection of personal information is built on several acts, cabinet orders and ministerial guidelines.

The Act on the Protection of Personal Information, which was enacted in 2003 and took effect in 2005, lays out the basic policy on the protection of personal information and the responsibilities and measures that the state and local governments may take. The duties that private entities should observe in processing personal information are also prescribed in the Act, while those that the government and semi-public entities, or Incorporated Administrative Agencies (IAA’s), may should adhere to are prescribed in the Act on Protection of Personal Information Held by Administrative Organs and the Act Protection of Personal Information Held by Incorporated Administrative Agencies, respectively.

The framework is illustrated in Figure 1, which follows.

Figure 1: The framework established in the Act on the Protection of Personal Information.



Source: Office of Personal Information Protection, Cabinet Office, „The Outline of the Act on the Protection of Personal Information and its Enforcement Status in Japan,“ January 23, 2007

Additional and detailed provisions are provided by the Cabinet and Ministers, each of whom has their own jurisdiction to oversee. The Cabinet approved a Basic Policy for the Act for the Protection of Personal Information on 2 April 2004, outlining the measures and actions to be taken by state and local governments and private entities to fulfil the principles and objectives of the Act. Ministers later issued guidelines for industries under their jurisdiction to set out sector- or industry-specific principles and rules to be observed.

Telecommunications is one of the exceptions where sector-specific regulation is more intense than general personal information protection regulation. The Telecommunications Business Act has provisions on telecommunication carriers' obligation to protect subscribers' information. The Act also requires telecommunication carriers to install necessary equipment and measures to fulfil the obligation.

4.1.2.1 Act on the Protection of Personal Information

Today, the overall framework for the protection of personal information is set forth by the Act on the Protection of Personal Information (Act No. 57 of 2003). The Act, which took effect in April 2005, outlines the principles and objectives for the protection of personal information and how personal information should be protected in the private sector. The main principle of the Act is that personal information should be handled in a cautious and appropriate manner with respect for individual information. The law imposes legal obligations for the protection of personal information on businesses which fall under certain criteria.

The Act on the Protection of Personal Information is accompanied by a few other acts which regulate the protection of personal information in public administrations and incorporated administrative agencies (quasi-government agencies).

4.1.2.2 Act for the Protection of Personal Information Held by Administrative Organs

In public administrations, certain aspects of the protection of personal data had been mandated by earlier legislation. The Act for the Protection of Computer Processed Personal Data held by Administrative Organs (Act No. 95 of 1988) had required that public administrations protect personal information in the course of computer processing.

In 2003, along with the Act on the Protection of Personal Information, the Act on Protection of Personal Information Held by Administrative Organs (Act No. 58 of 2003) was enacted, and personal information held by public administrations came into the scope of personal information protection.

4.1.2.3 Act for the Protection of Personal Information Held by Incorporated Administrative Agencies

In order to ensure the protection of personal data in public corporations established under the auspices of the government, another law, Act for the Protection of Personal Information Held by Incorporated Administrative Agencies (No. 59 of 2003), was enacted.

The three different „sectors“ (private enterprises, public administration, and semi-public administrative agencies) are covered by the three Acts. This set of Acts illustrates how personal information protection is regulated sector by sector.

4.1.2.4 Establishment of Commission of Information Disclosure and Protection of Personal Information

In addition to sectoral regulation, the establishment of a Commission for reviewing the process of information disclosure and the protection of personal information was also enacted as a separate law by the Act on the Establishment of the Commission of Information Disclosure and Protection of Personal Information (Act No. 60 of 2003)

The Commission is composed of 15 members, nominated by the Prime Minister with concurrence of the Diet. The role of the Commission is to give advice and consultation to the administrative bodies receiving complaints from citizens concerning information disclosure and the protection of personal information. The Commission has the authority to examine the internal documents and personal information that the administrative body in question has to review as part of the complaint process.

4.1.3 Basic Policy and Ministerial Guidelines

As the Acts only sets forth „high-level“ principles and objectives for the protection of personal information, a number of Cabinet- and Minister-level orders and guidelines have been formulated.

In 2004, a year before the full implementation of the Act for the Protection of Personal Information and other relevant Acts, the Cabinet adopted a policy document describing the direction policy measures should take and specifying measures which the national government may take and the actions which local governments and personal information handling entities may take in implementing and complying with the Act. The document titled the „Basic Policy for the Act on the Protection of Personal Information“, also calls for the engagement by all stakeholders, public and private, in implementation of the philosophy and principles of the Act.

The Basic Policy stresses that information society will only be achieved when all the necessary efforts for the protection of personal information have been taken, and that collaboration between the public and private, as well as voluntary action by private entities will be necessary.

The Basic Policy also encourages entities to disclose cases to the fullest extent possible when information breaches occur so secondary damage and similar cases may be avoided. In FY2005, a total of 1,556 cases of information breach were disclosed. With rising awareness of personal information protection among the public, businesses tend to disclose cases of information breach immediately to avoid reputation risk.

As of 31 March 2007, a total of 35 guidelines in 22 industry sectors have been published. Each of these guidelines is published by the Competent Minister. The guidelines are drafted in accordance with the Basic Policy by the Cabinet. Some guidelines, such as medical services, telecommunications, and financial services are normative and add to provisions of the Act of the Protection of Personal Information, while other guidelines are informative and should be understood as an interpretation of the provisions of the Act.

Business area	Guidelines
Medical Services	Guidelines on Appropriate Handling of Personal Information for Medical and Nursing Care Workers (Published: December 24, 2004. Revised: April 21, 2006.) Guidelines on Appropriate Handling of Personal Information for Health Insurance Association and Related Entities (Published: December 27, 2004) Guidelines on Security Management of Medical Information System (Published: March 31, 2005) Guidelines on Appropriate Handling of Personal Information for the National Health Insurance Association (Published: April 1, 2005)
Medical Research	Ethical Guidelines on Study of Human Genome and Genetics Analysis (Published: December 28, 2004) Ethical Guidelines on Study of Epidemiology (Published: December 28, 2004) Guidelines on Clinical Study of Gene Therapies (Published: December 28, 2004) Ethical Guidelines on Clinical Study (Published: December 28, 2004) Guidelines on Clinical Study of Human Stem Cell (Published: July 3, 2006)
Financial Services	Guidelines on the Protection of Personal Information in Financial Sector (Published: December 6, 2004) Practical Guidelines on the Security Management for the Protection of Personal Information in Financial Sector (Published: January 6, 2005) Guidelines on the Protection of Personal Information for Credit in Economy, Trade and Industry Sector (Published: December 17, 2004. Revised: October 16, 2006)
Information and Telecommunication	Guidelines on the Protection of Personal Information in Telecommunication Business (Published: August 31, 2004. Revised: October 17, 2005) Guidelines on the Protection of Personal Information for Recipients of Broadcasting (Published: August 31, 2004. Revised: March 28, 2007)
Industry in General	Guidelines on the Protection of Personal Information in Economy, Trade and Industry Sector (Published: October 22, 2004. Revised: March 30, 2007) Guidelines on the Protection of Personal Information for Businesses that Include Use of Personal Genetic Information in Economy, Trade and Industry Sector (Published: December 17, 2004)
Employment	Guidelines on the Measures for Businesses to Ensure Appropriate Handling of Personal Information Related to Employment Management (Published: July 1, 2004) Points of Consideration on the Handling of Personal Health Information Related to Employment Management (Published: October 29, 2004)
Seamen	Guidelines on the Measures for Businesses to Ensure Appropriate Handling of Personal Information Related to Employment Management of Seamen (Published: September 29, 2004)
Police	Guidelines on the Measures for Businesses under the Jurisdiction of National Public Safety Commission to Protect Personal Information (Published: October 29, 2004) Guidelines on the Measures for Japan Police Personnel Mutual Aid Association to Protect Personal Information (Published: March 29, 2005)
National Defence	Guidelines on the Protection of Personal Information Handled by Businesses and Neighbouring Entities Related to the Ministry of Defence (Published: May 25, 2006)
Judicial Affairs	Guidelines on the Protection of Personal Information Handled by Businesses under Jurisdiction of the Ministry of Justice (Published: October 29, 2004) Guidelines on the Protection of Personal Information in Credit Management and Collection Sector (Published: December 16, 2004. Revised: January 11, 2006)

Business area	Guidelines
Foreign Affairs	Guidelines on the Protection of Personal Information Handled by Businesses under Jurisdiction of the Ministry of Foreign Affairs (Published: March 25, 2005)
Finance	Guidelines on the Protection of Personal Information for Businesses under Jurisdiction of the Ministry of Finance (Published: November 25, 2004)
Education	Guidelines on the Measures for Businesses to Ensure Appropriate Handling of Personal Information of Students at Academic Institutes (Published: November 11, 2004)
Welfare Business	Guidelines on the Appropriate Handling of Personal Information in Welfare Businesses (Published: November 30, 2004)
Employment Services	Guidelines on the Appropriate Conduct of Equal Treatment, Indication of Working Conditions, Handling of Personal Information of Job Applicants, Duties of Employment Agencies and Indication of Job Description by Employment Agencies, Recruit Advertisers, Contracted Recruiters and Personnel Service Agencies (Published: November 4, 2004)
Personnel Service	Guidelines on the Measures for Personnel Service Agencies (Published: November 4, 2004)
Labour Union	Guidelines on the Measures for Labour Union to Ensure Appropriate Handling of Personal Information (Published: March 25, 2005)
Corporate Pension	Guidelines for the Handling of Personal Information on Corporate Pension (Published: October 1, 2004)
Land Infrastructure and Transport	Guidelines on the Protection of Personal Information under Jurisdiction of the Ministry of Land, Infrastructure and Transport (Published: December 2, 2004) Guidelines on the Implementation of the Act on Protection of Personal Information in Real Estate Transaction Sector (Published: January 14, 2005)
Agriculture, Forestry and Fisheries	Guidelines on the Measures for Businesses Related to Agriculture, Forestry and Fisheries to Ensure Appropriate Handling of Personal Information (Published: November 9, 2004)

For the public and semi-public sector, the Ministry of Internal Affairs and Communications published two guidelines:

- Guidelines on the Measures for Appropriate Management of Personal Information Held by Administrative Organs, and
- Guidelines on the Measures for Appropriate Management of Personal Information Held by Incorporated Agencies

One of the characteristics of the personal information protection „regime“ is that legislation is multi-layered. The Act for the Protection of Personal Information sits on top as a guiding principle. The Act also has provisions for the protection of personal information in the private sector, while the public and semi-public sectors are regulated by the Act on Protection of Personal Information Held by Administrative Organs, and the Act for the Protection of Personal Information Held by Incorporated Administrative Agencies respectively. In the private sector, Ministers publish guidelines for the protection of personal information in the jurisdiction that they oversee, thus optimizing the regulation in each jurisdiction.

The multi-layered approach is one of the key differences in the personal information protection „regime“ between Japan and the European Union. Although the Act on the Protection of Personal Information is administered by the Cabinet Office, it does not mean the Cabinet Office can direct or override the authority of other Ministries. In general, the role of the Cabinet Office is to take the lead in coordinating and aggregating various ministerial needs for legislation. As a result, in the current regime for the protection of personal information in Japan there is no centralized authority which can exercise government-wide enforcement power.

4.1.4 Scope of the Protection of Personal Information

Article 2 of the Act for the Protection of Personal Information states, „the purpose of this Act is to protect the rights and interests of individuals while taking consideration of the usefulness of personal information.“ This means the Act should respect the protection of personal information and its exploitation at the same time.

The Act defines personal information as „information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information as will allow easy reference to other information and will thereby enable the identification of the specific individual).“ However, the definition can be quite broad in practice, because the point of the definition is whether the piece of information (or combination of pieces of information) can identify an individual regardless of the nature of the information. Therefore personal names, addresses, and medical records all fall under the definition of personal information and are protected by the Act if they can identify an individual.

Sensitive information is defined in a sector-specific manner. The Basic Policy directs Ministers to review their jurisdiction and identify areas such as medical and financial services, and telecommunications, where handling of personal information needs particular attention and care.

In the case of telecommunications, the Ministry of Internal Affairs and Communications, published the Guidelines on Protection of Personal Information in Telecommunications Business[196], where sensitive information is considered to include „items related to personal belief, creed and religion,“ and „items which might cause social discrimination such as race, origin, physical and mental disability, crime records, and medical records.“ (Section 2, Article 4)

In the current regulatory context, only businesses or other entities which collect more than 5,000 instances of personal data for over six months are regarded as „entities

196 Ministry of Internal Affairs and Communications, Announcement No. 695, 31 August 2004.

handling personal information“ and subject to regulation. Other entities which do not deal with personal information to this extent are exempted from regulation. Entities handling personal information are required to (1) declare the objectives for collecting personal data and limit the use of the collected data within the declared objectives, (2) collect personal data in an appropriate manner and inform the information entities on the objectives for collecting personal data, (3) ensure the accuracy of the collected personal data, (4) install appropriate equipment and monitor employees and contractors to ensure the security of the collected personal data, (5) limit the distribution of the collected personal data to a third party, and (6) publish the objectives for collecting personal data and the procedures for disclosing, correcting and removing the collected personal data.

4.1.5 International Harmonization

The Quality-of-Life Council considered various issues of international harmonization in terms with personal information protection. Among the issues discussed, this subsection reviews the discussion on the APEC Privacy Framework because it might draw some comparative perspective against European harmonization efforts on personal information protection.[197]

In line with the 8 principles of the OECD, Asian countries recognise the importance of developing similar principles that better fit the reality of information protection in Asia. In November 2004, APEC ministers endorsed the 9 principles of the APEC Privacy Framework. The APEC Privacy Framework promotes a flexible approach to information privacy protection for the APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows.[198] Compared to the OECD principles, the APEC Privacy Framework is still immature. Steady discussion and coordination among the APEC members is being encouraged.

At the regular meetings of the Committee on the Protection of Personal Information of the National Quality-of-Life Policy Council, an advisory body to the Prime Minister at the Cabinet Office, Japanese legal and other experts discuss how to adopt the APEC Privacy Framework in Japan. The Committee was set up by the general assembly of the Council in July 2005. Currently, the Committee has 16 members and they comprised of academics in law or communications, journalists, business executives, lawyers, local governments officials, and representatives of consumer associations.

Recent discussion at the Committee can be largely summarised in two aspects. One is how to ensure international harmonization on the protection of personal information and the other is how the concept of the „third party organisation“ in the APEC Privacy Framework can be realized in Japan.

---

197 See also the discussion in Section 9.2.
198 <http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html>

Committee members recognise „the concept of privacy“ differs from country to country and, unlike in Europe, there is a lack a common understanding throughout the Asian region. It is necessary to establish a common understanding of privacy and protection of personal information, taking into account cultural diversity in Asia, as part of the process of implementing the Framework. To achieve this some committee members have suggested Asia needs to look beyond the regimes of the current forerunners, Europe and the United States, but instead suggest taking a lessons-learned approach these advanced examples to help establish a „third“ way based on implementation of basic law together with separate specific laws.[199]

In APEC discussions the Ministry of Economy, Trade and Industry handles issues on eCommerce and the Ministry of Internal Affairs and Communications deals with issues on telecommunications. While working on establishing a common framework at the international arena (i.e. Privacy Mark system etc.), the Japanese government also needs to coordinate domestic measures among the competent ministries in order to fit them to emerging new international standards.[200] In addition, in Europe, experts have noted national security demands are triggering tension regarding the protection of personal information. Asia needs to be prepared for the same kind of problem in the near future.

Japan also recognizes Asian cultural diversity is a difficult task to tackle, however, „Asian cultural diversity rhetoric“ should not be an excuse for not working on the personal information protection. In a globalised world, the flow of information becomes trans-border and it influences world-wide. It is said that the EU directives only apply to the EU countries, but the directives protect personal information of the EU citizens which might be transferred to the non-EU third country. Currently, Japan complies with these EU directives by applying specific individual contracts. However, it is likely that Japan will start to consider regulation similar to the EU directives, approving data transfer to a third country only when a „sufficient level of protection“ of the information is guaranteed.

Second, considering the APEC Frameworks recommendations about third party organisation, unlike the EU countries, the APEC member countries rarely have legislation on the protection of personal information. Among the 21 APEC economies, only Canada, Australia, New Zealand and Hong Kong have privacy oversight bodies. Clearly, a common understanding of what should be the implementing organisation of the APEC Privacy Framework cannot be reached at this stage. Implementation of the APEC framework will take time, reflecting each country’s pace of developing new legislation.

---

199 Summary of discussions at the Task Force on the Protection of Personal Information, 9p <http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070405kojin1.pdf>

200 Summary of discussions at the Task Force on the Protection of Personal Information, 9p <http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070405kojin1.pdf>

The Japanese system of personal information protection is a product of combining a system relying on action by the competent minister with a system of specific responsible councils. This system is fundamentally different from a system managed by a third party organisation. In addition, Japan has not created the position of Information Commissioner as some European countries have. The main problem in the Japanese system is that there is no organisation overseeing the whole system comprehensively. It only allows the competent ministers or councils to „react“ when information breaches occur.[201]

Many Asian countries have just started implementing legislation and the concepts of privacy or protection of personal information are still new. Even in Japan, which is considered to be one of the advanced countries on data protection in Asia, heated discussions take place over wide-ranged of issues in the Committee on the Protection of Personal Information. In short, the Japanese government has not reached a stage where it is able to indicate any clear direction or tangible solution for newly arising issues. As seen in the Japanese case, proper coordination between international standard and domestic legislation is a very complicated task. Most likely it will take some time to reach a consensus on framing the detailed APEC privacy framework among the member countries.

Discussions of the Committee on the Protection of Personal Information of the National Quality-of-Life Policy Council make clear the Japanese government has not reached a conclusion how it should approach the APEC Framework, and while the framework is being discussed and developed further it is unlikely the government will take any firm steps until the Framework stabilizes.

4.2 Arrangements other than law and regulation

Self-regulatory arrangements for the protection of personal information can be found in two streams. One is the self-regulatory arrangement coordinated by the Act for the Protection of Personal Information. In the light of the objectives of the Act, protection of personal information should be pursued on the initiative of businesses and other entities handling personal information. In this stream of self-regulation industry groups and trade associations are designated as „Authorized Personal Information Protection Organizations“ which promote industry-wide personal information protection.

In principle, however, the Act does not dictate how personal information should be protected and allows each player take necessary actions. In other words, the government formulates the regulatory environment and provides necessary assistance for the industry’s self-regulation to implement and maintain a working solution.

---

201 Summary of discussions at the Task Force on the Protection of Personal Information, 10p <http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070405kojin1.pdf>

The second self-regulatory approach is through labelling programmes. Currently, there are a number of privacy-labelling programmes in use in Japanese industry. Major initiatives include Privacy Mark and TRUSTe. In addition, there are industry-specific programs such as Japan Accreditation Council for Healthcare Information (JACHI) and Campaign Privacy. The following subsections will briefly describe how these labelling programmes function and review their effectiveness.

4.2.1 Government-arranged self-regulation

Although the Act on the Protection of Personal Information encourages self-help by each entity handling personal information, it also encourages industry-wide self-regulation. The Act for the Protection of Personal Information includes provisions for authorizing organizations in the private sector which intend to ensure the proper handling of personal information. These organizations are called „Authorized Personal Information Protection Organizations“, and are authorized by the competent minister who oversees the corresponding area of business.

Authorized Personal Information Protection Organizations are an entity or group of entities which intend to ensure the proper handling of personal information in a particular industry sector, sub-sector or geographic region. They form voluntarily and draw-up their own operating guidelines following an interpretation of the law. The guidelines should be publicly announced and all members agree to comply with them. The role of an Authorized Personal Information Protection Organizations is two-fold. One is to accept complaints from consumers and citizens concerning the handling of personal information and provide consultation and advice back to the consumers and citizens. Their other role is to raise awareness and provide their members with information on the proper handling of personal information.

As of 31 May 2007, a total of 34 organization are authorized.

Field	Authorized Personal Information Protection Organization
Securities	Japan Securities Dealers Association
Insurance	Life Insurance Association of Japan General Insurance Association of Japan Foreign Non-Life Insurance Association of Japan
Banking	All Banks Personal Data Protection Council
Trust	Trust Companies Association of Japan
Investment Trust	Investment Trusts Association
Securities Investment Consulting	Japan Securities Investment Advisers Association
Credit Bureau	Federation of Credit Bureaus of Japan
Credit Bureau and Consumer Credit	Association for Consumer Credit Information Protection

Field	Authorized Personal Information Protection Organization
Consumer Credit	Credit Personal Information Protection Council
Broadcasting	Secure Broadcasting Authorization and Research Center
Telecommunications	Nippon Information Communications Association
Industry in General	Japan Information Processing Development Corporation
Pharmacy	Federation of Pharmaceutical Manufacturers' Associations of JAPAN
Social Welfare and Nursing Care	Okinawa Council on Social Welfare Gifu Council on Social Welfare
Medical Services	All Japan Hospital Association Japan Hospital Association
Medical Services, and Nursing Care	Medical Network Support Center
Medical Services, Nursing Care, and Social Welfare	Ombudsman for the Rights of Patients
Chiropractic Therapy	Japan Therapist Association
Gift Merchandise	All Japan Gift Association
Funeral Services	JECIA Personal Information Protection Association Zenkoku Kokoronokai (Japan Heartful Society)
Printing and Graphics	Tokyo Graphic Services Industry Association
Retail	Japan Specialty Stores Association
Other	Japan Association of Personal and Healthcare Information Control Nippon Association of Consumer Specialists Association for Personal Information Protection of Nagano
Marriage Information Services	Marriage Information Service Council
News Paper Distribution	Business Cooperative for the Mainichi Shinbun Distributors of Osaka
Automobile Sales	Japan Automobile Dealers Association
Automobile Registration	Japan Automobile Registration Council

Source: Cabinet Office, List of the Authorized Personal Information Protection Organizations as of 31 May 2007[202]

Each organization has formulated guidelines on the protection of personal information in their business or subject area. Members of the organization are expected to respect the guidelines. These sector-specific guidelines are optimized to the needs and reality of the business or subject area.

The benefit of becoming a member of an Authorized Personal Information Protection Organization is not visible. However, through membership of an Authorized Personal Information Protection Organization, Entities Handling Personal Information are able to

202 <http://www5.cao.go.jp/seikatsu/kojin/ninteidantai.html>

show their readiness to handle personal information in a proper and appropriate manner and so gain trust from citizens.

The Act presupposes that, in principle, cases will be dealt with by the entity itself or the Authorized Personal Information Protection Organization to which the entity belongs. However, if the case cannot be resolved at the self-regulation level, it may be elevated to the Minister, who then considers the case and gives the entity in question an order. However, Ministerial actions are considered to be the last resort.

4.2.2 Other self-regulation efforts

In addition to the self-regulation framework that is assumed by the Act on the Protection of Personal Information, other efforts are also being made. Some of them are commercially driven.

4.2.2.1 Privacy Mark

The Privacy Mark system accredits organizations which implement appropriate measures for protecting personal data. Accredited organizations will be licensed to bear the Privacy Mark on their web site, which will show the organization's ability to protect personal data. The Privacy Mark program is compliant with JIS Q 15001:2006, *Personal information protection management systems – Requirements*.

The Privacy Mark system is operated in a hierarchical structure. The Japan Information Processing Development Corporation (JIPDEC) acts as accreditation authority, and actual accreditation is mostly delegated to designated organizations. The number of accredited organizations grew drastically after the Act on the Protection of Personal Information came into effect in 2005. In FY 2005, 553 organizations were accredited and licensed to bear Privacy Mark. In FY 2006, it rose to 2,395. In FY 2006, 3,798 organizations were accredited.[203]

The objectives of the Privacy Mark system are: (1) to enhance consumer consciousness towards personal information protection with the display of the privacy mark visible to the eyes of consumers; and (2) by promoting the appropriate handling of personal information, respond to heightened awareness toward the protection of personal information of consumer, and bestow incentives to gain social credibility on business operators.[204]

---

203 http://privacymark.jp/news/20070611/jikohoukoku_H18_20070611.pdf

204 Privacy Mark System pamphlet, 2 p. <http://privacymark.org/ref/info/PM_system_panphlet_v1.0_061006_Eng.pdf>

JIPDEC established a Mark System Committee consisting of scholars, individuals, representatives from business organizations, representatives of consumers and legal professionals. The Committee is responsible for (1) establishment and revision of standards and regulations involving the system; (2) designating and revoking designation of the designated organization; and (3) revoking privacy mark certification.[205]

The designated organizations are those that have applied for the designation and that have been approved to be designated by JIPDEC. Designated organizations receive applications from companies, screen and investigates companies submitting applications and appropriately certify or reject the use of Privacy Marks.[206] The effective period of Privacy Mark certification is two years. A two-year extension can be applied for after the two-years effective period. Renewal may be applied for every two years.[207]

The fees for application, screening and mark use are required upon application for the privacy mark certification. The total fee ranges from 300,000 yen to 1,200,000 yen on a biennial basis depending on the size of company. The fee is not necessarily low by Japanese economic standards. However, many companies showed interests in applying for Privacy Mark after the enforcement of the Act on the Protection of Personal Information, as Privacy Mark guarantees companies' credibility on the protection of personal information.

4.2.2.2 TRUSTe

The TRUSTe program is an international initiative. It accredits qualified web site operators based on the appropriateness of the handling of the personal data that the web site operators collect. TRUSTe in Japan was established in June 2006, and is operated by the Japan Privacy Accreditation Council. As of April 2007, 738 web sites had been accredited by the TRUSTe program.

TRUSTe is an international independent non-profit organization, which aims to establish trust with website users and achieve further development of the Internet industry. Based on the OECD's 8 privacy principles, TRUSTe ensures the protection of personal information, by promoting the concept for disclosing privacy policy, obtaining users' consent and educating users. Currently, TRUSTe has headquarters in the U.S. and an accreditation office in Japan. The structure of TRUSTe is similar to that of Privacy Mark system. TRUSTe is a granting organization and the designated organizations conduct actual screening of applications. After the written screening and interview, TRUSTe will grant the TRUSTe seal.

---

205 Privacy Mark System pamphlet, 3 p. <http://privacymark.org/ref/info/PM_system_panphlet_v1.0_061006_Eng.pdf>

206 Privacy Mark System pamphlet, 2-3 pp. <http://privacymark.org/ref/info/PM_system_panphlet_v1.0_061006_Eng.pdf>

207 Privacy Mark System pamphlet, 4 p. <http://privacymark.org/ref/info/PM_system_panphlet_v1.0_061006_Eng.pdf>

Currently, TRUSTe Japan has three brand seals: (1) Web Privacy Seal Program: It complies with 8 principles of the OECD and the Act on the Protection of Personal Information. This is the TRUSTe's standard program which accredits websites with privacy policy. This applies to regular websites, mobiles and mall shop programs; (2) eHealth Privacy Seal Program: This covers sensitive information at hospitals and medical institutions. It complies with Health Insurance Portability and Accountability Act in the U.S. This applies to regular and mobile websites; and (3) KIDS Privacy Seal Program: This is applied for websites which target children under 13 years old and the program requires parents' consent upon collecting children's personal information. Japanese laws do not provide specific provisions on children, therefore the program aims to ensure children's security and privacy. This program complies with The Children's Online Privacy Protection Act in the U.S. and it applies to regular and mobile websites.[208]

The fee for TRUSTe application consists of three types, which are license fee, screening fee and consulting fee (optional). The total cost ranges from 72,000 yen to 1,800,000 yen annually, depending on the size of the company.

TRUSTe provides five support services to help members with compliance: (1) Site review: This program reviews website every three months during the contracted year. If the website does not comply with TRUSTe's privacy standard, recommendation will be made; (2) Watchdog program: TRUSTe receives complaints from users in case the accredited company's response or reaction for users on the privacy protection is not sufficient; (3) Privacy breach liability insurance: Annual license fee includes a general liability insurance for companies whose yearly sales are less than 100 billion yen; (4) Detecting unsolicited e-mails program: When TRUSTe finds privacy problems on the websites, it will register itself as a dummy user and observes whether a smooth opt-out procedure can be conducted; and (5) TRUSTe sign: this is an automated website monitoring program which is conducted every 20 days. All of these five programs help the accredited companies to ensure an appropriate operation of the protection of personal information on their websites.[209]

4.2.2.3 JACHI

Japan Accreditation Council for Healthcare Information (JACHI) focuses on the protection of personal information in the medical field. While JACHI takes into account the advantage of efficiency and convenience of Internet use, JACHI considers that personal information which relates to person's health is one of the most sensitive types of information and requires the most careful handling. JACHI was established in 2006 in order

---

208 <http://www.truste.or.jp/main/seals.php>
209 <http://www.truste.or.jp/main/bukup.php>

to establish credibility for healthcare services, provide a moral code, provide an accreditation and screening services and train human resources.[210]

4.2.2.4 Japan Accreditation Council for Marketing Privacy: „Web Privacy Seal“

Web Privacy Seal is an industry-specific accreditation program operated by the Japan Accreditation Council for Marketing Privacy (JAMP). Web Privacy Seal examines and certifies the appropriate handling of personal data in short-term web sites which collect personal data for advertisement or prize campaigns. Once certified, web sites can bear a certification seal.

JAMP was established in 2005 and is an accredited Non-Profit Organization of the Cabinet Office. JAMP aims to promote economic activities by providing citizens an appropriate privacy protection service and establishing a system to educate staff in the marketing sections of companies.[211]

The basic concept of Web Privacy Seal provides (1) A standard for protection for personal information handled on websites; (2) A system to guarantees that websites comply with the standard; and (3) A solution for claims and complaints from users about websites.[212]

The principles of Web Privacy Seal are based on the internationally acknowledged privacy principles such as the 9 APEC principles, 8 OECD principles and the Act on the Protection of Personal Information in Japan. Web Privacy Seal emphasizes that a global perspective is lacking in other Japanese privacy labelling services. In addition, Web Privacy Seal offers the lowest license application fee, 3,150 yen monthly[213], less than half the cost of the lowest price offered by the other privacy labelling services.

4.3 Enforcement powers

4.3.1 Public authority

Under the current Japanese legislation, enforcement powers regarding private enterprises are somewhat limited because it assumes primary efforts should be taken by the private sector and other entities who actually handle personal information. Authorized Personal Information Protections Organizations are expected to act as the interface between citizens and businesses. The competent Minister will only intervene when a

---

210 <http://www.jachi-md.org/meaning/index.html>
211 <http://www.privacy.or.jp/outline.htm>
212 <http://www.privacy.or.jp/WPS/wps_page01.html>
213 <http://www.privacy.or.jp/WPS/wps_page02.html>

dispute cannot be settled privately. In this public intervention the Minister will consider the process and outcome of private arbitration when deciding what necessary action should be taken. The Act on the Protection of Personal Information requires personal information handling entities (private entities which carry more than 5,000 instances of personal information for over six months) to appropriately handle the personal information that they collect. If they fail, the Act may require them to provide a report on the handling of personal information to the competent minister (Article 32). In more serious cases, the competent minister may give advice to the entity (Article 33). Depending on the scale of incident, the competent minister may give recommendations (Section 1, Article 34) or orders (Section 2 and 3, Article 34) to personal information handling entities to take actions to satisfy the legal requirements. Failure to provide a required report or to comply with the minister's order may result in criminal offences. The former may result in a fine up to 300,000 yen, and the latter may result in either imprisonment for up to six months or a fine up to 300,000 yen.[214]

The law assumes the responsibility of protecting personal information is held by managerial officers and by operators who actually deal with personal information. Both managerial officers and operators will possibly charged with criminal offences when violations of the Act occur, e.g. breach or theft (Article 58 of the Act). However, some experts publicly argues that managerial officers may be easily be charged although operators who may have actually made breaches, possibly with intent, are less likely to be charged.

4.3.2 Private litigation

Although private litigation is not yet common to settle down disputes concerning personal information protection, case law is developing on compensation for privacy breaches under the law and by self-regulation

The first case of monetary compensation concerning the breach of personal information occurred in 2001. A group of citizens sued the City of Uji for the breach of personal information from the Basic Resident Registry (Juki-Net). The court ruled in favour of the citizens and ordered the City to provide compensation of 10,000 yen for each plaintiff. This case was the first demonstration in Japan that mismanagement of personal information could be a financial risk.

In June 2003, one of the largest convenience store chains, LAWSON, disclosed 560,000 instances of personal information. The company offered a 500-yen worth gift certificate per each information subject by way of compensation. LAWSON's payment has since formed the standard level of compensation for such disclosures of personal

---

214 <http://www5.cao.go.jp/seikatsu/kojin/kaisetsu/pdfs/tanpo.pdf>

information. In January 2004, Softbank, the third largest telecommunication carrier, leaked personal information of 4.5 million subscribers. The company offered a gift certificate worth 500 yen for the information subjects concerned. The compensation by Softbank reportedly amounted to some 4 billion yen.

4.4 Effectiveness

4.4.1 Effectiveness of legal and regulatory measures

According to the report on the enforcement status of the Act in FY2005 prepared by the Cabinet Office, the Minister for Financial Services exercised its power in 84 cases in total. In 83 cases, the Minister requested formal reporting, and in one case the Minister gave a recommendation. All the cases involved failure to comply with the requirement for the instalment of security control measures (Article 20). Nine cases out of the 84 involved failure in the supervision of employees (Article 21), and 19 cases[215] addressed failure to appropriately supervise subcontractors.

The Minister of Health, Labour and Welfare exercised power on four cases. All were charged with violation of the requirement for the instalment of security control measures (Article 20). Examining statistics of the both ministries, during FY 2005, the competent ministers requested 87 reports and made one recommendation (one report is covered by co-jurisdiction of the both ministries).[216]

---

215 Note: Some of the cases were charged with violation of multiple number of Articles. Thus, the accumulation of content-oriented case number and the total case number does not match.
Summary Report on the Enforcement Status of Act on the Protection of Personal Information in FY 2005, Cabinet Office, June 2006 <http://www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf>

216 Summary Report on the Enforcement Status of Act on the Protection of Personal Information in FY 2005, Cabinet Office, June 2006 <http://www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf>

Table: The Status of Exercise of Authorities by the Competent Ministers (FY 2005)[217]

Competent Minister	Type of Authority Exercised	Relevant Articles
Minister for Financial Services	Collection of reports: 83 cases Recommendation: 1 case	Article 20 (instalment of security control measures) Article 21 (supervision of employees) Article 22 (supervision of contractors)
Minister of Health, Labour and Welfare	Collection of reports: 4 cases	Article 20 (instalment of security control measures)
Total	Collection of reports: 87 cases in total Recommendation: 1 case in total	Article 20: 88 cases in total Article 21: 9 cases in total Article 22: 19 cases in total

The Basic Policy for the Act on the Protection of Personal Information encourages entities to disclose cases to the fullest extent possible when information breaches occur so secondary damage and similar cases may be avoided. In FY2005, a total of 1,556 cases of information breach were disclosed. With rising awareness of personal information protection among the public, businesses tend to disclose cases of information breach immediately to avoid reputation risk.

While enforcement of the Act has spread steadily, a number of Japanese private and public sector organizations have overreacted when attempting to comply with the Act. As a background we can consider two factors. One is increasing awareness of personal information protection among people as a result of the introduction of the Act, while the other is misunderstanding of the current legal system.

As a result of these two factors, Japan has been experiencing the following three emerging problems: (1) Refusal to provide information to respond to inquiries based on laws, such as the national census. This also includes instances where an enterprise refused to respond to a lawful inquiry from the police and an inquiry from a bar association; (2) Refusal to provide information when it is necessary for protecting the life, well being, or property of an individual. Providing personal information in emergency cases is necessary and it can be a matter of life or death. Significantly, provision of information to the list of purchasers should be permissible in the case of product recall; and (3) Creation and provision of lists is difficult in general. People even feel that it is against the law to make lists of students and parents in schools. All of these cases are based on misunderstanding of the intent and scope of the Act on the Protection of Personal Information.

---

217 Summary Report on the Enforcement Status of Act pin the Protection of Personal Information in FY 2005, Cabinet Office, June 2006, 2p http://www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf
Note1: Under Article 52 of the Act and Article 12 of Cabinet Order of the Act, the Prime Minister delegates authority to the President of the FSA.
Note2: Overlapping cases arising from co-jurisdiction are counted respectively.

These misunderstandings about the law can be serious and in some cased quite distressing. On the morning of 26 April 2005 the derailment of a West Japan Railway Company (JR West) killed 106 passengers and the train driver. Following the accident, the railway company and hospitals receiving the injured both refused to offer the information of casualties to family members for fear they may infringe their privacy and personal information under the misunderstood law.[218] Although disclosure of personal information in emergencies is considered to be lawful even without prior consent of data subjects, this was not fully understood at that time. As mentioned, other minor cases, such as refusal to answer the national census or to provide information to law enforcement authorities have also been reported at the Committee on the Protection of Personal Information of the Quality-of-Life Council.[219]

The Cabinet Office is currently suggesting several measures to address these problems, such as raising awareness and understanding of the Act, encouraging discussion by the Quality-of-Life Policy Council, and working with the inter-ministerial Committee on the protection of personal information.[220]

4.4.2 Effectiveness of arrangements other than law and regulation

Authorized Personal Information Protection Organizations report to the supervising Ministry on the inquiries and claims that they have received and the actions that they have taken in response. The table below summarized the activities of the Authorized Personal Information Protection Organizations in FY2005. Each Authorized Organization is supervised by one or multiple Ministries, and the figures were aggregated ministry-by-ministry.

---

218 JR West rejects disclosure of casualties' information to municipal authorities. (11 May, 2005) <http://www2.asahi.com/special/050425/OSK200505110052.html>

219 Minutes of the Quality-of-Life Council. <http://www5.cao.go.jp/seikatsu/shingikai/kojin/kojinjyouhouhogobukai-index.html>

220 Summary Report on the Enforcement Status of Act pin the Protection of Personal Information in FY 2005, Cabinet Office, June 2006, 2p <http://www5.cao.go.jp/seikatsu/kojin/foreign/enforcement-status2005.pdf>

Supervising Agency/Ministry	Complaints received	Actions taken against entities handling personal information				
		Reporting by hearing	Reporting by document	Advise	Recommen-dation	Other action
Financial Services Agency	237	55	1	135	1	0
Ministry of Inter-nal Affairs and Communications	114	59	0	0	0	2
Ministry of Health, Labour and Wel-fare	0	0	0	0	0	0
Ministry of Econ-omy, Trade and Industry	107	54	0	2	0	0
Ministry of Land, Infrastructure and Transport	0	0	0	0	0	2
Total*	355	118	1	137	1	4
* Total figures do not correspond to the sum of the figures above because complaints and actions may be counted in more than one Ministries						

Source: Cabinet Office, The Outline of the Act on the Protection of Personal Information and its Enforcement Status in Japan (January 2007)

In 2006, Nippon Information Communications Association, the Authorized Personal Information Protection Organization in telecommunications, reportedly received 229 complaints or inquiries from consumers concerning personal information protection. Among these, the Association investigated 62 cases. The majority of the inquiries were made because the person believed their personal information might have been breached.[221] Most of the cases were resolved after complaints or inquiries were placed.

The effectiveness of privacy labelling in Japan is yet to be seen, because many Japanese companies began to formalize their efforts to protect personal data only after the Act on the Protection of Personal Information Protection took effect. The table below shows the number of the organizations each year which received Privacy Mark accreditation during the period FY1998 to FY2006. As of March 2007, 7,549 entities held privacy marks.

Year	1998	1999	2000	2001	2002	2003	2004	2005	2006
# of accreditation	58	71	96	120	172	286	553	2,395	3,798

The number of the organizations which received Privacy Mark accreditation

Source: JIPDEC[222]

221 Based on the writer's personal interview with MIC official in May 2007.
222 <http://privacymark.jp/news/20070611/jikohoukoku_H18_20070611.pdf>

The Privacy Mark may be revoked when the accredited entity cannot perform the required duties. Since the instalment of the Privacy Mark, only the accreditation of one entity has been revoked to date. Requests/warnings, which are the second heaviest penalty to revocation, have been given to seven entities to date.[223]

Privacy Mark covers areas other than electronic communications, but as telecommunication carriers and information service providers comprise 40% of accredited organizations, we can conclude the trend is also significant for the electronic communications sector. Industry is showing greater interest in and respect for privacy labelling. According to a survey by the Ministry of Economy, Trade and Industry (METI) in May 2006, 55% of the responding companies take the Privacy Mark into consideration when they choose contractors.[224]

Another survey[225] shows that information breach and theft are top concerns in using electronic commerce. 75.4% of the respondents are concerned with unauthorized use of the credit card information that they provide when they purchase online. 71.0% of the respondents are concerned with the breach of personal information. In addition, 94.2% of the respondents answer that they would be more ready to buy online if the security or trustworthiness of online shops were certified by a third party.

Disclosure of information breaches is not formally mandated by the Act on the Protection of Personal Information, although entities handling personal information are encouraged to disclose breaches whenever possible in order to prevent secondary damage and similar breaches occurring again. The Ministry of Internal Affairs and Communications, Financial Services Agency, and Ministry of Agriculture, Forestry and Fisheries of Japan have requirements on the formal reporting of information breaches in the guidelines in their respective jurisdictions.

4.4.3 Effectiveness of enforcement mechanisms

Currently, the number of instances where enforcement actions were taken by the government is too small. Therefore, it may be too early to generalize the effectiveness of enforcement by the government.

However, another interpretation of the small number of enforcement may be that government enforcement is required to a lesser extent because the enforcement arrangements other than law and regulation work effectively so far. Still, the fact that enforcement actions may be taken definitely affect the behaviour of the citizens and businesses in favour of protecting personal information and privacy. Opinion polls imply that a majority of the population know about legislation to protect personal information, and many

---

223 By hearing from the Japan Information Processing Development Corporation.
224 <http://privacymark.jp/pr/20060526.pdf>
225 FujiSankei Business i <http://www.business-i.jp/news/sou-page/news/200703090043a.nwc>

of them believe it will promote the protection of personal information. Businesses are taking the issue quite seriously, too. Some of our business respondents turned out to be even positive in trying to comply with the duties to protect personal information because it will eventually lead to confidence from their customers.

4.5 Concluding comments

4.5.1 Characteristics of the Japanese Personal Information Protection Regime

Japanese legislation on personal information protection has been largely successful. An opinion poll taken by the Cabinet Office in September 2006 showed 80 percent of the respondents knew about the Act on the Protection of Personal Information, and three-quarters of respondents believed public awareness and concern for the protection of personal information was increasing. The polls also showed 70 percent of those who know about the Act feel private and public entities have made progress in the protection of personal information[226]. On the business side, another Cabinet Office-led survey of entities handling personal information showed more than half clarified who should be responsible for the handling of personal information and published a privacy policy[227].

Three years after implementation, the effectiveness of the Act for the Protection of Personal Information is should be examined, and whether it requires revision should be considered. The Committee on the Protection of Personal Information, which has responsibility under the Quality-of-Life Council, is nearing conclusion of the first such three-year review. However, when the Committee met in June 2007, it adopted a draft conclusion, which does not mention the possibility of the revision of the Act, although it points out there is much room for additional effort in raising public awareness and understanding concerning the Act. It is highly unlikely that the Act will be revised for some years.

The Act has encouraged both public and private entities to handle personal information in an appropriate manner. It also strengthened existing efforts such as the Privacy Mark. As discussed, the number of businesses and organizations acquiring Privacy Mark accreditation increased significantly after implementation of the Act on the Protection of Personal Information.

---

226 Cabinet Office poll on the protection of personal information is available from <http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20070202kojin3-2.pdf>. 1,811citizens aged 20 or above from a sample of 3,000 responded to the survey.

227 Cabinet Office survey on the protection of personal information by private entities <http://www5.cao.go.jp/seikatsu/shingikai/kojin/20th/20060728kojin3-1.pdf>. Sample: 20,000 entities, 2,335 replies collected.

There have been seen cases where citizens and businesses overreacted to the Act based on misunderstanding of its provisions and the general legal framework. Misunderstanding of the objectives of the Act led to a number of notable cases where even lawful disclosure of personal details was declined based for misguided reasons. However, it is expect that this kind of overreaction will diminish with time.

In the short-term, the personal information protection regime added an additional burden and responsibility to enterprises, whether private or public. However, the market recognized the benefit and importance of having personal information protection in place. It is also beneficial for enterprises to comply with the law in order to achieve a balance between „use“ and „protection.“ If enterprises ignore such risks and do away with sufficient investment in information security and personal information protection, they will end up taking action only after an incident happens. Such remedial action will in many cases cost as much as any reasonable preventative measures, and will also cause significant damage to the enterprise’s reputation.

Reputational risk has become and important factor for Japanese business as they determine their privacy policies and take preventative measures.

In Japan, there are no statutory provisions protecting privacy, and currently no rulemaking is scheduled. In practice, privacy is protected through the right to pursue happiness defined by Article 13 of the Constitution of Japan, and provisions on defamation or contempt in the Penal Code and tort in the Civil Code. But these are not sufficient to protect privacy to the fullest extent.

Since very few privacy or personal information protection cases have been handled under the Penal Code, it is impossible to take a preventative measure citing precedent. Besides, the right to self-determination and right to peaceful life are not recognized as such in Japanese legal context. However, with increasing awareness of privacy protection, some experts point to the need to legislate an act to protect „privacy in general,“ rather than the current indirect approach to privacy.

The Act on the Protection of Personal Information does not use a term „privacy“. The scope of protection is personal information, but this protection is applied indirectly through the regulation of entities handling personal information. Privacy is protected simply as a side-effect of this regulation of how personal information is handled.

Also, some consider the Act on Protection of Personal Information is too strict in terms of regulation. One expert interviewed claimed the Act is based on the old-fashioned OECD 8 principles. It makes no distinction between basic and sensitive information, which, the expert claims, results in confusion and overreaction among citizens when interpreting of the Act. Other experts point out that in the current environment the negative „chilling effect“ of people misunderstanding the intent of the legislation and refusal to release information overrides the positive effect of protecting information. However, there is widespread agreement that Japan must have a legal system to protect privacy

or this aspect of personal information. The current regulatory environment may be improved by revising the current legal system.

As a conclusion, statutory provisions on „privacy“ should be established. Also, jurisdiction of the Act on Protection of Personal Information should be limited to only privacy related data, all other personal information should be left out. By so doing, the current confusion where some believe almost no personal information may be shared would be avoided. It is important that the law focus on preventing the „abuse“ of information, but not to limit proper „use“ of information.

5 South Korea

The Constitution of the Republic of Korea (South Korea) is explicit in its protection of privacy, Article 17 states „The privacy of no citizen shall be infringed“, Article 18 that „The privacy of correspondence of no citizen shall be infringed.“ At the same time, South Korea is a relatively young democracy. Direct and fair Presidential elections were not held until 1987, and when we look at the situation of privacy in society, we find strong protections in the law addressing some industry sectors, but privacy as a fundamental right has only recently become a concern for society at large.

An example of this apparent lack of sensitivity to the need for privacy is the widespread use of the National Resident Registration Number in offline and online transactions. The resident registration number is a 13-digit number issued to all South Korean residents. The first six digits indicate a person's date of birth, the seventh their gender. The next four digits signify a code for the person's place of birth. The twelfth digit is used to differentiate those born on the same date in the same place and the final digit is used to verify that the number has been recorded correctly, a check digit derived from the others.

The resident registration number itself reveals some personal information, but it how it is so extensively used that creates the potential for privacy violations on a massive scale. The number has long been used to identify a person in commercial and other interactions: for identification in banking and commerce or employment, and to simply prove a person is who they say they are. It is now also being used widely online for many kinds of identification purposes, from registering for a new email account, which cannot be created anonymously, to simple registration for an e-commerce site, registration for a web portal or search engine and any number of services. Use of the number has become almost a default requirement and it is given out freely.

This extensive use leads to a situation where a number unique and identifiable to a person is used in many different databases associated with many different types of data, from communication –email, online discussion forums, social networking systems– to e-commerce transactions, search histories and web browsing. The potential for privacy violations are very great.

In July 2006, a search program based on Google developed by MIC found resident registration numbers of 903,665 Koreans on 6,337 websites. According to MIC, the entire 13-digit number of 95,219 Koreans was available on the websites of 993 organizations, 334 of which were public institutions and 659 private entities. The first six digits, identifying a person's date of birth, were available for 808,446 people on 5,344 websites[228]. Also in 2006, 1.2 million people found their resident registration numbers had been

---

228 „Gov't Search Reveals Massive Online ID Leak“, 1 August 2006, Digital Chosunilbo <http://english.chosun.com/w21data/html/news/200608/200608010032.html> (last accessed June 2007)

used to create accounts for the popular online game Lineage. Hackers used the numbers to make fake accounts to create virtual goods useful in playing the game and progressing through its many levels, selling these virtual items for real money.

In March 2007, the Ministry of Government Administration and Home Affairs began an online program to allow users search for use of their resident registration numbers on Internet websites. The program was available for one month and was accessible through the ministry's, municipal governments', and others agencies websites to search the Internet and compile a list of websites using their registration number. The user could then begin process which would require the website operator to delete the number.

The government, Ministry of Information and Communications, is trying to find alternatives to the use of the registration number. To date it has not invested in developing such substitute mechanisms, instead the ministry has attempted to impose a requirement to develop substitutes on the private sector. Some larger companies are developing proxy systems that separate the resident registration number from personal data collected or processed because of the person's use of their service, but there is no national initiative to address the problem.

Government's lack of support for industry in this area is surprising in that is goes against a history of government led industrial development and support for industry, and is not consistent with current national IT policies.

Since the 1950s South Korea has advanced rapidly from being one of the poorest countries in Asia to the 11th largest (GDP) economy in the world[229], growth that has been the result of strong government industrial policies, particularly support for large conglomerates known as chaebol. Official support for the chaebol collapsed after the economic crisis of 1997, but ministries, particularly the Ministry of Information and Communications continue to use policy measures to encourage and support industry sectors.

South Korea is one of the world's most technologically advanced countries and the government's industrial policy today focuses on promoting Korea further as an advanced ICT nation and adopted the concept of „ubiquitous information society" as the national industrial policy.

U-Korea (U-biquitous Korea) or IT839 strategy is based on the idea of anyone and anything having the potential to always be connected to the network at anytime and from anywhere. It offers both great benefits and the potential for significant abuse. User benefits such as location aware information services, RFID chips helping with purchases or identifying dangerous substances and enabling more effective delivery or

---

229 World Bank, July 1, 2006, data for the year 2005. International Monetary Fund, World Economic Outlook Database, September 2006, data for the year 2005.

distribution mechanisms, need to be balanced against the potential for abuse through increased surveillance and traceability, and the potential breach of personal data on an unprecedented scale.

A „Protection of Location Information Act“ was enacted in 2005, and a telecommunications industry standard for the use of RFIDs and protection of privacy has been adopted. As is the case with many other new acts administered by the Ministry of Information and Communications, the protection of location information act also has a role in promoting location services industry. This dual role of privacy protection and industry promotion is a feature of Korean data protection legislation.

Legislation to protect privacy and promote trust is in place for the ICT sector but not in the private sector generally. Legislation is sectoral and administered by the relevant ministry. New legislation addressing privacy protection for the private sector broadly is under consideration, three different drafts are currently before the National Assembly. Each draft suggests different measures and degrees of protection, but all propose that the protection of privacy should become the responsibility of the Prime Minister’s office, rather than industry specific ministries.

Korea is among the leading nations in the deployment of very high-speed networks, advanced ICT applications, mobile phone technologies and other „ubiquitous“ services. However, legal protections necessary to ensure privacy and trust in this new environment are lagging. It is not clear that legislation protecting against abuses of personal data has caught up with the enthusiasm for the positive aspects of ubiquitous information society and the powerful drive of the U-Korea strategy to develop and implement new technologies, services and applications.

5.1 Measures to enhance privacy and trust

South Korea is a signatory to the Universal Declaration of Human Rights, and of the International Covenant on Civil and Political Rights. Fundamental and inviolable human rights are also provided in the South Korean Constitution, enforced in 1988. In addition to Article 17 and 18 which make specific provisions for rights relating to privacy, the Constitution provides rights guaranteeing equality and non-discrimination, to personal liberty and personal integrity, and freedom of speech, press, assembly and association. In the past, many of these rights have been denied in the name of National Security, particularly relating to the country’s relationship with North Korea, and abuse continues particularly in areas of wiretapping and surveillance.

However, since the Presidency of Kim Dae Jung (1998-2003) and more notably Roh Moo-Hyun (2003 - present), such violations have been reducing in severity. President Roh has sought to increase the direct involvement of Non-Governmental Organizations and citizens in policy-making processes, this has served to increased oversight of official activities and raised awareness of rights issues in Korean society. The involvement

of Korean civil society in national policy making processes is one reason concern for fundamental privacy rights is increasing. The high level of use of ICTs in Korea and people's experience and knowledge of these technologies may explain why we often hear strong concerns expressed for the protection of rights in the nascent ubiquitous network society.

Privacy law has been extended with the Korean courts recognizing a „right of publicity", allowing an individual to control the commercial use of their identity[230]. The Korea Information Security Agency (KISA) found many websites collected personal information without user's permission and the agency has begun levying penalties on transgressors. Spam has become a severe problem, many Koreans find email made useless by the amount of spam flooding their mailboxes. These massive problems with spam continue regardless of legislation implemented in 2001 adopting an opt-out approach to spam and increasing the amount of monetary and other sanctions that can be applied to spammers. More recent legislation grants ISPs the right to develop criteria for blocking spam and develop means to prevent its circulation.

Korea has adopted the OECD privacy guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and implemented them in laws enacted between 1994 and 2002.

Act on Promotion of Information and Communication Network Utilization and Information Protection

The Act on Promotion of Information and Communications Network Utilization and Information Protection (enforced in January 2001) is the main piece of legislation for the protection of privacy in electronic communications. Article 1 defining the purpose of the Act is quite clear, the Act promotes the use of information and communication networks and protects user's personal information when they use information and communication services. The legislation is more than a law about privacy rights, it serves as industrial policy for the promotion of Korean ICT industries. The second chapter of the Act addresses the promotion of utilization of information networks, privacy and security are addressed in later chapters. It is a sectoral act addressing the information and communication industry and is administered by the Ministry of Information and Communications (MIC).

A companion Act dealing with information protection in the public sector, Act on the Protection of Personal Information Maintained by Public Agencies 1996 (enacted 1998) secures personal information held by public agencies and gives allows citizens rights to control that information (details of the act are discussed below.)

---

230 H. Nam, „The Applicability of the Right of Publicity in Korea," 27 Korean J. of Int'l and Comp. L.45, 49 (1999). See also W. Han, „Infringement of the Right of Publicity and Civil Liability," 12 Human Rights and Justice 109, 116 (1996) (in Korean). Referenced in Privacy and Human Rights 2005: South Korea, Electronic Privacy Information Center Washington, DC, USA, Privacy International London, UK.

The Promotion of Information and Communications Network Utilization and Information Protection provides a comprehensive regime for the promotion of use of information networks and the protection of information carried over those networks in the private sector. The Act adopted eight principles recommended by the OECD 1980 privacy guidelines, and these form the basis of Korean policy towards privacy protection. The Act defines personal information as „information concerning anyone living that contains the code, letter, voice, sound, and/or image, which allows for the possibility for that individual to be identified by name and resident registration number (including information which, if not by itself, allow for the possibility of identification when combined with other information). „Users" are defined as „individuals who use the information and communications services rendered by information and communications service provider". Service providers should gather the minimum amount of data necessary.

Chapter 4, „protection of personal information", Chapter 5 „protections of juveniles in information and communications networks", and Chapter 6, „securing the safety of information and communications networks" are the key privacy related sections of the Act.

The rights of users are well defined. Provisions on collection of personal information are provided in Articles 22 and 23. Information and communications service providers must obtain user consent before gathering personal information unless the information is simply part of a process of actualizing a contract (Article 22 (1)). Furthermore, if personal information is to be passed to a third party then the reason for this transfer and the identity of the third party must be notified to the user (Article 22 (2.3)). Information must not be passed to a third party in violation of these provisions.

And service providers may not gather any personal information „such as political ideology, religion, and medical record, which is likely to excessively infringe upon the rights, best interest, and privacy of the relevant user", unless the collection of such information is granted under other Acts, for example, the Medical Information Act (Article 23 (1)). Service providers must also gather the minimum information necessary to deliver their information and communications services (Article 23 (2)).

Users may withdraw from an agreement made under article 22 giving their consent for the service provider to gather and hold information about them (Article 30 (1)). Users are entitled to control their own information: they have a right to review personal information held by a service provider and to request that it be corrected if found to be erroneous. The service provider must take prompt action to destroy any personal information on cancellation of consent, and must quickly take steps to make any legitimate corrections.

The Act provides information protection for children (under 14 years of age), a legal representative must provide consent to gather children's personal information. The Act contains a chapter providing measures to protect juveniles from harmful information distributed over communications networks such as „lascivious sex and violence information" and recommends the development and dissemination of screening software

and „juvenile protection technology“. Article 42 states that content harmful to juveniles as described by the Juvenile Protection Act must be „labelled as harmful to juveniles in a labelling method stipulated by Presidential Decree.“

A user may claim compensation from a service provider if any of the above provisions are violated, and the service provider cannot be released from their responsibility if they fail to prove the „non-existence of their aberrant intention or negligence regarding the harm to the user“ (Article 32). This article only describes indemnification, the Act provides legal penalties for some violations under a section for „Penal Provisions“ (Chapter IX.)

Article 50 of the Act provides a right for the user to refuse to accept unsolicited advertising by email. Users have an option to opt-out after which sending further spam email is prohibited. The subject line of all unsolicited email must include the words Advertisement or Adult to indicate their content, and opt-out instructions and the name and contact address of the sender must be included.

Information and communications service providers have a number of defined responsibilities. They are to minimize personal information collected, and to notify and clearly explain to users how their personal information will be used and processed. Out of purpose use of personal information is prohibited, particularly the transfer of information to third parties, and the service provider has a responsibility to allow users to access information held about them and to correct that information if necessary. Security of information must be ensured, both through technological, managerial and administrative safeguards, and personal information must be promptly destroyed if the user withdraws their consent. The service provider should designate a person in charge of administering the personal information, this person should handle users' complaints about the use of personal information.

Section 4 of the Act creates a „Personal Information Dispute Mediation Center“ to mediate disputes concerning personal information, and describes the roles of authorities responsible for administering information protection measures. The mediation centre and related processes was created to be a lightweight and fast moving self-regulatory process for dealing with complaints and problems regarding personal information. These self-regulatory measures are described in Section 5.2 below.

The Korea Information Security Agency (KISA), operating as an agency of the Ministry of Information and Communications, has the duty to implement measures necessary to protect information and for the secure distribution information. KISA is responsible for oversight of the mediation centre and related self-regulatory activities. There is no central data or privacy protection commissioner empowered to ensure the law is applied, KISA's role is somewhat equivalent to that of a data protection commissioner, but it is not independent of government and does not have full powers of investigation and enforcement.

The Act was revised on 25 May 2007 (effective from 26 May 2008) with the intention of enhancing provisions concerning self-regulation. Section 44-4 of the Act allows service provider's organizations to establish and implement guidelines that protect users' information and ensure safe and credible information and communication services. The provision is very general and has the nature of self-regulation imposed through the Ministry's external powers. The revision builds on earlier paragraphs of section 44 (44-2 and 44-3) which require online service providers to implement „self-regulatory" guidelines regarding practices for the deletion of articles that infringe on other's privacy, defame another person or persons, and may be harmful toward juveniles.

Act on the Protection of Personal Information Maintained by Public Agencies

Enacted 1998, the Act on the Protection of Personal Information Maintained by Public Agencies secures personal information held by public agencies and gives allows citizens rights to control that information. Older than the corresponding protecting information controlled by the private sector, the public sector act does not address any broader public policy issues, it only addresses the protection of information. The Act is administered by the Ministry of Government Administration and Home Affairs (MOGAHA).

The Act defines a „public agency" as „any national administrative agency, local government, or other public agencies provided by Presidential Decree", and „Private information ... means the information concerning a living person including the full name and resident registration number, etc., by which the individual concerned can be identified (including information by which the individual concerned cannot be identified but can be identified by simple combination with other information)", Article 2, sections (1) and (2) respectively.

Users have the right to make a written request to inspect any personal information on file held by any agency. On receipt of such a request, the head of an agency must, if there is no justifiable cause, allow the user to inspect the information within 15 days of receipt of the request. Users are also able to request that information about them be corrected, and again the head of the agency concerned should respond without delay. Should the agency refuse to accept a request for inspection or correction, a user can appeal under the Administrative Appeals Act.

Public agencies may collect and possess „as many private information files as is necessary to properly execute jurisdictional operations" (Article 4 and Article 5), however, „the head of a public agency shall not collect private information that may noticeably infringe upon the fundamental personal rights of a person such as one's ideas and belief" (Article 4.) The agency should inform MOGAHA of the type of information it collects, for what purpose it is collected, and should make a public announcement to this effect at least once each year in the official Gazette. MOGAHA also publishes a public list of these databases in an official journal. Each agency must take measures to ensure the security and integrity of the information it collects. Questionnaire respondents and people inter-

viewed did not express confidence in MOGAHA's enforced of the legislation, believing it to be lenient.

Agencies should not transfer information they manage to another agency for purposes other than those for which it was originally collected. In addition, any person within the agency who has access to the personal information the agency manages must not disclose or leak the information.

The Minister of Government Administration and Home Affairs may investigate the conditions by which an agency manages personal information, and may provide advice and recommendations regarding its protection. The Act provides leeway for agencies in the collection and handling of personal information they possess, however there are penalties that can be imposed for violations of the Act.

Protection of Communications Secrets Act 2002

The purpose of the Act is to protect secrecy of communications and to promote freedom of communications. Administered by the Ministry of Information and Communications, the Act covers all communications under the Ministry's remit, i.e. postal mail services and all electronic communications, including Internet. It describes broad arrangements under which communications can be monitored or intercepted.

As noted above, while the number of interceptions has declined slightly in recent years, the total remains high. According to a report by the Electronic Privacy Information Center and Privacy, MIC disclosed 917 cases of government wiretapping in the first half of 2004, an increase of 14.8 percent on the second half of 2003.[231]

Article 3, the main provision of the Act, states „no person shall censor any mail, wiretap any telecommunications, provide the communication confirmation data or record or listen to conversations between others that are not made public without recourse to this act, Criminal Procedure Act or the Military Court Act". Communications acquired through illegal means in violation of Article 3 will not be admissible as evidence. The Act provides significant exemptions allowing for the restriction of communications when there is a „substantial reason to suspect that a crime ... is being planned or committed or has been committed, and it is difficult to prevent the committing of the crime, arrest the criminal or collect the evidence".

Measures to „restrict" communications can be granted to a prosecutor or police officer conducing a criminal investigation by application made in writing to the competent court. Communications may also be restricted for reasons on national security, „when the national security is expected to be put in danger and the collection of intelligence is re-

---

231 Privacy and Human Rights 2005: South Korea, Electronic Privacy Information Center Washington, DC, USA, Privacy International London, UK.

quired to prevent such danger“. Emergency measures to restrict communication without seeking permission of a court may be taken to counter an imminent threat to the national security, planning or execution of serious criminal acts, acts that may cause death or serious injury.

Any person who intends to make, import, sell, distribute, possess, use or advertise any tapping equipment must obtain an authorization of the Minister of Information and Communication. This provision does not apply in the case of other government agencies, however, any state agency (except the intelligence and investigative agencies) must report the introduction of any tapping equipment on a six-monthly basis to MIC.

Article 11 defines an obligation to keep secrets, and prohibits public officials who have obtained any communications using measures under the Act from disclosing or leaking any information they have learned during the course of their work.

Protection of Location Information Act (2005)

Effective since August 2005, the act requires carriers to obtain consent before location information is collected, used or provided. The act stipulates penalties ranging from fines to imprisonment for violations. When providing location information to third parties, carriers must immediately notify the person whose information is being disclosed. Individual location data should only be utilized without prior agreement for purposes of public welfare, the most obvious and non-intrusive being use by emergency services to locate a caller in the case of an emergency.

However, according to a report by the Ministry of Information and Communication „Status on Location-Based Services of Mobile Telecommunications Companies“, the three major mobile carriers provided location information in 180 million cases from August 2005 to June 2006 and did not provide such notification[232]. The law states users should be notified each time location information is transferred to a third party, however the law does not clarify how notification should be carried out. Carriers have tended to provide notification to user’s mobile portal mailboxes, most users would not know about these notifications as new messages to these portal mailboxes is not typically sent to the user’s phone. Access to these mailboxes is usually fee based, users would typically need to pay to receive these notifications from the carrier.

The Protection of Communication Secrets Act is currently being amended in early 2007 to allow law enforcement authorities to ask service providers to provide GPS guided information on the location of surveillance targets.

---

232 „Wireless Carriers „Illegally“ Operated Tracking Services“, Digital Chosunilbo, 5 February 2007, <http://english.chosun.com/w21data/html/news/200702/200702050016.html> last accessed June 2007.

National Human Rights Commission (NHRC)

Created by the National Human Rights Commission Act 2001, the Commission has a broad mandate to investigate and remedy human rights violations and discriminatory acts. Human rights being defined as rights guaranteed by the constitution and international human rights treaties entered into and ratified by the nation. Complaints can be brought to the Commission when provisions of Articles 10 through 22 are violated by state agencies, local governments, detention or correctional facilities while performing their duties. The Commission can only consider complaints against private sector entities based on allegations of discriminatory acts. Consequently the Commission only hears privacy related complaints against public sector entities.

Article's 17 and 18 of the constitution relating to the protection of privacy come under the Commission's competence, however privacy is not specified in the National Human Rights Commission Act and is not a major focus of the commission's work. Only a small number of staff is assigned to privacy and data protection issues and experts suggest the Commission lacks trained staff and expertise in the area. To monitor all state and local government agencies effectively the Commission staff working on privacy issues would need to be increased significantly and provided with appropriate training.

The Commission has recently been receiving complaints about the use of CCTV camera and biometric systems such as iris and finger print recognition systems.

Complaints about privacy account for only about five percent of all complaints, however the Commission does pass judgments. For example, in May 2007 the Commission ruled on a complaint that a person trying to use a telephone information service provided by a call centre of the Korean Customs Service was asked to provide her 13-digit National Resident Registration Number. The complaint was that it was unreasonable to require personal information including the resident registration number for services that do not require personal identification. The Commission ruled that forcing a person to provide their resident registration number in this case was a violation of Article 17 of the constitution, and recommended to the Customs service that users should be able to gain access to its information services without having to provide their resident registration number.

The Commission can only issue recommendations, or present opinions in court cases. It cannot require other agencies to make changes or impose penalties on them. However, Commission has significant standing in Korean society, it is strongly associated with democratic reforms of recent decades and its recommendations carry weight.

Other legislation that affects privacy and trust of electronic communications include:

The Basic Act on Electronic Commerce, aspects of which address privacy protection and the security of computers and networks used for electronic commerce, including the

obligations of information providers and online retailers and the government regarding the protection of consumer information.

The Consumer Protection Act, which prevents harm to consumers and develops standards for consumer rights.

The Information and Communication Network Act, which provides obligations on information communication service providers regarding privacy protection.

The Framework Act on Informatization Promotion, which identifies the protection of privacy and maintenance of security of information and data as being among the basic principles of informatisation policy. The purpose of the act is to provide guiding principles for achieving an „advanced information and communications industry infrastructure".

The Electronic Signature Act, requires certification authorities to protect personal data when carrying out all certification service, and adopts sections of the Act on Promotion of Information and Communications Network Utilization and Information Protection to protect users of digital signatures.

MIC Guidelines and Directives, The Ministry of Information and Communications also issues directives and guidelines on matters concerning personal information protection to telecommunications and Internet providers. These directives and guidelines are intended to respond quickly to emerging issues or to regulate specific service providers in detail.

Directive on Personal Information Protection (DPIP) and Guideline on Personal Data Protection over the Internet (GPDPI) are examples[233]. DPIP prescribes privacy principles and provisions in more detail than the data protection legislation, which is based on the OECD's 8 privacy principles. For example the Act stipulates that service providers have the duty to obtain the data subject's consent before collecting personal information. The DPIP describes how the service provider should obtain consent and how it should collect and use a user's information such as their telephone number, email address, electronic signature, website information, etc. GPDPI stipulates similar requirements for Internet service providers and website managers when they collect a user's personal information. Other guidelines have been introduced on privacy protection for example in the use of CCTV, RFID systems, the use of bio-metric information.

MIC's „RFID Privacy Protection Guideline" was issued in the autumn of 2005 (dated July 2005, but not implemented for some months.) The Guideline is not mandatory but is applicable to both the public and private sector. The Guideline identifies „personal information" as information about any living person that may identify that person, including information that when combined with other information could identify the person.

---

233 Unofficial translations of the guideline's titles

The recording of personal information in the RFID tag is not permitted without the user's consent, and if such information is recorded what is recorded shall be notified to the user in an easy to understand manner. The service provide must notify and gain the user's consent if they wish to link information contained in the RFID tag to other personal information.

The RFID service provider must make clear when an RFID is attached to an item, and a user must be able to easily deactivate any RFID tag attached to an item after purchase. Unless explicitly permitted by law, RFID tags may not be attached to any article in such a way that the user will be unaware of the tag's presence. RFID tags may not be implanted in the human body. The guideline has to some extent been superseded by the industry self-regulatory measures described below, but until such time as a law about the use of RFID's an privacy is enacted, MIC's guidelines apply to the use of RFIDs in all sectors whereas the industry standard on RFID's an privacy is observed only by the telecommunications industry. Any new law would be sectoral and the public sector likely subject to different conditions. However, at the moment the guidelines apply to both the public and private sectors.

In January 2006, MIC released new guidelines restricting the collection of bio-metric data from individuals. The guidelines apply to both government and private sector. Individuals must give their consent before bio-metric information is collected, and data collectors must return or destroy the data at the individual's request. The guidelines also require data collectors to hold the data securely and prevent unauthorized access. The guidelines were issued after a representative of the ruling Uri Party revealed that the MIC had compiled a bio-metric database on 5,620 people, including juveniles.

MIC has also introduced guidelines on installing and use of CCTV cameras to protect the privacy of individuals and reduce infringements. Bills about the use of CCTV are being drafted in cooperation with the Ministry of Government Administration and Home Affairs.

5.2 Arrangements other than law and regulation

5.2.1 RFID tags and privacy

In March 2005 the Telecommunications Technology Association published an „RFID Privacy Protection Guideline" as an industry standard. Members of the association and NGOs expert in privacy issues drafted the standard. As a standard, it does not carry the authority of enacted legislation, but has been adopted by the Korean telecommunications sector and is important when considered as part of the U-Korea national ICT plan.

The standard places limitations on the writing of personal information on RFIDs and the type of information that may be collected. Consumers should be notification when an RFID tag is attached to an object, they should be informed of the features and function of the RFID tag, and what information is recorded by the RFID tag. In the case of items used by the public a mechanism for stopping the function of the RFID should be provided. The standard also requires notification is made when RFID readers have been installed, and consumers are informed about the technical and administrative measures taken to protect personal information in the RFID system. The standard also states RFID tags should not be transplanted into the human body.

The standard's rules only apply to collection of information that affects personal privacy.

5.2.2 Korea Information Security Agency and the Personal Information Dispute Mediation Committee (PICO)

The Korea Information Security Agency (KISA), operating as an agency of the Ministry of Information and Communications, has the duty to implement measures necessary to protect information and for the secure distribution of information. One of KISA's roles under the Act on Promotion and Communication Network Utilization and Information Protection is to operate the Personal Information Dispute Mediation Committee (PICO).

Created by Presidential Decree Article 26 „Operation of Reporting Center on Infringement of the Personal Information", PICO was founded to protect personal information in the private sector and to handle complaints regarding the infringement of personal information under the Act on Promotion and Communication Network Utilization and Information Protection.

The committee has 15 members, senior people from academia, public sector, legal profession, service provider industry and communication user associations, and not for profit non-governmental organizations. KISA acts as the secretariat to the committee.

PICO functions as an alternative dispute resolution system, created as a quick and convenient means to mediate disputes. It monitors compliance with the information protection provisions of the Act and receives complaints from users. The dispute resolution system functions either online or offline. PICO investigates the facts of a complaint and advises corrections in the case of minor violations.

Any person may file an application for the mediation of a personal information dispute involving a communication service provider, or any dispute involving personal information processes by a travel agency, airline carrier, department or discount store, hotel, or educational institution. These types of organizations were added to the scope of the Act as it was felt they collected and processed large amounts of personal information utilizing information and communications systems.

PICO's mediation process is free of charge. Within 60 days of receiving the application, the committee will examine the case and prepare a draft mediation. The parties in the dispute then have 15 days in which to decide whether or not to accept the mediation. If they accept then the committee prepares a written mediation which both parties will then formally agree to. Parties in the dispute have no legal obligation to follow the mediation procedure, and may withdraw from the process at anytime. If a mediation plan is accepted it is considered the equivalent of an agreement in civil law between the parties.

The committee may also reject to consider an application for mediation, and the grounds for rejection must be informed to both parties. If both parties fail to agree on the committee's mediation, then the committee can re-examine the case and provide another mediation within a further 60 days. The committee will stop handling the dispute if either party files a lawsuit regarding the dispute.

If the case brings to light a significant violation of the Act and the service provider does not remedy the situation then PICO notifies the Ministry of Information and Communications, police or prosecutors office as appropriate. In 2003 PICO received 845 complaints, 497 of which went through the mediation process and mediation was accepted in 482 cases. Three complaints progressed to legal action. In 2004 PICO received 1,210 complaints, again over 98% were resolved through mediation. In both 2003 and 2004, the most common complaint was the collection of a minor's personal information without the consent of a legal guardian, over 50% of complaints in 2003 and 30% in 2004.

PICO is one of a number of alternative dispute resolution systems created to address issues broadly concerning electronic commerce.

5.2.3 Privacy labels

Korea Association of Information & Telecommunication (KAIT) has implemented a system of certification to assess the level of security and privacy protection for Internet sites. Established under provisions of the Act on Promotion of Information and Communication Network Utilization and Information Protection, KAIT was created as a public-service corporation and is supervised by the Ministry of Information and Communications. However, it operates as a non-profit organization independent of the Ministry and its activities related to privacy can be viewed as self-regulation rather than being imposed through legislation. KAIT's mission is to strengthen the global competitiveness of the domestic ICT industry.

KAIT introduced a pair of trustmarks, the „i-Safe" security mark and „e-Privacy" privacy mark, awarded to sites that meet a set of criteria for implementation of security standards and policies and the protection of consumer privacy. The i-Safe mark was estab-

lished in July 2000, and e-Privacy in February 2002. The marks are administered by a 15-member committee that includes members from MIC, Fair Trade Commission, Consumer Protection Board, lawyers and academic experts.

The e-Privacy mark is designed to guarantee privacy protection, the i-Safe mark has two types: the first guarantees privacy protection, system security, and safety for online shopping, the second guarantees privacy protection, system security, and consumer safety using financial and medical services online.

The e-Privacy mark can be displayed on Internet sites that safeguard the collection of personal information, maintain the rights of data subjects (users), comply with disclosure responsibilities, safeguard the rights of children under the age of 14, and provide remedies for user disputes over the treatment of personal information. These are essentially the main provisions of the Act on Promotion and Communication Network Utilization and Information Protection, and also uphold the OECD's eight privacy principles.

The certification process for the e-Privacy mark reviews 84 criteria and requires that the organization has a privacy policy and internal management of privacy access to customer information. The i-Safe mark reviews 199 criteria (depending on sub-type). As of February 2007 154 sites had been certified and granted the e-Privacy mark. The i-Safe mark had been award to 48 sites by February 2007. Indications are that the end of 2006 had certified 180-190 companies, most being Internet service providers or related online service companies. 204 sites had been certified at the end of May 2005, the total by the end of 2007 is not expected to exceed 230. Certification for the i-Safe mark includes on-site inspections.

Certified sites are reviewed annually and non-compliance results in a notice recommending corrections, a warning of recommendations are not acted on, and then either a withdrawal or permanent termination of certification with no reapplication for certification possible for one to three years.

The low number and narrow sectoral interest is the result of the marks being closely associated with the industry specific Act on Promotion and Communication Network Utilization and Information Protection. The data protection law is not generally applied to all industries so few have knowledge of or interest in the privacy mark program. Also KAIT does not promote its services aggressively, it provides the marks on a not-for-profit basis. Five common types of site use the marks: portal sites, e-commerce websites including some general merchants, online gaming services, telecommunication and ISPs, and a limited number of financial sector companies. Changes to the marks certification policy and criteria come through internal development, and to reflect any amendments to the Act.

KAIT also supports and operates the Chief Privacy Officer Council, a group of privacy officers established as a discussion forum, to research projects to develop industry-

specific privacy proposals and guidelines. The Council also submits proposals to government on improvements to relevant laws and policies.

KAIT cooperates internationally with the Japanese Information Processing Development Corporation (JIPDEC), and is beginning to build a relationship with eTRUST of the United States. KAIT and JIPDEC established as mutual recognition agreement „Korea-Japan Reciprocal online Privacy Mark Program“ in 2002 and mutually recognize the validity of each other's marks.

5.3 Enforcement powers

Penalties for violations of laws protecting privacy are potentially severe, with prison terms with labour recommended in many cases. However, the laws seem not to be enforced to their full powers, particularly in instances of tapping and similar breaches. The statutory penalties for the main laws are described below.

Promotion of Information and Communication Network Utilization and Information Protection

Article 62. The penalty for disclosure of personal information to third parties (Article 22 and Article 24 of the Act), or for a person who harmed any other person's information, or infringed, stole or disseminated the secrets of any other person in breach of Article 49 (Protection of Secrets) shall be punishable by imprisonment with prison labour for not more than 5 years or by a fine not exceeding 50 million won.

Article 64. Any person who provided media materials that are harmful to juveniles for earning profits without affixing a warning label shall be punished by imprisonment with prison labour for not more than 2 years or by a fine not exceeding 10 million won.

Article 66. The representatives of a corporation, agent, other employee of a corporation or an individual in violation of Articles 62 or 64 shall also be punished by a fine described in the relevant Article in addition to the punishment of the actor committing the act in violation of those articles in connection with the business of said corporation or individual.

Article 67. Describes fines for negligence by persons or corporations for various failures to obtain user's consent before gathering personal information according to Article 22(2), or for breaches of Article 23 prohibiting the collection of certain types of personal information, or for failure to notify the user for various types of change in service or business practice (outsourcing, transfer through a merger or other acquisition, change in internal information management, etc). A fine not exceeding 5 million won may be levied.

Protection of Communications Secrets Act 2002

Penal provisions for violation of sections of the Act are strict, but there is some doubt as to whether they are enforced. Some examples of penalties that may be administered include contravention of Section 3 of the Act by censoring mail, wiretapping, recording or listening to conversations of the act, or a person who has leaked or disclosed such communications or conversations, shall be punished by imprisonment with prison labour for not more than 10 years or by suspension of qualification for not more than 5 years. Anyone who commissioned or asked for cooperation in executing communication restricting measures without appropriate permission of a court or under emergency measures shall be punished by imprisonment with prison labour for not more than 10 years. A person who violated Article 11's obligation to keep secret the content of communications learned during the course of an action to restrict communications shall be subject to imprisonment with labour for a terms not exceeding 5, 7 or 10 years depending in the circumstances of the case.

Penalties for failing to keep written permissions for communication restricting measure or for an emergency wiretapping statement, for manufacturing, possession, importing, sale or distribution of tapping equipment with obtaining authorization are for imprisonment with labour for not more than 5 years or by a fine not exceeding 30 million won. A person who fails to follow provisions of the act for discontinuing any emergency communication restricting measures shall be punished by imprisonment with prison labour for not more than 3 years or by a fine not exceeding 10 million won.

5.4 Effectiveness

Questionnaire respondents and others interviewed in Korea all requested anonymity. On the record comments would need to cleared by their respective organizations, which respondents suggested would either lead to participation being denied or responses diluted. The complex nature of the questionnaire and that people were responding in a second language further strengthened their wish not to be quoted.

As the titles of key pieces of legislation make clear, to-date the purpose of data protection law in Korea has been twofold: to enhance privacy protections but also, and perhaps primarily, to promote the development of the information and communication business sector. The government's focus on ICT industrial policy has been extremely successful, Korean technology companies are now global brands, and Korean citizens among the world's most advanced users of broadband and other communication technologies. However, almost all respondents suggested that Korean users were at least until very recently generally unaware of their privacy rights and were probably disinterested. Respondents suggested that this situation was changing and privacy was becoming an important issue, not least because of concerns over the misuse of the National Resident Registration Number (RRN).

Respondents broadly agreed the greatest threat to privacy was the wide-spread use of RRNs as a means of identification for even the most trivial of online uses. Users tend to give the number out freely for trivial registrations, but it is also used in financial transactions, employment and other important transactions. KISA reported it received 18,206 complaints about the misuse of RRNs in 2005 and 23,333 complaints in 2006 (these are specific individual complaints in addition to the large breaches of RRNs noted above.) One person interviewed suggested the resident registration number could be described as a privacy-violating infrastructure in its own right.

The Ministry of Information and Communications (MIC) and Korea Information Security Agency (KISA) have encouraged industry to come up with solution to the RRN problem. However, respondents from two major communications companies remarked that the government has not taken the lead in research, instead expecting the private sector to carry most of the costs. One possible answer to the problem called the Internet Personal Identification Number Service (i-PIN) is now undergoing trials. i-PIN uses a system of trusted third parties to provide a replacement online identity number not associated with any personal information. Companies expect implementation of the new service to be expensive and respondents commented they are not receiving support from the government to meet these costs. The official approach toward privacy was well illustrated by one civil society interviewee who commented that until now government's priority had been to promote industry concerns over the public interest, privacy protection was only beginning to become important.

5.4.1 Effectiveness of legal and other measures

Legislation, particularly the Act on Promotion of Information and Communication Network Utilization and Information Protection, Act on the Protection of Personal Information Maintained by Public Agencies, and Protection of Communications Secrets Act 2002, provide MIC, KISA and the Ministry of Government Administration and Home Affairs (MOGAHA) with broad powers to protect privacy in electronic communications, however the legislation has not been rigorously enforced. Some respondents commented that while businesses under KISA's remit were aware of the legislation and its obligations, it may not be well understood by smaller companies and those in other sectors handling personal data online.

Breaches of personal information are becoming more common, but there is no recourse to collective action under Korean law and individuals are limited in how they can respond when their personal information is compromised. Breaches resulting from negligence by a service provider can result in fines up to US$10,000 for each occurrence, but without the opportunity for collective action, individual cases are hard to bring. A government official commented that bad publicity and damage to a company's reputation could be as significant as a monetary penalty. Industry players also commented on concern for their reputation and competitive position as a driver for ensuring data protection.

KISA received 18,000 privacy related complaints in 2005 and 23,000 in 2006. In some respects KISA acts as a clearing house for complaints about online services and after investigation many complaints were found to be related to other matters such as quality of service issues and were referred back to the company. However, in 2006 800 cases were investigated further for privacy violations to seek some resolution between the parties. Over 90% of these complaints were resolved without need for legal action under the Act. When the complaint was found to be valid the company concerned would typically provide some compensation. In 2006, KISA also conducted site inspections on 44 businesses in the course of investigating privacy complaints, and 50 of the 23,000 complaints were transferred to the police for criminal investigation. KISA's powers are limited, it monitors websites for potential violation and can conduct investigations and site visits with MICs agreement, KISA can make recommendations but corrective action can only be ordered by MIC.

Communications service providers interviewed spoke highly of MIC's responsiveness in developing and revising guidelines in light of comments from industry, particularly a guideline on the technical and management protection of personal data which is essentially a security guideline, but forms the basis of advice on conducting privacy audits.

The high level of resolution without resorting to the courts –the lack of a collective action option not withstanding– and the also high success rate of mediation of over 98% by the Personal Information Dispute Mediation Committee (PICO), suggests that legislation is effective to the extent that it is applied. One government official suggested that the low take-up of Korea Association of Information & Telecommunication (KAIT) privacy trustmark labels might be attributed to the comparative strength of the law. The KAIT trust marks are well designed, but KAIT were unable to provide any information about the number of certificated mark holders later found not to be compliant with the mark's criteria, or provide any details of the types of penalties that had been handed out. KISA and MIC are limited to supervision of the private sector.

The National Human Rights Commission (NHRC) has a broad mandate to investigate complaints of privacy violations by public sector entities, but privacy is not a major focus of NHRC's work and it has a limited staff and expertise in the area. NHRC may also only make recommendation or present opinions in court cases, it cannot impose penalties on other government agencies.

Past industrial policy has helped the ICT sector become one of the driving forces of the Korean economy and it was suggested that the sector does not further need government promotion and support. The sector's success has made the need for data protection even more important as the new ICT services are embedded in society, while user's privacy is not adequately protected. Privacy legislation needs to catch-up with the success of industry. It was agreed by all respondents that Korea needs a new comprehensive and independent data protection regime, not the industry specific and fragmented system of today.

6 Malaysia

When considering approaches to privacy and trust in Malaysia it is important to recall the country's somewhat fragile multicultural relationships, and relatively short history since independence from colonial rule. The Constitution was adopted when the country achieved independence in 1957. The Internal Security Act, legislation which provides the government with far reaching powers over the rights of Malaysian citizens, was enacted in 1960, towards the end of a period of communist insurrection and state of emergency[234].

The Constitution of Malaysia does not refer to a right to privacy, however a section „fundamental liberties" provides the right to freedom of speech and expression; the right to peaceable assembly; and right to form associations[235]. Malaysia is a signatory to the Universal Declaration of Human Rights, but the Malaysian National Human Rights Commission restricts its application to those „fundamental liberties provided for" in the Constitution and to provisions consistent with the Constitution[236]. Malaysia is not a signatory of the International Covenant on Civil and Political Rights, however, as a member of the Commonwealth Malaysia has affirmed its commitment to protect human rights and freedom of expression through statements issued by the Commonwealth Heads of Government meetings[237].

Against this historical and also cultural background there is no strong tradition of concern for privacy and trust in society, and it wasn't until a national IT strategy was established in the mid-1990s that legislation and regulation relating to privacy and trust in the communications sector began to be considered.

In 1996, the National IT Council (NITC), chaired by the Prime Minster, was created to develop and coordinate IT policies and strategies at the national level. NITC would help Malaysia achieve the economic policy goal of becoming a global hub for ICT services and industry, part of Prime Minster Dr. Mahathir Mohamed's vision for Malaysia to become a fully developed country by 2020.

The Council recognized that ICT sector would not develop unless there were laws and regulations to prevent the abuse of IT and multimedia technologies, and the Malaysian public would only accept the flagship e-government and e-commerce applications and services if they had trust and confidence that transactions were reliable and secure and

---

234 For example, see Article 149 of the constitution which grants „special powers" for parliament against „subversion, organized violence, and acts and crimes prejudicial to the public" during a declared emergency, including the promotion of ill-will and hostility between different races or other classes likely to cause violence. This article supersedes Part II of the constitution on fundamental liberties.

235 Constitution of Malaysia, Part II Fundamental Liberties, Article 10, clause (1) a, b, c.

236 Privacy and Human Rights 2005: Malaysia, Electronic Privacy Information Center Washington, DC, USA, Privacy International London, UK.

237 Memorandum on the Malaysia Official Secrets Act 1972, Article 19, September 2004, makes detailed reference to Malaysia's commitment to International Human Rights agreements and treaties.

personal information protected. These concerns led to a series of activities in the late 1990s and early part of the next decade to:

- develop a national security policy framework
- enact legislation to protect personal information
- promote the positive use of the Internet
- harmonize current laws to facilitate the use of electronic media[238]

However, when viewed from the standpoint of personal and civil liberties, privacy still does not enjoy strong protection in Malaysia. The limited laws, regulations and other measures that exist to address privacy concerns do so from an approach of protecting information and data security rather than an approach to privacy as a fundamental right of the individual.

Various new „cyberlaws" were enacted in the late 1990s under the national IT policy plan, they included the Communications and Multimedia Act which restricts the interception of telecommunications traffic and provides most guidance on issues relating to privacy and electronic communications. However, provisions in new and previously existing statutes counter these pro-privacy provisions, enhancing police and government rights to access and intercept data, and to wiretap and seize equipment. For example, the Anti-Corruption Act empowers the Attorney General to authorize the interception of mail and the wiretapping of telephones in corruption investigations. The Computer Crime Act allows police to inspect and seize a suspect's computer equipment without a warrant, including a requirement to provide law enforcement authorities with all encryption keys for any encrypted data. The Sedition Act has been used to attempt to identify persons for anti-government speech online, and the penal code makes it an offence to publish defamatory statements or representations with intent to harm. These laws tend to be broad, each has been used to infringe privacy rights of online communications[239].

When the Multimedia Super Corridor (MSC) was introduced in 1996 as a new region for IT related industries, the heart of the program to establish the country as a global ICT hub, one of the foundation principles in the MSC Bill of Guarantees was to „ensure no Internet censorship". Companies locating in the new MSC development area, either the new Putrajaya centre for government or Cyberjaya multi-media city would be able to conduct their business free from any threat of censorship. However, the Bill of Guarantees also has exemptions for cases affecting the national interest and the freedoms promised are not perfectly guaranteed[240].

---

238 COMNET IT/UNESCO Global Survey on On-line Governance published in 2000, Country Study on Malaysia, and historical information about the Multimedia Super Corridor (MSC)

239 Privacy and Human Rights 2005, ibid

240 Further information about the Bill of Guarantees available on the MSC website, section „why msc. malaysia?"

6.1 Measures to enhance privacy and trust

Malaysia has no explicit constitutional right to privacy. Article 10 of the Constitution of Malaysia recognizes the right to freedom of speech and expression, peaceable assembly and association, however these rights are subject to qualifying clauses in the same article giving government the power to restrict them in the interest of security of the nation and „friendly relations with other countries, public order or morality and restrictions designed to protect the privileges of Parliament or of any Legislative Assembly or to provide against contempt of court, defamation, or incitement to any offence“[241].

Malaysian courts have tended to take a narrow approach to freedom of speech, often favouring to restrict speech while upholding national security and morality, and by protecting individual's reputation against defamation. Privacy has not been considered by any Malaysian criminal court, but in 2001, the civil court was asked to decide if there was a right to privacy under the common law. The judge decide that not only is there no constitutional protection of privacy, but the common law should be based on the English common law prior to 1957 –the year of Malaysian independence– and in English law before 1957 the infringement of privacy had not been recognized as a form of tort. Consequently, the right to privacy is not currently recognized under the Malaysian common law system[242].

Personal Data Protection Act

A comprehensive personal data protection act was proposed as one of the first batch of new cyberlaws to be developed under the National Electronic Commerce Master Plan drawn up in the mid-1990s. Drafting of the law began in 1998. The rationale for a new data protection law was it „would assist in transforming Malaysia into a communications and multimedia hub“ and „would promote e-commerce by creating an environment of trust and confidence through personal data protection“[243].

To date there have been two quite different versions of a personal data protection act. The first was proposed in 1998 and ready as a draft bill for consideration by parliament in 2002. It was based largely on the UK and Hong Kong data protection acts and reflected European Union data protection directives. The second version, sent to the Attorney-General Chambers in March 2003, and expected to have been tabled before Parliament in 2004, owes more to U.S. style legislation; it supports an industry self-regulatory approach and safe harbour provisions.

---

241 Article 10, Clause (2), Part II - Fundamental Liberties, Constitution of Malaysia

242 In the case Ultra Dimension Sdn Bhd v Kook Wei Kuan (2001) 751 MLJ 1, the judge stated „As English Common Law is applicable in Malaysia pursuant to Section 3 of the Civil Law Act 1956, privacy rights which is not recognised under English Law is accordingly not recognised under Malaysian law. Thus, the Respondent does not have the right to institute an action against the Appellant for invasion of privacy rights.“

243 Ministry of Energy, Communications and Multimedia, March 2001

A draft of the first personal data protection bill was made available online for public comment in 2000, the first time draft Malaysian legislation of any kind had been made public and comments invited in this way. In addition to the industrial policy goals mentioned above, the privacy aims of the legislation were to:

1) regulate the collection, possession, processing and use of personal data by any person or organization so as to provide protection to an individual's personal data and safeguard the privacy of and individual, and

2) establish a set of common rules and guidelines on handling a treatment of personal data by and person or organization.

Section 2 of the 2002 bill defined personal data as „any information recorded in a document in which it can practically be processed wholly or partly by any automatic means or otherwise which relates directly or indirectly to a living individual who is identified or identifiable from that information or from that and other information in the possession of the data user including any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual." Like the UK Data Protection Act, the definition is broad, including both „opinion" and „indication of the intentions".

The bill would appoint a Commissioner for Personal Data Protection and a Personal Data Protection Tribunal, however the commissioner was to be responsible to a Minister and not act independently from government. The bill would define general requirements, but the Commissioner and industry sector concerned would develop detailed industry specific requirements. Self-regulatory codes of practice were to be introduced to provide principles for operating the data protection regime and as a first line of complaint and resolution before any escalation to the Commissioner and possible action under the law. The draft would regulate the transfer of consumer data to third parties.

The bill presented a number of data principles to be observed when data was collected, held, used or processed. These principles addressed the manner, purpose and use of personal data, and under what circumstances it may be disclosed, how accuracy must be maintained, including a right to correction, the period of retention, security standards, and that information must be made available to the data subject about how the data users policies and practise regarding the subject's data. No matching of personal data was allowed unless the data subject and Commissioner both consented.

There were also a broad set of exemptions that included issues of national security, defence and international relations. Overall, the draft did little to actually prevent or limit the gathering of personal data, it stipulated the manner of collection and how it may be processed[244].

---

244 E-Commerce and Privacy Issues: An Analysis of the Personal Data Protection Bill, Ida Madieha Azmi Private Law Department, Kulliyyah of Laws, International Islamic University Malaysia (April 2002) for detailed description of the 2002 draft bill.

Proposed penalties included criminal fines of up to 250,000 ringgit and imprisonment of up to four years. Civil damages for data subjects (including compensation for injury to feelings) were also included.

In addition to being the first draft legislation made available online for public comment, the Ministry of Energy, Communications and Multimedia (MECM) also began a program of public meetings and a national „road show" explaining the intent and potential benefits of the legislation to state legislatures, local industry and citizens. This type of public relations exercise for new legislation was unprecedented and should be seen as a reflection of central government's concern over gaining acceptance for concepts of privacy and data protection in the law. The process of promoting the concepts of data protection and privacy also included recommendations for training for the judiciary, public prosecutors and policy in Internet law and data protection issues. It is not known if the latest versions of data protection legislations will include similar recommendations for training and education. The bill was expected to be enacted in March 2002, but in October 2001 MECM Minister Datuk Amar Leo Moggie commented in the press that increasing requests for exemptions to the act, particularly opposition from the states, as well as business and some government agencies, complicated the drafting process. By the end of 2002, then Prime Minister Dr Mahathir Mohamad characterized data protection principles as a burden on business and an impediment to effective policing[245]. There seems to have been disagreement over whether strong personal data protection would enable or hinder Malaysia's goal to become an ICT hub. Around that time, Malaysia was also beginning Free Trade Agreement negotiations with the United States and these may also have influenced the change of approach.

What happened next is somewhat unclear. Towards the end of 2002 draft was removed from the ministry website and discussion about data protection ended. A new personal data protection bill then emerged in 2003 that was significantly more industry friendly and adopted a U.S.-style safe harbour approach rather than the earlier draft's more European style.

The drafting process for this bill was confidential. Minister Moggie's comments make clear lobbying from both industry and within the government greatly affected the bill. As privacy is not considered a fundamental right it is no surprise that it is vulnerable to such influence. In addition, the bill was being drafted during a period of great change in international relations, with national security priorities taking precedence over fundamental rights in many countries. Perhaps instructive that while the 2001 U.S. State Department report on Human Rights was highly critical of Malaysia's use of the Internal Security Act to restrict political speech, and particularly the treatment of Deputy Prime Minister Anwar bin Ibrahim, in 2002, U.S. Attorney General John Ashcroft supported the ISA comparing it to the USA Patriot Act.

---

245 Privacy and Human Rights 2005, ibid

Momentum is growing again for some personal data protection bill to be enacted, and there is some hope that a bill may be taken to parliament during 2007. Details of this rumoured bill are not publicly available.

The Communications and Multimedia Commission Act 1998

The Act established the Malaysian Communications and Multimedia Commission with powers to supervise and regulate communications and multimedia activities in Malaysia, and to enforce the communications and multimedia laws as defined by the Communications and Multimedia Act 1998. The Commission issues licences under the Communications and Multimedia Act 1998, the Postal Services Act 1991 and the Digital Signature Act 1997. It has no direct mandate regarding privacy and trust beyond supporting the generally favourable environment for the communications and multimedia sectors.

Communications and Multimedia Act 1998

The Communications and Multimedia Act was one of the first batch of „cyberlaws" developed as part of the Multimedia Super Corridor and National IT plan. The Act regulates the converging communications and multimedia industries: telecommunications, broadcasting and computing.

The Act is written in broad terms, it attempts to encourage competition and reduce regulation through the adoption and promotion of industry codes of practice and self-regulation[246]. In addition to providing the legal underpinning for the conduct of these industries, the Act also has a role in promoting economic policy with provisions that aim to make Malaysia a global hub for communications, multimedia and content services.

The Act makes no direct refer to the protection of privacy, or to policies to explicitly promote trust in the area of electronic communications. However, the Act contains a number of provisions related to communications privacy:

Section 234 „Interception and disclosure of communications prohibited" is the clearest statement in the Act prohibiting the interception and disclosure of communications. It prohibits the unlawful interception or attempted interception of communications; the disclosure or attempted disclosure the content of communications knowing or having reason to believe it was obtained through interception; using or attempting to use the contents of any communications knowing or having reason to believe it was obtained through interception. This section covers as „communications" all Internet based communications, from an e-commerce transaction to e-mail.

Penalties for violation are a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both. Employees of service providers are ex-

246 Codes of practice are discussed in 6.2 below

empted from these provisions when conducting normal work necessary to protect network operation, however random monitoring is not permitted.

Section 249 establishes rules for searches by the police of computers and includes being given access to encryption keys.

Section 252 grants powers to intercept communications. A public prosecutor may authorise the police to intercept or to listen to any communication transmitted or received by any communications without a warrant if the prosecutor believes the communications is likely to contain any information relevant to any investigation into an offence under the Act. Authorisation may given orally, only after the fact must it be provided in written form.

Section 265 allows the Minister to determine if a licensee or class of licensees must implement the capability to allow authorised interception of communications, and may specify the technical requirements for authorised interception capability.

The Act allows the government to remove websites that have obscene or offending content and under Section 211 of the Act it is an offence punishable on conviction by a fine or imprisonment for a content applications service provider or person using their services to provided „indecent, obscene, false, menacing, or offensive in character with intent to annoy, abuse, threaten or harass any person."

Other „cyberlaws" relevant to privacy and trust:

Digital Signature Act 1997

Enforced in October 1998, the Act gives legal recognition to digital signatures and enables secure online transactions through their use. Section 43 of the Act provides a duty of the subscriber named in a certificate to exercise reasonable care in handling the private key and to prevent its disclosure to any person not authorised to create the subscribers digital signature. The key is the private property of the subscriber who rightfully holds it (Section 43), and a licensed certification authority holding a subscriber's private key shall hold the key as a fiduciary of the subscriber. Section 72 of the Act imposes an obligation of secrecy on anyone who gains access to any confidential information obtained under the Act.

Like the Communications and Multimedia Act, the Digital Signature Act also allows search and seizure without a warrant if the police officer concerned has reasonable cause to believe that the delay caused in obtaining a warrant would adversely affect the investigation or evidence.

Computer Crimes Act 1997

Enacted in June 2000, the Act created several offences relating to the misuse of computers. The Act deals with a range of issues related to unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offence, to modify of the contents of any computer and for wrongful communication.

Telemedicine Act 1997

The Act, yet to be enforced, regulates and controls the practice of telemedicine, from inside and outside Malaysia by registered practitioners. It allows licensed medical practitioners to practise medicine using audio, visual and data communications. All existing medical confidentiality protections apply to any information about the patient obtained or disclosed in the course of the telemedicine interaction. Any image or information communicated or used during or resulting from telemedicine interaction which can be identified as being that of or about the patient will not be disseminated to any researcher or any other person without the consent of the patient. Contravention of the act can result in a fine not exceeding 100,000 ringgit or to imprisonment for a term not exceeding two years or to both.

These three Acts make no direct reference to privacy, and appear motivated by the mechanics of protecting information rather than an interest in protecting a fundamental right.

Measures against Spam

The Communications and Multimedia Act does not deal directly with spam, but it does regulate the content of email message and can he applied to countering spam in some circumstances. Section 233 of the Act states „A person who initiates a communication using any applications service, whether continuously, repeatedly or otherwise, during which communication may or may not ensue, with or without disclosing his identity and with intent to annoy, abuse, threaten or harass any person at any number or electronic address, commits and offence“ and could be used to deal with some spam, although it has not been used in this way to date, and any case would need to prove that it was the intent of the sender to annoy, abuse, etc.

The Computer Crimes Act is written broadly could be used to provide penalties against spam as an abuse of computer and network facilities.

The Banking and Financial Institutions Act 1989 (BAFIA)

The Banking and Financial Institutions Act (BAFIA) provides the financial and banking industries with by far the strongest protection of privacy and confidentiality of information of any sector. The provisions are with respect to information relating to transactions in this sector, not electronic information more broadly.

Employees of banks and financial institutions governed by the Act have a duty of secrecy under Section 97(1) which provides that at no time during or after their employment shall they „give, produce, divulge, reveal, publish or otherwise disclose, to any person, or make a record for any person, of any information or document whatsoever relating to the affairs or account“ of any customer. Persons who may have such information described in Section 97(1) in their possession may also not disclose it to any other person.

There are exemptions to these secrecy rules that allow for disclosure of information during the normal course of doing business, in some civil and other legal proceedings, some instances of bankruptcy. Information may also be disclosed under any Federal Law made to a police officer investigating into any offence under such law and the disclosure being limited to the accounts and affairs of the person suspected of the offence.

Section 43(2) of the Act also exempts the disclosure of customer credit information required by the credit bureau of the Central Bank of Malaysia. I July 2006, as a means to raise the level of protection to the level offered to other banking and financial institution customers under BAFIA, the Ministry of Finance requested the Bank Negara Malaysia, the Malaysian Central Bank, to study and draft a proposal to establish a Personal Data Protection Act to monitor private credit reference agencies that have personal information about bank clients.

The privacy protections in BAFIA –although again the text of the Act does not mention the word privacy– appear to have created confidence and trust in the online banking industry which are popular both as a mobile and wireline service. An inspection of leading online banks show they have privacy policies in place explaining customer’s rights and the service they can expect.

In 2005, Bank Negara agreed to follow BASEL II guidelines and recommendations, and BASEL II compliance should be achieved by the Malaysian banking sector by 1 January 2008. BS7799 best practise security standard certification has been adopted by the banking and insurance industries and these security and operational standards have raised the level of protection of confidential customer data. It can be expected that local IT companies providing database and other services for the financial sector will also be coming into compliance with these standards.

6.2 Arrangements other than law and regulation

The Communications and Multimedia Act introduced a self-regulatory regime and adoption and promotion of industry codes of practice. These voluntary codes provide a potential framework for improving the protection of consumer information, privacy, and increasing trust, but to date have proved ineffective. Industry representatives interviewed in the course of our research commented they were aware of the codes and

some had participated in the forum that oversaw and developed them. However, none were able to mention specific instances when codes were directly considered in relation to privacy. They could only assume a code may apply to issues concerning the protection of privacy. Compliance with the voluntary code is not mandatory under the Act.

Privacy is not a concern for most users and is clearly a nascent concern in Malaysian society. Non-profit organisations active in human rights focus on more the essential right to free speech and abuses of these rights.

The Communications and Multimedia Consumer Forum and General Consumer Code

The Communications and Multimedia Consumer Forum of Malaysia was established in February 2001 as a requirement of Communications and Multimedia Act. Forum members are all telecommunication service providers, broadcasters (television and radio) and Internet service providers licensed by Malaysian Communications and Multimedia Commission (MCMC), and consumer associations, women's organizations, Bar Council, youth organizations, institutions of higher learning and individuals. The Forum's objective and purpose is to:

1) Promote the national policy objectives as stated in the Communications and Multimedia Act

2) Draft, develop and prepare Codes that protect the rights of the Consumer pursuant to the provisions of the Act.

Matters that might be considered by the Consumer Forum are described in Section 190 of the Communications and Multimedia Act and while not limited to the following, the matters specified include information about service, rates and performance, fault repair, advertising and representation of services, billing and related issues, and „ any other matter of concern to consumers." Data protection, personal information and privacy are not explicitly mentioned.

The Forum developed the General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia, which was registered in October 2003. The protection of consumer information is one of eight objectives of the code. Compliance with the code is a condition of the licence granted to all companies licensed to operate under the Communications and Multimedia Act.

The Forum provides a channel for consumer complaints and provides advice on settling disputes related to the code it developed. The Forum monitors service delivery and compliance with the code, and can administer sanctions for breaches of the code by members.

The code defines a „Consumer" as a „person who receives, acquires, uses or subscribes to the services relating to communications and multimedia within the meaning of the Communications and Multimedia Act 1998. This includes a Customer". „Personal

Information“ is defined as the „information collected by the Service Provider from the Customer and that which identifies the Customer“. These are quite narrow definitions within the confines of the Act.

The Service Provider has broad responsibilities for the protection of personal Information, and these are presented as „guiding principles which could be adopted“, particularly that a Service Provider may collect and maintain information about a consumer for tracking practices, however good practices for the collection and maintenance of such information should be followed, with the information concerned:

- Fairly and lawfully collected and processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Not kept longer than necessary
- Processed in accordance with the data subject’s rights
- Secure
- Not transferred to any party without prior approval from the Consumer[247]

These highly subjective guiding principles „which could be adopted“ are supported by code rules which make more stringent demand on the service providers:

Service Providers should adopt and implement a „protection of consumer information policy“ that protects the privacy of identifiable information[248]. The sharing of best practises among business partners to further promote the protection of consumer information in encouraged.

Consumers should be given choice in how information collected about them is used. Service providers should take reasonable steps to assure that data is accurate, complete and timely and for the purposes for which they are to be used. There should be methods for correcting inaccurate information, and procedures to assure data quality should be considered.

„A Service Provider’s policy on the protection of consumer information should be made available [in] the most accessible, easy to read and understood manner“ and should be

---

247 General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia, Part 2, Section 2.2. General Principles, October 2003

248 This is the only time the word „privacy“ appears in the code, Section 2.3 Code Rules, ibid.

disclosed each time individually identifiable information is collected. The policy must state what information is being collected and for what use, including any third party distribution of the information.

A simple check of provider's website shows these „notice and disclosure" statements are often lacking, only a small number of service providers meet the requirements of the code rules and principles[249]. Complaints received by the Forum are generally on billing issues.

Other measures

No alternative dispute mechanism has been developed for use in the communications sector in Malaysia. Privacy and Trust labelling and marks are not being used by any domestic company, TRUSTe, for example, lists no Malaysian companies among its members. Some local offices of international companies do advertise the use of such marks and labels. Online banks have adopted international security marks, but not specifically marks or labels related to privacy.

Some Malaysian scholars have taken the view that a lack of recognition of a general right of privacy is unacceptable in a country following Islamic teaching as its major religion. It runs contrary to most Islamic teaching on privacy where it is clearly defined, for example The Universal Islamic Declaration of Human Rights, article XXII Right of Privacy, simply expresses this right as „Every person is entitled to the protection of his privacy."[250] Dr. Ida Madieha Azmi, a professor at the International Islamic University Malaysia describes Islamic teaching as providing privacy rights in two normative frameworks: a prohibition on the intrusion into another's privacy and instructions and guidance for keeping secrets. Within this framework, many Muslim scholars view personal privacy as a fundamental human right. Professor Azmi contends: „the concept of privacy in Islam seems to cover all the 4 aspects of the right to privacy, viz:

i) Information privacy,

ii) Bodily privacy

iii) Privacy of communications

iv) Territorial privacy"[251]

---

249 General Consumer Code, Code Rules, Section 2.3

250 „Why has Data Protection Law been delayed in Malaysia? Nothing to do with Islam and Who needs it anyway?", presentation by Ida Madieha bt. Abdul Ghani Azmi - International Islamic University Malaysia, at The British and Irish Law, Education and Technology Association, 6-7 April 2006, Malta.

251 Ida Madieha Azmi unpublished work of, Private Law Department, International Islamic University Malaysia. „

6.3 Enforcement powers

The nature of Malaysia law is such that enforcement powers are one the one hand potentially extremely strong, while legislation and other measures directly effecting violations of privacy and trust are in practical application very weak. For example, the Minister's powers under the Communications and Multimedia Act in making or re-making regulations (section 16) are potentially very broad. The Minister may change the conditions of licenses, and cancellation or suspension could potentially be made even on grounds of „the public interest" (section 37). However, in practice the codes promoted by the Act do not seem to be monitored for compliance and are not enforced. Regarding more extreme enforcement measures, we have mentioned the potential effect of laws such as the Internal Security Act.

Some examples of the potential penalties that could be brought to bear in enforcing legislation mentioned in 6.1 follow.

Communications and Multimedia Commission Act 1998. Network Service Providers have some obligations to maintain privacy and integrity of customer data under provisions of the Communications and Multimedia Act and the Commission has the power to suspend or cancel licenses for serious or repeated violations. Violations could include those relating to the confidentiality and disclosure of information[252].

Communications and Multimedia Act 1998 is written in broad terms and the Ministry and Minster have wide-ranging potential powers for enforcement. Section 234 prohibiting the interception and disclosure of communications provides for a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding one year or to both for interception, inappropriate disclosure or use of information obtained by interception of communications. However, the enforcement of conditions of the act on licensees is through the threat of suspension or cancellation of their licence.

Under the General Consumer Code, if a consumer complaint were not upheld by the Consumer Forum and then ignored by the Ministry, it is possible that a person could begin a civil suit against the company, to sue them for a violation of privacy, loss of confidentiality or whatever their grievance.

Telemedicine Act 1997, contravention of the act through the disclosure of any image or information without the patients consent can result in a fine not exceeding 100,000 ringgit or to imprisonment for a term not exceeding two years or to both.

Banking and Financial Institutions Act 1989 (BAFIA) treats violations of privacy and confidentiality more seriously than any other statute, and is the only one to do so in a direct

---

252 Section 37 of the Communications and Multimedia Act allows for the suspension or cancellation of licences granted under the Act

way. Disclosure of confidential information can lead to subject to fines of up to 3 million ringgit or to imprisonment for a term not exceeding five years.

6.4 Effectiveness

A respondent's comment „People are not yet aware of privacy as an issue" captures the situation of privacy and trust in Malaysia. In interviews, experts from all sectors commented generally that people did not yet seem aware of privacy as a right: it is not a concern raised in the media or society generally, other than in exceptional circumstances such as the illegal wiretapping and surveillance of a notable public figure such as former Deputy Prime Minister Anwar Ibrahim. International activities such as data protection discussions in ASEAN and the APEC Privacy Framework have little effect on Malaysian society at the present time. Consequently the effectiveness of privacy and data protection is very limited. It was notable that the country's leading civil society Internet rights advocacy organization itself did very little work on privacy issues, instead focusing on fundamental rights and freedom of expression.

There is no direct reference to the protection of privacy or policies to promote trust in electronic communications in any major communications legislation. However, service and network providers are beginning to be aware that the protection of privacy is valuable to the corporation, particularly in terms of reputation in the marketplace. There was a general sense from all respondents that improved data protection is now necessary as Malaysia's Internet and e-commerce sector continues to grow.

Legislation for the Banking and financial sectors provides protection for personal data and confidentiality, and the sector is also subject to international agreements and standards that provide some protection for privacy.

6.4.1 Effectiveness of legal and other measures

The regime of cyberlaws introduced in the mid 1990s to provide a legal framework to enable the growth of Malaysia's multimedia industry are based on a self-regulatory approach, and the voluntary codes introduced by the Communications and Multimedia Act's provide a potential framework for improving the protection of consumer information, privacy, and increasing trust, but to date have proved ineffective. Provisions of the General Consumer Code, developed from provisions of the Communications and Multimedia Act, regarding the protection of consumer information are not being widely observed. Very few websites carry privacy statements with the information the code requires, and notice and disclosure statements also required are often lacking. Only a small number of service providers meet the requirements of the code rules and principles, and the Consumer Forum overseeing the code has done very little to monitor for violations or deliver any penalties.

Industry respondents commented they were aware of the codes and some had participated in the forum that oversaw and developed them. However, none were able to mention specific instances when codes were directly considered in relation to privacy. They could only assume a code may apply to issues concerning the protection of privacy. Compliance with the voluntary code is not mandatory under the Act.

There is a culture of privacy in Malaysian society, particularly principles stemming from Islamic teaching, but that tradition has not yet transferred online.

There are indications from the Ministry of Energy, Water and Communications that a new data protection bill will be taken to the Malaysian Parliament later in 2007, yet there has been no official confirmation of this from the ministry, and industry experts are at the moment sceptical about such progress. If a bill moves forward it is expected to be favourable to industry interests, following the US model and „safe harbour" provisions. However, industry generally is said to oppose any new bill that would increase their costs of doing business, and the banking and insurance industries are said to be against any omnibus data protection bill that would likely increase their liabilities further than their own sector specific legislation does at present. Outside the government itself the financial sector is probably the largest holder of personal information and is also very influential on government policy.

One factor that might encourage the government to go ahead with new data protection legislation is that the amount of personal information the government processes is increasing rapidly. Many „flagship" e-government programs are coming into use, for example the national smart identity card MyKad, and centralized government databases coordinating information between agencies in programs such „smart schools" and „telehealth", so the amount for personal data being gathered, processed and retained is increasing rapidly. Government may come to believe that data protection legislation is necessary to complement to the e-government processes it is bringing online.

7 India

Unlike the United States or the European Union, India has not yet enacted separate legislation for privacy rights against private parties. Within the national legal framework, the Fundamental Rights enshrined in Part III of the Indian Constitution provide protection for several international human rights such as the right to life and personal liberty, freedom of speech and expression, and freedom of assembly. In studying Indian data protection, it is important to distinguish between two concerns. Indian companies processing data from multinationals outsourced to India have strategic regulatory concerns regarding the data protection regimes from which their data is outsourced. This is the subject of legitimate and heightened concern in view of recent '*causes celebres'* in security breach (notably Bank of America and HSBC data breaches). What is termed 'Business Process Outsourcing' (BPO) comprises a very large foreign currency earning ($11billion) industry in India. The second concern is the rights of Indian citizens under its law and constitution. As India is a developing country with 2million consumer broadband Internet connections in a nation of 1.1 billion, privacy and trust in e-commerce is low on the list of legislative concerns. Nevertheless, recent developments in mobile data and government information sharing have given rise to legislation which we detail in the chapter.

Reflecting increased concern in India about data protection laws enacted in other countries, the National Task Force on Information Technology and Software Development submitted an „Information Technology Action Plan" to the Prime Minister in July 1998, calling for the creation of a National Policy on Information Security, Privacy and Data Protection Act for handling computerised data[253]**.** European Union, and especially UK, companies account for around 20% of information technology revenues for India in 2003, with the United States a far larger trading partner. IT Act Section 72 remedies for breach of confidentiality and privacy. The section deals only with disclosure of confidential information and not with interception and therefore is limited in its scope[254]**.**

Multinational business and its local partners has led policy in privacy and security due to the prevalence of BPO (Business Processing Outsourcing) activities conducted within India. India is a noteworthy example of a country where security is seen as an essential part of marketing and 'adding business value'. If Indian companies do not appear to take security seriously, multinational software companies and financial institutions, which now regularly outsource and offshore their work to Indian companies, may look elsewhere. In this respect, the attitude towards security has been market-driven and led by industry and by bodies like the National Association of Service and Software Companies (NASSCOM).

---

253 NTF on Information Technology & Software Development, Basic Background Report, 961998

254 Mustafa Faizan (2004) Privacy Issues in Data Protection : National and International Laws, Practical Lawyer WebJour 16 at http://www.ebc-india.com/practicallawyer/index.php?option=com_content&task=view&id=634&Itemid=1

7.1 Measures to enhance privacy and trust

Constitutional right to privacy

The Indian Constitution does not explicitly guarantee a fundamental right to privacy. However, the Constitution embodies Fundamental Rights in Part III, which are enumerated in Article 14-30. Extensive interpretation by the Supreme Court has, however, deduced the right to privacy from the Right to Life and Personal Liberty enshrined in Article 21. The Supreme Court has interpreted the phrase *„… no person shall be deprived of his life or personal liberty except according to procedures established by law …"* to imply that *„… those who feel called upon to deprive other persons of their personal liberty in the discharge of what they conceive to be their duty must strictly and scrupulously observe the forms and rules of the law".* A triple-test that can be applied to any law is consequently that: 1) it must establish a procedure, 2) the procedure must withstand the test of fundamental rights conferred under Article 19, and 3) it must withstand the test of Article 21 in that the procedure authorizing interference is right, just, fair, and neither arbitrary, fanciful, nor oppressive.

This means that the right to privacy as conferred from Article 21 of the Indian Constitution is not absolute, but can be superseded under certain conditions. Case law has subsequently defined the boundaries of the right to privacy, balancing it against other rights and interests.[255] Following these court rulings it can be found that: 1) there is a right to privacy, and unlawful invasion of privacy can result in liability of the offender in accordance with the law; 2) the constitutional recognition of privacy protects individuals against unlawful invasion of privacy by the government; and 3) the right to privacy may be lawfully restricted to prevent crime or disorder, or to protect other rights.

The Indian right to privacy is limited to „first generation rights". The constitutional right of privacy is only enforceable against the state and not against private entities.[256] Legislative competence in the area of privacy is with the national Parliament.[257] The 'dualistic' approach in respect to the incorporation of international law into national law followed in

---

255 See Kharak Singh v State of UP (AIR 1963 SC 1295); People's Union for Civil Liberties (PUCL) v Union of India (1997) 1 SCC 301; Gobind v State of M.P. (1975) 2 SCC 148; Pooran Mal v Director of Inspection (Investigation) of Income-tax, New Delhi (AIR 1974 SC 348); X v Hospital Z (AIR 1999 SC 495),

256 EPIC and Privacy International (2005) Privacy and Human Rights 2005, An International Survey of Privacy Laws and Developments, available at: http://www.privacyinternational.org/index.shtml?cmd[342][]=c-1-Privacy+and+Human+Rights&als[theme]=Privacy%20and%20Human%20Rights&conds[1][category.....]=Privacy%20and%20Human%20Rights

257 India is structured as a federal state. According to Article 246 of the Indian Constitution, legislative competences are divided into three categories: List 1 with exclusive Union (i.e. federal) competences, List 2 with exclusive State competences and List 3 with concurrent competences of the Union Parliament and the States. Article 248 in connection with List I also confers legislative competence in respect of any other matter not enumerated in List II and III to the national Parliament

India requires international agreements not only to be ratified, but also to be transposed into domestic law to become enforceable (which is within the legislative competence of the Union). Nevertheless, courts can interpret domestic law in the light of (not yet transposed) international agreements or fill gaps within domestic law by resorting directly to the international agreements. India has ratified the International Covenant on Economic, Social and Cultural Rights (CESCR), and the International Covenant on Civil and Political Rights (but has not signed the Optional Protocol);[258] the International Covenant on Civil and Political Rights includes in Article 17 the right to privacy. United Nations guidelines are applicable to India, but India has not signed the OECD guidelines.

7.1.1 Data protection law

No specific legislation pertaining to data protection has been enacted in India. The protection of personal data in India is mainly achieved through contract law, and the IT Act. However, there are some other applicable laws such as the Information Technology Act 2000, Indian Copyright Act 1957 (as amended 1999) and other copyright law, Indian Penal Code, Special Relief Act 1963, Consumer Protection Act 1986 and Consumer Protection (Amendment) Act 2002, Indian Contract Act 1872, and customs and practices developed with the passage of time. The Information Technology Act 2000 ('IT Act') may be amended in 2007/8 by the Information Technology Amendment Bill (2006) Bill No.96, as introduced in the Lok Sabha (Parliament) on 15 December 2006.

Information Technology Act 2000

The IT Act lays out the framework for data security and for dealing with cyber-crime. This Act is based on Resolution A/RES/51/162 regarding the Model Law on Electronic Commerce adopted by the General Assembly of the United Nations on 30 January 1997; it entered into effect on 17 October 2000. The focus of the Act is e-commerce and e-government, and it tackles a broad spectrum of relevant issues such as digital signatures, computer crime, hacking, and breach of confidentiality. The Act does not focus on „personal data". In fact it does not incorporate a concept of „personal data" at all. Concerns have been expressed that the Information Technology Act (even if amended according to the not yet adopted proposal) might not suffice to ensure adequate protection; the requirements in respect of purpose limitation, accuracy, transparency, right to access, rectification and opposition established by the Article 29 Working Party are not (sufficiently) met.

---

258 Office of the United Nations High Commissioner for Human Rights, Status of Ratification of the Principal International Human Rights Treaties as of 09 June 2004, available at: http://www.unhchr.ch/pdf/report.pdf

The Act establishes amongst others:

- Civil liability for data and database theft, unauthorized digital copying, downloading and extraction of data, unauthorized transmission, inappropriate use of unauthorised cookies, spyware, or digital profiling.

- Liability for hacking with intent or knowledge of unauthorised access, causing wrongful loss or damage by destroying or altering information residing in a computer, or diminishing its value or utility. This can be interpreted as being the case if a sensitive email saved in a computer is accessed without authorization as it loses its value.

- Penalties for breach of confidentiality and privacy by disclosing electronic material without the consent of the concerned person. This is, however, limited to persons to whom power has been conferred under the Act, or under rules or regulations made pursuant to the Act. This restricts the obligation to authorities such as the Controller of Certifying Authorities, or the Adjudicating Officer.

The Act also proposes a National Computerised Records Security document to act as a policy document for security requirements within government. This Act also created a National Policy on Information Security, Privacy and Data Protection. Privacy is explicitly (albeit briefly) mentioned in the Act, where the need to protect consumer privacy is summarized as: any collection and distribution of other persons' information and electronic records to third parties without authorisation, is punishable by law. The Act also provides law enforcement authorities with broad discretion: for example, under certain circumstances Section 69 allows interception of any information transmitted through computer resources, and penalises those who refuse to disclose encryption keys with a sentence of up to seven years' imprisonment. Furthermore, the Act brings into force digital signatures and the associated regulatory and legal infrastructure required for electronic documents to be accepted in the same way as their paper counter-parts. The digital signature regime became operational in February 2002.[259]

A proposal for amending the IT Act was published in December 2006 and was under discussion in committee in the Parliament (Lok Sabha) in spring 2007. These amendments would include privacy protection by introducing a new section on „handling of sensitive personal data or information" with reasonable security practices and procedures. The terms „sensitive personal or information" as well as „reasonable security practices and procedures" would be defined by the Central Government in consultation with industry self-regulatory bodies. To conform with the Council of Europe Convention on Cybercrime, computer related offences (e.g. unauthorized access, unauthorized

---

259 EPIC and Privacy International (2003) Privacy and Human Rights 2003, An International Survey of Privacy Laws and Developments, available at: http://www.privacyinternational.org/survey/phr2003/countries/india.htm

download of data, causing denial of access, introduction of viruses) would be punishable with imprisonment, if committed dishonestly or fraudulently. An amendment of the Section 72 liability for data and privacy violations has been proposed that would amongst others make intermediaries (network service providers) liable for violations in respect to the privacy of their subscribers' data if the violation was intended to cause injury to the subscriber (a requirement that can only rarely be expected to occur). On the other hand, intermediaries will not be held liable for pornographic material accessed through their sites. Another amendment is to make the Act technology neutral (e.g. replacing the „digital signatures" with „electronic signatures"). Some experts feel that amendments to the Act and development by case law are sufficient to confer data protection to individuals and organisations,[260] others feel that this is not the best way to establish a sound data protection regime in India. Those in the latter school of thought feel that a separate law should be adopted dealing with data protection not as a by-product but as its main aim.[261]

7.1.2 Specific ISP Regulation

Indian regulation of ISPs and ENCP equivalents is governed by both statute (notably the Telegraph Act 1885 as amended) and the amendments to licences implemented by the Ministry of Commerce and Industry, and regulated by the Telecom Regulatory Authority of India. Indian Telegraph Act 1885 governs lawful interception by the government in case of any public emergency or in the interest of public safety. In 1996 the Supreme Court ruled that wiretapping is a „serious invasion of an individual's privacy"[262] and that phones can only be tapped if the Union Home Secretary or his or her counterpart at State level have issued such an order, that the government must prove that this is the only means to obtain the sought information, and that a high-level committee should be established to review the legality of each interception. Recordings or transcripts of tapped phone calls are not generally accepted as primary evidence in Indian courts, however this is admissible in terrorist cases under the Prevention of Terrorism Act (POTA) and the Unlawful Activities (Prevention) Act (UAPA).

---

260 E.g. Dalal, P. (2005) Data Protection Law in India: A Constitutional Perspective, available at: http://advocatepraveendalal.blogspot.com/2005/06/data-protection-law-in-india.html; Dalal, P. (2006) The needs and modes of data protection, The TRIPS Analysis: Data Protection Law in India (Part II), Magazine of Intellectual Property & Technology, available at: http://www.ipfrontline.com/printtemplate.asp?id=10637

261 E.g. Nair, L. (2005) Does India need a separate data protection law?, in the World Data Protection Report Volume 5 Number 12, December 2005, available at: http://www.knspartners.com/files/BNA%20Article-180106.pdf

262 EPIC and Privacy International (2005) Privacy and Human Rights 2005, An International Survey of Privacy Laws and Developments.

ISP Licences

The privacy and security terms of ISP licences are typically those concerned with preventing foreign control of national data[263]. ISP licences were until recently freely available to nationals, while ENCP-equivalent licences were more restricted. Majority foreign ownership (up to 74% from 49% prior to reforms) has recently been permitted in reforms of 2005 and 2007 and some European operators have bought Indian companies. The restrictions include in Paragraph B include:

> (vii) The Chief Officer Incharge of technical network operations and the Chief Security Officer should be a resident Indian citizen…For security reasons, domestic traffic of such entities as may be identified /specified by the licensor shall not be hauled/routed to any place outside India. The licensee company shall take adequate and timely measures to ensure that the information transacted through a network by the subscribers is secure and protected. The officers/officials of the licensee companies dealing with the lawful interception of messages will be resident Indian citizens…
>
> (viii) The Company shall not transfer the following to any person/place outside India:- Any accounting information relating to subscriber (except for international roaming/billing) (Note: it does not restrict a statutorily required disclosure of financial nature) ; and (b) User information (except pertaining to foreign subscribers using Indian Operator's network while roaming).
>
> (ix) The Company must provide traceable identity of their subscribers. However, in case of providing service to roaming subscriber of foreign Companies, the Indian Company shall endeavour to obtain traceable identity of roaming subscribers from the foreign company as a part of its roaming agreement.

In addition to these specific conditions regarding Indian nationals' control of data and transfer outside India, the government has reiterated its control over ENCP security:

> The licensee company is not allowed to use remote access facility for monitoring of content. Suitable technical device should be made available at Indian end to the designated security agency/licensor in which a mirror image of the remote access information is available on line for monitoring purposes. Complete audit trail of the remote access activities pertaining to the network operated in India should be maintained for a period of six months and provided on request to the licensor or any other agency authorised by the licensor. The telecom service providers should ensure that necessary provision (hardware/software) is available in their equipment for doing the Lawful interception and monitoring from a centralized location… It shall be open to the licensor to restrict the Licensee Company from operating in any sensitive area from the National Security angle.

---

263 Ministry of Commerce and Industry (2007) Enhancement Of The Fdi Ceiling From 49 Per Cent To 74 Per Cent In The Telecom Sector – Revised Guidelines Press Note No. 3 (2007 SERIES) of 19 April 2007.

> In order to maintain the privacy of voice and data, monitoring shall only be upon authorisation by the Union Home Secretary or Home Secretaries of the States/Union Territories. For monitoring traffic, the licensee company shall provide access of their network and other facilities as well as to books of accounts to the security agencies. The aforesaid Security Conditions shall be applicable to all the licensee companies operating telecom services covered under this Press Note irrespective of the level of FDI.

This control is also applied to the BPO sector via the control over ENCP operators:

> Other Service Providers (OSPs), providing services like Call Centres, Business Process Outsourcing (BPO), tele-marketing, tele-education, etc, and are registered with DoT as OSP. Such OSPs operate the service using the telecom infrastructure provided by licensed telecom service providers and 100% FDI is permitted for OSPs. As the security conditions are applicable to all licensed telecom service providers, the security conditions mentioned above shall not be separately enforced on OSPs.

There is therefore a greater apparent focus on security and national integrity of the data environment than the privacy rights of the citizen-subscriber. Liberalisation and introduction of foreign competition is permitted only insofar as it complies with national information security restrictions.

7.1.3 Other Sectoral Regulation

Whilst not directly concerned with the privacy aspects of e-Communications, there are a number of other relevant statutes that are indirectly pertinent in India.

7.1.4 Generic Private Law

Indian Contract Act, 1982

In accordance with this Act, if a party breaches a contract, the other party is entitled to receive compensation for any loss or damage so caused. This means that (e.g. European) data protection standards can be introduced into the contract and become binding. Increasingly, outsourcing/BPO contracts also include a clause on international arbitration or dispute resolution, and a different governing law than Indian law is often agreed to govern the contract.

7.1.5 Federal and State Law

Interviewees have informed the study team that proposals for data protection law have been drafted in Kerala and Andhra Pradesh. However, the national legislators expect that the IT Act amendments will either predate or supersede such legislation, and little heed is paid to it by national lawmakers. While several states have model laws across

e-commerce subjects (e.g. digital signatures), interviewees and other sources suggest the letter of the law is not always strictly enforced. It may be therefore advisable to maintain scepticism about the wider impact of any state-level legislative proposals.

7.2 Enforcement of Legal Protection of Privacy

There is no data protection authority in India, nor is there a probability of such a specific regulator. In the absence of a Data Protection Act and of a specific Data Protection Authority in India, remedy has to be sought in court under the general rules of law and the afore-mentioned Acts. Under the Credit Information Act, the Reserve Bank of India may be empowered to impose penalties on credit information companies; this would make the Reserve Bank a regulator in this area. However, the required regulation has not entered into force yet. In March 2000, the Central Bureau of Investigation established a Cyber Crime Investigation Cell (CCIC) to investigate offences under the IT Act; the CCIC is a member of the Interpol Working Group, and its competence covers the whole of India. Similar cells have been set up at State level.[264] The IT Act introduces a separate judicial authority mechanism by establishing three authorities competent in arbitration and adjudication for settlement of civil disputes under the Act: 1) Controller of Certifying Authorities, 2) Adjudicating Officer, and 3) Presiding Officer of the Cyber Regulations Appellate Tribunal. The Adjudicating Officer has to follow the principles of law of torts when granting compensation, he or she is in the role of a quasi-judicial body created to dispense civil justice with regard to the Act. If he finds that the offence would require punishment instead of mere financial penalty, he is called upon to transfer the case to the magistrate. For the appeal of matters under the Act, the Cyber Regulation Appellate Tribunal (headed by one person) has been established. It is entitled to appeal jurisdiction both on fact and law over the acts of the Controller of Certifying Authorities and the Adjudication Officer. The second appeal goes to the High Court.

7.3 Effectiveness of self-regulatory arrangements

India's substantial outsourcing industry is based on US and European data standards. It enforces these contracts through litigation and contractual enforcement as well as a variety of industry best practices in self-regulation**.** The effectiveness of general contractual enforcement in the local legal system is widely considered to be affected by the slow and laborious litigation process. There is strong effective coordination between government and the private sector (notably NASSCOM) regarding the measures necessary to sustain confidence in the BPO sector for mainly US and British investors. By

---

264 EPIC and Privacy International (2003) Privacy and Human Rights 2003, An International Survey of Privacy Laws and Developments, available at: http://www.privacyinternational.org/survey/phr2003/countries/india.htm

contrast, there is relatively little activity in enforcing private citizens' rights in India against companies, and only recent legislation to permit citizens to monitor government use of their data. As seen in Section 7.2, the regulation of network and service providers is focussed on nationality requirements and security, with the protection of subscriber information privacy very much a 'work in progress' by comparison with developed Western countries.

Industries such as accounting and law, have Self-Regulatory Organisations (SRO) that have established a code of conduct. Recently the telecom and banking industries have also set up SROs developing codes for handling customer data. Similar tentative SRO initiatives are also ongoing in the IT and the BPO sector. NASSCOM has warned that Information Security could easily become the „Achilles heel" of Indian BPO companies. While such companies market their process efficiencies and cost savings to Western firms, the need for them to advertise adherence to prevailing national and international security and privacy standards is clear. Under the aegis of NASSCOM, several initiatives have been launched to establish self-regulation in the BPO industry:

- The 2004 initiative '4E Framework for Trusted Sourcing' includes the responsibility to report to its members on legislation affecting the industry, including a responsibility to inform ands educate its members on industry legislation affecting companies such as the US Health Insurance Portability Accountability Act (HIPAA), US Gramm-Leach-Biley Act (GLBA), and UK Data Protection Act, and other required legislation[265].

- The 2005 National Skills Registry[266] initiative for individual vetting checks the credentials of BPO staff by collecting demographic information, details of academic qualification etc. Management of this information is done on a contractual basis between the IT professional who is a member of the Registry and the company operating the system. The Registry has over 100,000 individuals' data. The database and its policy is called „Fortress India", allowing employers to identify employees with criminal records. Arguably such a scheme, which is designed to put security first, would breach employee privacy rights in Europe.

- The June 2007 launch of the Data Security Council of India aims at developing the best practices into a code of conduct, and introducing a kind of accreditation/label proving compliance with these best practices, which might also require the audits. NASSCOM aims at establishing local security fora of Chief Information Security Officers in cities with a large number of companies.

---

265 This 'encapsulates engagement, education, enactment and enforcement for ensuring information security in the Indian outsourcing industry. The association is setting up an advisory board to evolve best practices, both from a regulatory and compliance perspective.' See The Hindu (2004) 4 June, Nasscom projects software services revenue at $20, at http://www.hindu.com/2004/06/04/stories/2004060405911400.htm

266 https://nationalskillsregistry.com/

National newspaper The Hindu commented:

> „The initiative is in line with Nasscom's Trusted Sourcing campaign and raises the data security bar for the $31.3-billion IT software and services export industry, which has been the eye of a storm over incidents of data security breach… The newly formed independent body, to be headed by Mr Shyamal Ghosh, will enable India-based software companies to voluntarily sign up for certification or accreditation, depending on their size. The verification would then be carried out by third-party auditors. The accredited companies would have to adhere to certain standards of security compliance, failing which they would be liable for punitive action in the form of an enquiry, dis-accreditation and even a penalty."[267]

As the body has just been formed it is impossible to state what effectiveness it might have. NASSCOM members perform staff training and information about data protection as part of their security awareness training and data protection best practices.

The Reserve Bank of India (Banking), Telecom Regulatory Authority of India (Telecom) and Securities Exchange Board of India (for securities trading) have issued guidance regarding privacy and trust for electronic communication. The call register for mobile telephony telemarketing (supported by the Indian Banks Association and Indian Cards Council) requires banks to establish a Do Not Call register. The Telecom Regulatory Authority of India (TRAI) has initiated a consultative process for regulating unsolicited calls, and proposed that the company DNC registers are consolidated into a national register.

Indian BPO companies often conform to standards-based instruments in use in Western countries, including conformance with business process British Standard 7799. Furthermore, SAS-70 audit is becoming increasingly common. SAS-70 helps service companies to implement and improve internal controls and to ensure minimal disruptions from auditors working for their clients. There is a huge variety of industry practices across sectors and service providers, partly due to there being no lowest common standard. There are multiple other reasons:

1. Data protection fixes were introduced *ad hoc* during BPO activity, as a retrofit;
2. There is resistance to privacy results from both BPOs and multinational clients;
3. Some multinational clients have consequently „over-reacted" to scandals.

---

267 The Hindu (11 June 2007) *Nasscom working on data security council* at http://www.thehindubusinessline.com/2007/06/11/stories/2007061101150200.htm

A good example is the requirement that no new hire has worked for a rival BPO in previous twelve months – e.g. no recruit for INFOSYS who worked for Wipro within a year. Interviewees indicate this would not be applied even to board directors in multinationals' home countries. There is the view that levels of 'Chinese Walls' are tending in some cases to extreme and counter-productive 'gold plating'. As a general rule, multinationals „get what they pay for": any level of information privacy they choose. One corporate interviewee states that:

> „Outsourcing in India is in tiers: you can compare it to the rating system for hotels – you get what you pay for, five star or less".

There seems to be a practice in India to consider two types of sensitive data – [1] payroll data on internal employees, which is not outsourced much so far; [2] client data, where there is increasing use of software data masking to add extra security. There is huge variety in the practices between audited functions:

- whereas BPO data processing is carried out in almost laboratory conditions (no cameraphones, paperless operations, no pen drives)
- the IT function technical staff are allowed their own laptops, pen drives, camera phones etc.
- It is perhaps not appreciated by companies just how inter-related these two functions are, in India and elsewhere.
- IT outsourcing is therefore a potential 'compliance hole' –to secure BPO data without checking IT systems is not a very functional approach.

European companies undertaking BPO agreements still rely upon contractual means for protecting and preserving data. Having appropriate statutory protection with stipulated statutory penalties, damages and other remedies would act as a good deterrent against a breach of data privacy. The new amendments proposed to the IT Act 2000 could be interpreted as a 'box-ticking exercise', as an attempt to include a data protection commission would be to fly in the face of any real compliance-enforcement possibility – let alone any real interest amongst the 1.1 billion population as opposed to the roughly 20m 'urbanites' with broadband at work or home. Comprehensive data privacy requires a cultural shift towards taking digital enforcement as a higher priority. Foreign laws do impact on Indian companies – there are the EU Standard Contract terms and compliance audit to ensure compatibility. There is also compliance with California Statute 1386 (duty to disclose any information security breach law) which is monitored on an ongoing basis on behalf of some concerned clients. That can be seen from the Indian perspective as a real 'gold standard', to have continual monitoring in case of unintended and non-harmful breach.

The perception of privacy in India domestic policy diverges significantly from the Western one. Two studies recently focused on assessing the level of awareness about privacy issues in India, and privacy related concerns. In India the concept of privacy is understood in the context of the physical home (48%) rather than in the context of information privacy (only 14% of the Indian interviewees compared to 61% of US subjects related privacy to this aspect). Indians see data security and privacy as a much lesser problem than their US counterparts, and are less concerned about the security of computerized information. Only 21% of Indian subjects are concerned about identity theft compared to 82% of US subjects. 21% of Indians are concerned about keeping computerized information secure while in the US it is 79%. This different perception of threats to privacy goes hand in hand with a high trust in both Indian government (81%) and businesses (86%). An analysis of 89 Indian e-commerce websites within the studies also revealed that only 29% had posted privacy policies.[268]

7.4 Applicability and relevance to Europe

India is a rapidly developing country with a substantial outsourcing industry based on US and European data standards. It enforces these contracts through litigation and contractual enforcement as well as a variety of industry best practices in self-regulation**.** The effectiveness of general contractual enforcement in the local legal system is widely considered to be affected by the slow and laborious litigation process. It is obvious that India is placed in the position of rule-taker rather than rule-maker in its relations with both the US and Europe. Though there is strong effective coordination between government and the private sector (notably NASSCOM) regarding the measures necessary to sustain confidence in the BPO sector for mainly US and British investors, there is little activity in enforcing private citizens' rights in India against companies, and only recent legislation to permit citizens to monitor government use of their data. The regulation of network and service providers is focussed on nationality requirements and security, with the protection of subscriber information privacy very much a 'work in progress' by comparison with developed Western countries. India is therefore focussed in practice on demonstrating itself as a reliable partner for BPO activities, rather than on domestic privacy policies.

---

268 Kumaraguru, P., Cranor, L. (2005) Privacy in India: Attitudes and Awareness, In Proceedings of the 2005 Workshop on Privacy Enhancing Technologies (PET2005), 30 May - 1 June 2005, Dubrovnik, Croatia; abailable at: http://lorrie.cranor.org/pubs/PET_2005.html; and Kumaraguru, P., Cranor, L., Newton, E. (2005) Privacy Perceptions in India and the United States: An Interview Study, available at: http://www.cs.cmu.edu/~ponguru/tprc_2005_pk_lc_en.pdf

8 International Comparisons

The approaches to safe guarding privacy vary widely across the countries we studied. In fact, no two countries share the same approach. That said, it appears that the European Union exhibits the most comprehensive approach to privacy protection.

8.1 Laws and Regulation

8.1.1 Privacy Rights

Unlike the EU, in the countries we have studied, an explicit constitutional right to privacy is not the judicial norm. Korea is the notable exception. However, the lack of an explicit provision has not necessarily hampered the development of a privacy right by statutory, common, or international law. In India, Japan, South Korea and the United States, the courts have interpreted the existence of a right to privacy based on other rights enumerated in the country's constitution; however, the Malaysian courts have not.

8.1.2 Comprehensive Laws

Japan is the only country studied which has enacted a comprehensive data protection law. However, three countries (India, Malaysia and South Korea) are considering such legislation. Japan's overall framework for the protection of personal information is set forth by a series of three acts series of three acts: a Basic Law to protect personal information and two further Acts which require the protection of personal information in the private sector, in public administrations and in incorporated administrative agencies (quasi-government agencies), respectively. In 1998, South Korea promulgated the Act on the Protection of Personal Information Maintained by Public Agencies 1996 which secures personal information held by public agencies and gives citizens rights to control that information. The Korean non-comprehensive approaches contrast sharply with EU Directive 95/46/EC which provides the overall European framework for data quality and proportionality principles, the transparency principle, the security principle, the existence of rights of access, rectification and opposition and restrictions on onward transfers.

8.1.3 Sector-specific Laws

All of the countries included in the study have laws governing privacy practices for ECSPs and ECNPs. However, only the EU and the U.S. have laws which relate to infrastructure products. The EU is now considering the privacy issues presented by the terminal equipment associated with RFIDs. Though U.S. statutes generally do not impose any obligations on developers of infrastructure products, the Computer Assistance

for Law Enforcement Act (CALEA) requires that infrastructure products for electronic communications networks be technologically enabled for legally authorized monitoring of communications. U.S. and India are the only countries where jurisdictions have imposed privacy regulation on electronic communications at the local or state level. However, the local regulations in the U.S. and India are thought to be generally weak were it not for the presence of a national framework.

8.1.4 Effectiveness

We would begin by noting that it is difficult to meaningfully evaluate an overall privacy regime, and doubly so to make a meaningful comparison between different countries with significantly different institutions. As Bennett and Raab put it: „It is one thing to describe and analyse the international instruments, codes, commitments, technologies, and other elements that compose what we have called regimes of privacy protection. It is quite another thing to evaluate any or all of these in terms of the effect they may have – singly or together – upon protecting individual privacy. … It remains a major problem that there exists *no satisfactory way of evaluating or measuring the approximation of regulatory laws and mechanisms to the goal of protecting privacy*."[269]

Each of the country chapters provides a discussion of the effectiveness of law and regulation and of other measures in that country. This section provides brief highlights.

In the United States, the FTC pursues cases on behalf of consumers. Our indicates that the frequency of enforcement actions and the amounts collected in fines are relatively small (given the number of people affected); nonetheless, respondents felt that the fear of enforcement has a deterrent effect on market players. Protection of privacy takes place at different levels in the U.S. – for example, many states require disclosure of privacy breaches. Multiple survey respondents emphasized that the lack of an overarching privacy framework should not be interpreted as implying an overall lack of protection of privacy.

Many of the respondents from the Asian countries that we studied felt that their countries should be going much further in establishing a legal framework for privacy, and in enforcing the laws that are available. In countries like Malaysia and India, where there is little law to protect the electronic privacy of individual citizens, there is little that we can say about the effectiveness of enforcement.

In Europe, official EU statistics from Eurobarometer indicate that data controllers rated the level of protection offered by their respective data protection laws as 'medium.'

---

269 Bennet and Raab, op. cit., page 235.

8.2 Enforcement Measures

8.2.1 Public Authorities

The ability of a public authority to take action against a private organization is quite varied across the countries studied. In the United States, the Federal Trade Commission is perhaps the most recognized authority for taking actions on behalf of consumers particularly against ECSPs. Statutes confer enforcement powers on federal and state authorities covering the activities of ECNPs and ECSPs. In India, there are consumer protection organizations, but they do not deal specifically with privacy, and their effectiveness is questionable (although financial institutions have recently begun to take an interest in this area). In Malaysia, the Ministry of Energy, Water, and Telecommunications has powers to act against ECNPs and can in theory impose fines and prison sentences. In South Korea, the Korean Information Security Agency (KISA) has limited enforcement powers over the ICT sector as an agency of the Ministry of Information and Communications. In Japan, a Minister who oversees a particular sector may intervene in a case and take a number of actions (up to and including an order to the company). In Europe, each Data Protection Authority is granted supervisory powers under Directives 95/46/EC and 2002/58/EC, and has criminal, commercial and individual rights of enforcement against a wide variety of data controllers.

8.2.2 Private Litigation

The private right to use litigation in response to breaches of privacy is varied across the countries studied. In the U.S., although there is a perceived ability to undertake private litigation, the costs tend to deter private individuals from doing so. In addition, the victim of a privacy violation can only bring a private suit against an ECNP or an ECSPs to seek damages for the improper (i.e. illegal) release of electronic and stored communications only if there is a specific statutorily created cause of action.

In India, data protection is in general governed by an individual contract or a Service Level Agreement with the ECSP or ECNP. Where foreign firms outsource services to an Indian firm, these contracts are commonplace. In the event of a breach, enforcement is via suit, as a matter of contract law. These actions are typically brought under the client's national law (mostly U.S. or EU) in the case of foreign clients.

By contrast, in Japan, complaints from private citizens concerning personal information protection are primarily dealt with as an administrative procedure brought to the Minister who oversees the firm (i.e. the Minister responsible for the sector in which the firm operates), when the complaint cannot first be settled privately. Malaysia follows a similar administrative approach; however, Malaysia provides for the bringing of a civil suit should the Consumer Forum or the Ministry not provide adequate relief.

8.3 Measures other than law and regulation

This section compares the countries studied in terms of their approaches to co-regulation and self-regulation; PETS; and standards.

8.3.1 Co-Regulation and Self-Regulation

Arrangements vary among the countries. In Malaysia, South Korea and Japan, co-regulation and self-regulation are generally based upon guidelines driven by legislation. In the U.S., India and Europe, self-regulatory schemes are much more 'bottom-up', reflecting market driven forces.

Privacy labels and codes of conduct both represent prominent form of self-regulation. Different countries implement them in different ways. TRUSTe is a well known privacy labelling scheme in the United States and Japan. In the U.S., ECNPs and ECSPs have also developed codes of conduct which in some instances are regularly audited. In India, Business Process Out-sourcing (BPO) companies have implemented internal codes of conduct which are compliant with the audit requirements of their customers; however, this seems to be a more 'reactive' implementation of codes of conduct (driven mainly by business need) than in the United States. In Malaysia, the Communications and Multimedia Act supports a self regulatory approach with the development of industry codes of practice. A Communications and Multimedia Industry Code of Practice which includes privacy principles has been registered. In South Korea, a committee has been set up (run by KISA) to mediate complaints against ECNPs and ECSPs in the private sector. Guidelines are also issued from the Ministry relating to technical and security aspects of network operations. A privacy mark system is in existence, run by the Korean Association of Information & Telecommunication. In Japan there is a co-regulatory regime where the law allows organisations to form Authorised Personal Information Protection Organisations.

Possibly the best known self-regulatory regime in Europe is the Safe Harbour regime and the development of the model of Binding Corporate Rules[270] between organizations that have offices in both Europe and the United States. However, as of yet, the effective implementation of Safe Harbour has been elusive; moreover, the BCR model is largely untested and unproven.[271]

---

270 BCRs should be viewed as co-regulatory rather than self-regulatory inasmuch as the DPAs must approve any BCR. That is precisely why they should be viewed as largely hypothetical at this stage, since so few companies have approved BCRs.

271 See Jan Dhont, Maria Veronica Perez Asinari, Yves Poullet, Joel R. Reidenberg, and Lee A. Bygrave, *Safe Harbor Decision Implementation Study*, Eur. Comm'n Internal Market DG Contract No. PRS/2003/A0-7002/E/27 (19 April 2004).

8.3.2 Standards and PETS

Awareness of international standards such as ISO 17799 and 27001 is high in the United States, but its implementation is less popular. Companies have achieved ISO 17799 or 27001 accreditation, but generally not for all of their respective organizations. In India, respondents felt that awareness by BPOs of varying international standards in this field was high, due to the requirement for them to be compliant with such standards to attract business. The adoption of standards in Western Europe and the United States is generally market-led, driven by companies choosing to do so for reputational or business reasons or to comply with certain requirements. By contrast, the use of sector-specific guidelines in Japan is encouraged by the government.[272] Such guidelines are specific to each industry or business area, and those covered by these guidelines are expected to abide by them.

As regards Privacy Enhancing Technologies (PETS), our survey found significant interest in the use of PETS, but many respondents felt that there has been limited actual deployment of PETS to date. We found extensive use of technologies that contribute to security and privacy, including firewalls and encryption. We also found that some 40% of all market players in our expert survey claim that their firms use some form of PETS.[273] This seeming disparity may in part reflect different understandings as to what constitutes PETS – the term PETS was not widely recognized by respondents in Korea, for instance, and not at all by respondents in Malaysia.

8.3.3 Effectiveness of measures other than law and regulation

In the U.S., TRUSTe along with other self-regulatory measures such as codes of conduct were seen by many market players to be the fairly effective self-regulatory tools; however, consumer advocates and lawyers expressed doubt as to their effectiveness, given limited enforcement powers, and also as to their practical ability to inspire consumer confidence. Many interviewees reported that the larger companies were vigourously pursuing a number of self-regulatory measures to help protect privacy, and that internal codes of conduct and technology were seen to be generally effective.

In India, awareness of foreign regulations was very high, and respondents commented that BPO organizations are sometimes required to be audited to the same standards as their customer companies. However, a number of high profile incidents suggest that implementation may not always be up to snuff in practice.[274]

---

272 See Section 4.2.
273 See Sections 2.2.2 and 9.3.
274 Man held in HSBC India scam probe BBC News 28th June 2006 available at http://news.bbc.co.uk/1/hi/business/5122886.stm (visited 19th July 2007).

In Malaysia, interviewees felt that the use of Privacy and Trust marks by domestic companies was very low. Interviewees were also vague on the application of certain industry codes to the protection of privacy.

In Korea, the role of PICO (the Personal Information Dispute Committee) operated by KISA was regarded by respondents as being effective as a place where users could make a complaint; however, take up of the trustmark system is low compared to the large ECSP market in South Korea.

In Japan, there are various labelling schemes, and interest in them is growing. For example, the number of companies receiving accreditation for the Privacy Mark scheme is increasing year on year (with telecommunication companies making up 40% of these accredited organisations). Interviewees additionally reported that the public was 'hyper-aware' of personal information protection issues.

In Europe, although the importance of self-regulation has been recognised, Safe Harbour continues to be ineffective.[275] Large disparities also exist in the promotion of codes of conduct. Although many companies have deployed information security solutions and organisational measures to help protect personal privacy, the effectiveness of these systems continue to be measured by the companies themselves.[276]

---

275 See Jan Dhont, Maria Veronica Perez Asinari, Yves Poullet, Joel R. Reidenberg, and Lee A. Bygrave,, op. cit.

276 Ryan, Rose IDC Market Analysis 2006: Worldwide Security Compliance and Control 2 0 06.201 Forecast and Analysis : Going Beyond Compliance to Proactive Risk Management p 10

9 Common Themes

As noted in the Introduction, the protection of privacy has to be viewed as a complex and interrelated system. The tendency is to focus primarily on legal and regulatory aspects; however, self-regulatory and co-regulatory aspects play an important complementary role in many countries, and these interact with technological and practical considerations in complicated ways.

This chapter deals with a number of over-arching themes that reflect these considerations. The discussion is for the most part motivated by our extensive interviews with stakeholders in the countries studied. U.S. respondents tended to speak at greater length than other interviewees, and many were willing to be quoted (typically without attribution); consequently, many of the quotations in this chapter are from U.S. respondents.

Section 9.1 deals with the complex trade-offs among regulatory, self-regulatory and co-regulatory arrangements. Section 9.2 deals with frameworks for privacy protection, notably with the relevant European Directives and with the APEC privacy framework. Section 9.3 deals with technological standards and Privacy Enhancing Technologies (PETS). Section 9.4 deals generally with costs and benefits of data protection, while Section 9.5 discusses the merits of a comprehensive, over-arching framing for privacy protection. Finally, Section 9.6 reflects on the impact of the differences in privacy protection regimes among the countries and regions that we studied, in particular in regard to the impact of these differences on trans-border data flows.

9.1 Regulation versus self-regulation versus co-regulation

Many respondents had strong views as regards the relationships between regulation, self-regulation and co-regulation. In this regard, the views of U.S. respondents were particularly illuminating. The differences in perspective between industry respondents and consumer advocates were particularly striking. It should be noted that the respondents' views often addressed regulation in general rather the specific applicability to electronic communications privacy.

Some market players argued for self-regulation in preference to conventional regulation. Some expressed scepticism as to the effectiveness of law and regulation. As a representative comment: „I am not convinced that introducing provisions like criminal accountability (as in [Sarbanes-Oxley]) is the solution to the problem, because what it means is that once a year the Chief Officers need to sign a report – not really anything new – just signing a report as well as filing it. I am not sure that this by itself makes for better protection, or that they are taking it that much more seriously. It is less than lip service being paid, because [failures are more likely to be attributable] to ignorance … or failing to think through all the ramifications of security vulnerabilities … than malfeasance."

Several responded in terms of privacy labels as an example of successful self-regulation. As one example: „They are very helpful for customer retention and customer confidence if people have seen them over a long period of time in other places (e.g. TRUSTe, BBOnline, Verisign); there are also various security standards to which enterprise industry will look to see if you are compliant, … and so these sorts of things are very helpful as it gives consumers and enterprises a certain comfort level when they go into a relationship as to what they might expect from the service provision and its compliance with privacy rules. These companies would not be around for long enough and would not have the respect they do in the community if [they did not do a good job]. For the most part (from what I hear), people are generally satisfied with self-regulatory mechanisms compliance, particularly in recent years." And another: „The TRUSTe label is a trusted brand. It is like when the 'normal' people started buying things on the internet, and they started seeing icons that alleged to represent security, and that became a big business for companies like Paypal. Privacy is the same – if you have a mark that is respected and known, … you will win."

Market players in our survey were not uniformly enthusiastic about self-regulation. This is consistent with experience – in 2005, for example, Microsoft publicly called for a comprehensive national privacy law in the United States.[277] One U.S.-based market player saw substantial risks inherent in self-regulation, and also expressed doubts about the ability of self-regulation to reign in abuses by government: „I am concerned about self regulation, I know that everybody is trying; [some companies] have succeeded, but it is not clear to me that without some kind of fine other than embarrassment this will work. Some companies just go out of business when they get caught. But what do you do to the Department of Agriculture (a US Federal government department recently in the news for losing data)? It is just a bit harder to say that the government regulation will fix it if a reasonable percentage of the leaks come from the government itself." In this same vein, another U.S. respondent opined: „Many organisations will only do something if it is actually written down in law, so self-regulatory mechanisms are great for the pro-active companies amongst us. We will go out and do as much as we can. But companies that do not have the resources will not bother with it."

Consumer advocates expressed concerns that purely self-regulatory arrangements were of uncertain effectiveness. In the case of voluntary codes of conduct, for example, sanctions for violations were rare to non-existent. In the absence of an effective enforcement mechanism, it was not clear that organizations would be sufficiently motivated to rigorously adhere to the codes to which they nominally subscribed. A U.S.-based respondent put it this way: „Self regulation has been an *alternative* to privacy protection; it has not been a *path* to privacy protection. This is the basis of our objection."

---

277 See Microsoft advocates comprehensive privacy legislation, Nov. 3, 2005, http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx

Consumer advocates expressed similar concerns about obligations for organizations to publish their privacy policies. They felt that scarcely any consumers actually read the privacy policies, and fewer still understood them. Consequently, organizations published policies that enabled them to do whatever they wanted. Thus, rather than constraining the organization's behaviour, the published policies served instead primarily to enable organizations to do nearly anything they wanted with personal data, and to insulate the organization from legal consequences for their actions.

One respondent put it this way: „The approach that the U.S. took in the 1990s was that it encouraged companies to develop privacy policies and the FTC stood in and said if you don't comply with your policy, it is a form of deception and we can prosecute you under consumer protection laws. … This is, in my view, not as effective as the European Union approach, and tends to create what can be described as a race to the bottom – if a company is going to be held to its privacy policy, then the obvious solution is that they develop a policy that offers as little as possible. The policy almost becomes a disclaimer or a waiver with the company saying, in effect, if you do business with us we will use your data in these ways and if you object to it, then take your business elsewhere. From a legal perspective, this is a privacy policy that the FTC would enforce, but from a consumer perspective this offers no protection. This is one of the consequences of the US approach: … Notices are created which instead of offering protection, instead disclaim any responsibility. … You run into privacy black holes which [reflect] the absence of any real meaningful oversight or enforcement, even though there may be very elaborate law and regulation."

For this reason, the consumer advocates often preferred co-regulatory arrangements over purely self-regulatory arrangements. They preferred arrangements where some public agency would retain explicit authority to evaluate and either accept or reject a code proposed by an industry body, and then to provide back-up enforcement in the case of violations. For example, a U.S.-based consumer advocate had this to say of privacy labels: „From a consumer perspective, they are seen as not very effective because they, like privacy policies, allow companies to do what they want. The labelling systems have tried to impose somewhat higher standards, but we would prefer to have a legal framework."

For analogous reasons, consumer advocates had some discomfort with purely voluntary codes of conduct. One respondent felt that codes of conduct were relatively effective; another said that they could be effective if properly backed up by legislation. The U.S. respondent said: „Codes of conduct are great when they implement statutes – in the U.S., we do have some codes which comply with statutes, and in some [instances] fill in for areas where there are no statutes, but again I think you need the solid foundation of the legal obligation, and you need to have codes of conduct that are meaningful and effective."

A U.S. respondent noted that generic codes of conduct typically have to be adapted to the circumstances relevant to any particular industry. „… Let's say an association pro-

poses a code to which an organization can then subscribe – rarely if ever are you going to have an organization that comes to receive one of these and can take it and use it as it. Every industry is a little bit different and has to change their processes to comply with a given law and this is one of the things that makes the EU model clauses most difficult to use and latch onto because they are so rigid in their terms that it made it impossible initially to take them and draft them and incorporate into your own compliance regime – sort of like 'a square peg in a round hole'. A certain amount of tweaking has to be done …"

9.2 Privacy frameworks

In recent years, there seems to have been strong interest in the privacy framework put forward by the Asia-Pacific Economic Cooperation (APEC) forum.[278] Given that four of the five target countries in our study (Japan, South Korea, Malaysia, and the U.S.) are members of APEC, the study team had expected to find strong interest in the APEC framework.

Somewhat to the surprise of the study team, none of our respondents volunteered the APEC framework as a significant factor in the deliberations on privacy in their respective countries. Those who were aware of the APEC framework viewed it as a possible long term interest, not an immediate concern. A Japanese respondent noted that there was interest in crafting a general approach to consumer privacy, but emphasized that the APEC privacy framework was just one of several approaches under discussion – it was not necessarily viewed as representing the way forward.[279]

Upon closer examination, this is perhaps not surprising. The APEC framework is conceived at a very high level. It could be viewed as an admirable statement of principles, but it lacks the kind of concreteness and specificity that would be required for implementation in a given member economy.

The APEC Privacy Framework is meant to accommodate a very wide range of implementation options[280] among APEC member economies.[281] It strives simultaneously to „… be consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Data Flows of Personal Data", and also to accord „… due

---

278 APEC, APEC Privacy Framework (2005), available at http://www.apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1.

279 For a discussion Japanese interest in the APEC Privacy Framework, see Section 4.1.5.

280 See especially Section II of the privacy framework, „Giving Effect to the APEC Privacy Framework", on page 31. See also page 34 – the guidance for international implementation is confined to exchanging information, not to practical measures.

281 APEC members have historically been referred to as „economies" in order to avoid the need to determine whether members such as Hong Kong and Taipei should be viewed as being countries.

recognition to cultural and other diversities that exist within member economies".[282] Given the enormous diversity of the APEC membership,[283] it is perhaps not surprising that this would necessarily lead to a framework that was very broad, but not very prescriptive.

Much the same could be said about the 1980 OECD Guidelines[284] themselves. They provide a useful set of principles, and OECD has supplemented them on occasion with practical advice[285]; nonetheless, they are not intended to provide a detailed road map for implementation.

Meanwhile, the OECD continues to do interesting and potentially valuable work in the realm of international coordination in regard to privacy. They recently published a Recommendation on privacy cross-border data flows[286], as well as a Recommendation on electronic authentication.[287] We understand that the OECD also hopes to launch a global survey of privacy in electronic communications at some future date.

In many respects, the European Directives have had a more direct impact on practice in the countries we studied, and probably elsewhere as well. The European Data Protection and e-Privacy Directives influence other countries through several vectors:

- They place certain constraints on non-EU countries in regard to trans-border data flows.
- Firms based in EU Member States reflect the Directives in out-sourcing arrangements with firms in other countries. This was emphatically clear in our interviews in India.[288]
- The European Directives represents a working, demonstrated model that is specific enough to be implemented, while still providing enough flexibility to accommodate the needs of 27 distinct Member States.

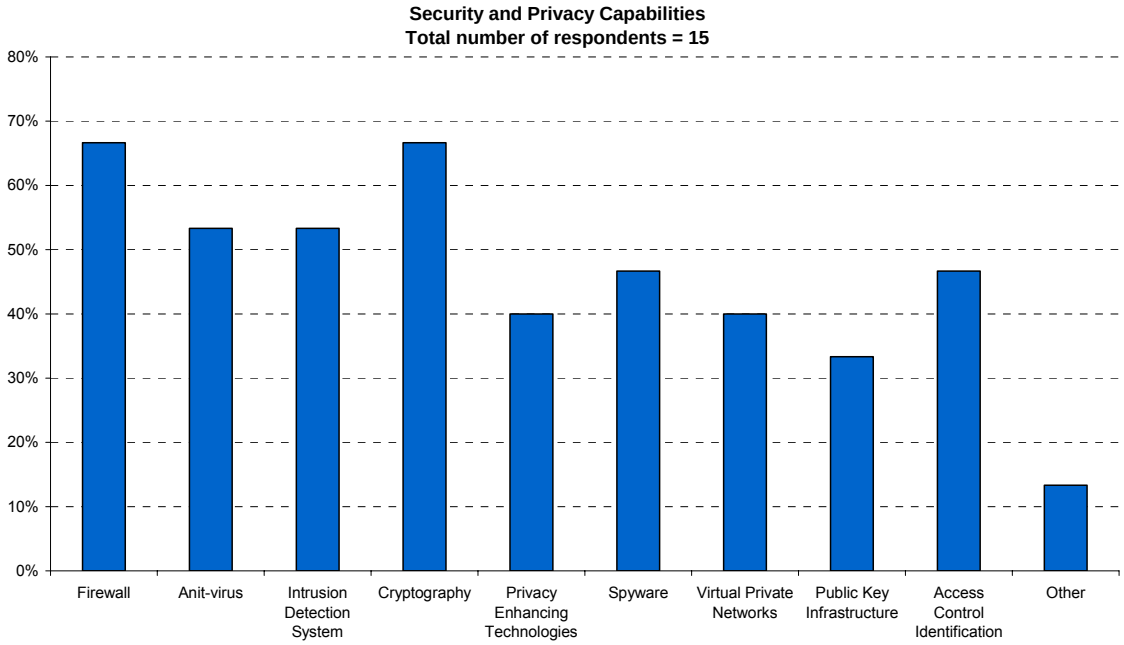
---

282 APEC Privacy Framework, op. cit, page 3.
283 See http://www.apec.org/apec/member_economies.html.
284 OECD, *Guidelines on the Protection of Privacy and Trans-Border Data Flows of Personal Data* (1980), available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
285 For example, OECD, *Privacy Online: OECD Guidance on Policy and Practice* (2003).
286 OECD, *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy* (June 2007), http://www.oecd.org/dataoecd/43/28/38770483.pdf.
287 OECD, *OECD Recommendation on Electronic Authentication and OECD Guidance for Electronic Authentication* (June 2007), http://www.oecd.org/dataoecd/32/45/38921342.pdf.
288 Somewhat the same could be said of U.S. privacy practices. For example, some Indian BPO (out-sourcing) firms were obliged to conform to California requirements to disclose breaches of personal data.

9.3 Privacy Enhancing Technologies (PETS) and technological standards

We asked respondents: „Which of the following information security products or services do you use?" Market players responded as follows:

Figure 2: Information security services used



Source: responses to this survey

Two privacy service company respondents considered SSL by Verisign to be the most commercially significant offering in the entire space of self-regulation of privacy in electronic communications.

The term PETS was not widely recognized by respondents in Korea, and not at all by respondents in Malaysia. Nonetheless, Korea has had a strong interest in PETS. Korea has made significant and early standards developments in SSL technologies, notably in SEED, a 128-bit symmetric key block cipher developed by KISA and industry experts starting in 1998. This choice has been a mixed blessing – since the world moved to different standards, Koreans have been limited in their choice of browsers, and the resulting monoculture is arguably a security risk. For a number of years, the Korean MIC and Korea Telecom (KT) have been developing a localized version of P3P, as yet without any outcome.

Views among market players on the effectiveness of these security measures in ensuring privacy were somewhat mixed. Some indicated that, despite serious efforts on the part of their respective organizations to maintain a high level of security, one could not take too much comfort in the absence of *known* breaches. As a U.S. industry participant put it, „[T]he other thing we found about security is that it is not interesting if you get in to a system, the interesting point is whether anybody notices. And right now it is very hard to notice whether your private data have been accessed…" At the same time one respondent spoke favourably of practices in India: „[P]rivacy requirements are driven by the customer organisation and the BPOs are contractually obliged. The main focus for BPOs is around security to meet their obligations. The customer companies specify the privacy set up and the BPOs will then implement the technical measures to meet this requirement. The view is that Indian BPOs are relatively good at this – they do a good job on the technical side of implementing security measures – the real challenges are with the human resource issue (e.g. personnel vetting) which is less mature in India and these are now being addressed through NASSCOM's National Skills Registry initiative."

Respondents from privacy service companies tended to be somewhat more optimistic about the effectiveness of privacy and security solutions, but they cautioned against resting on one's laurels. For example: „We are usually ahead of the actual threats which are seen in the wild. This doesn't mean that there are not more threats which are out there which we need to continue to develop responses to."

A range of technological standards, most of them more directly relevant to security than to privacy, potentially complement privacy arrangements. One of the most prominent of these is ISO/IEC 27001. ISO/IEC 27001 is an information security management system (ISMS) standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. Its full name is ISO/IEC 27001:2005 - *Information technology – Security techniques – Information security management systems – Requirements*. Many respondents referred to ISO 27001, and a number referred to it as significant for Business Process Out-Sourcing (BPO) firms in India.

Only one respondent indicated that they had implemented the W3C Platform for Privacy Preferences. Six respondents indicated that they were not. Some had never heard of P3P; some considered it too hard; still others saw no need in their respective national markets. A U.S. consumer advocate said that P3P „…is not useful. To me, P3P was simply a way of coding the notice and choice approach to privacy protection, which is much less helpful than the traditional fair information practices approach. Our definition for Privacy Enhancing Techniques is a 'technique that minimises or eliminates the collection of personally identifiable information.' All the other approaches are about getting consumers to consent to a disclosure of their data. We don't view this as privacy enhancing."

Multiple respondents felt that security technology was effective, but that in many cases users failed to properly employ features (for example, encryption). One noted that poor

personnel practices could also undermine technological measures – insufficient vetting of new hires, for example, could nullify the effectiveness of technological safeguards.

A U.S. consumer advocate had this view: „My optimistic view of the links between data protection legislation and technology is [that] if the data protection legislation can internalise the costs of the risk of the misuse of personal information, then companies will … not simply develop better practices, they will develop better techniques which will enable commerce without the collection of so much personal information. [There is an] analogy with the environmental world, [where the goal of policy is to motivate] companies to do a better job of manufacturing with minimal impact on the environment."

A U.S. telecoms industry respondent felt that, even though large enterprise was investing in security and privacy technology for the enterprise as a whole, that there was in some sense surprisingly little actual use of PETS *by individual employees* even in instances where the technology was straightforward and mature. „The big companies are buying mature and advanced technological solutions. … Most companies do not use privacy enhanced mail (e.g. PEM or S/MIME). If they do have a need it is internally, in which case they use a VPN, so things are well enough protected. Even with individuals, there is not that much use of privacy enhanced email. This is an example of good technologies in some respects beyond the research stage and at the product level, but people are not concerned enough about the risk to use the privacy-enhancing technologies."

9.4 Perceived costs and benefits of data protection

No respondent was able specifically quantify the costs or benefits of arrangements in support of any aspect of privacy and trust. In fact, many respondents were emphatic in noting that it was difficult if not impossible to provide hard metrics. For example: „You want a return on investment, then good luck. One of the hardest questions in research in cyber security and privacy is metrics. 'How secure are we?' No one can answer the question, it depends on so many things, and on peoples' interpretation. We don't have good metrics on security and privacy. Another issue is definitions." Another opined: „[I]t is very hard to understand what the ROI is for investing in privacy and security. The smaller the organisation, the less clear the ROI – there are some simple security measures that have a clear ROI (virus protection, firewalls, that sort of thing)." A U.S. consumer advocate said, „[P]rivacy does not have metrics that are as well defined as some other areas where we might consider social protection legislation (e.g. the environment) over time (which we do have). Cost benefit metrics are necessary for privacy protection. Downstream costs of misuse of personal data only increase over time. My hunch is that whatever can be done now to minimise those costs will be money well spent. … Most companies would say that they do not invest as much in [privacy and security] as they should. It's very difficult to translate benefits to the end user. If a better job could be

done of making people aware of security risks and the need for good security, then maybe over time consumers might understand the costs."

Given the complexity of the subject, this is perhaps not surprising. Nonetheless, quite a few of our respondents provided comments that help to illustrate the cost/benefits trade-offs involved.

Multiple U.S. market players felt that respect for privacy served to enhance trust, and that the financial benefits of maintaining a good reputation exceeded any costs. (One respondent disagreed.) One U.S.-based respondent put it this way: „Our firm's behaviour is not based on cost benefit analysis – we have a very significant brand … [B]ecause our business is the business of managing data, we aim to be the best at managing data. We know what we need to do. We are not perfect and we have incidents and the environment where we operate is becoming more complex … I think that if I were in the business of creating a business case or justifying investment in this area, there is not a whole lot to draw upon … [Y]ou can make surveys of consumers and individuals in a any country and ask whether privacy is important, and they say yes, but how much does it cost to rectify a data breach or a security breach?"

A similar view from another U.S.-based respondent: „[O]ur brand is synonymous with trust. [Our firm is] a premium price company, its offerings have a lot of customization – people turn to [us] and know that they can trust the company. Part of this is knowing that you are going to get a consistent, quality experience every time at all your 'touch-points'. We may not always deliver on this, because there is no perfection here, but this is the aim. … [W]e rarely make an explicit marketing pitch saying we do a good job of protecting data; it's built into how we operate, and it is an assumption."

Others made substantially the same argument by claiming that the costs of failures to maintain privacy exceeded any benefits (e.g. the money saved). One said: „If it starts hitting the first page of *USA Today*, and the broader public starts asking questions, then it becomes a sales tool. If you then stand up and say our service is more secure – whether that is true or not – it may become a sales tool. Competitive advertisement clearly follows news reports." Another said: „The Return on Investment is always a question of economics and brand. It's like with buying insurance: If I don't buy insurance and something happens, what is this going to do to my stocks? It is also important what my competitors do – of course, no one wants to talk about their security and privacy stance. So it is really hard to convince people to do it."

Another U.S. respondent spoke thoughtfully of a trade-off between the need for economic development, and the respect for privacy as a human right. „[C]omplex regulation makes it more difficult to launch and grow businesses – that in and of itself is not an argument for not having some policy on this area, but it does signal that you have to be careful … [I]n an information-based services based economy (like most of the Western countries), deeply regulating the nature of data flows and data handling should be done with great care, because [ICT] is the medium by which productivity is generated. So in

fact this is an economic development issue, as well as it being a human right (which is also extremely important) … [B]oth interests (privacy as a human right and as an economic development issue) need to be reflected, and no-one has come up with how to do that."

Korean and Malaysian respondents were unable to answer our questions about cost benefit. Large IT companies recognized the costs of implementing enhanced security products and mechanisms to protect privacy, and recognized the need for privacy and its importance to the corporation in terms of reputation, public relations and even competitiveness; however, they had not considered privacy protection in terms of cost benefit in either the sense of a formal project management discipline or an informal decision making processes. Their lack of response to these questions perhaps reflects the generally limited sensitivity to privacy and its importance to the business process that we observed in these countries.

9.5 The desirability of a comprehensive framework for data protection, analogous to that of the European Union

Most respondents felt that a harmonized, cross-sectoral law should be implemented, or at the very least the current state of the law should be improved/clarified. Most felt that their respective countries are moving forward with this; however, as one respondent stated, „comprehensive data privacy requires a lot more than just a new law."

Even so, there was a tendency, particularly in the United States, for industry players to view the desirability of a comprehensive privacy framework differently from consumer advocates. For market players, the motivation was primarily to simplify regulation. Consumer advocates argued instead that the lack of a comprehensive framework in the U.S. left the consumer at a significant disadvantage.

A consumer advocate told us: „I have been making the argument for the past 20 years to Congress that what is required is a combination of a privacy framework approach combined with sectoral legislation. The European approach to privacy protection is generally more sensible and more practical. [It] is more respectful of privacy rights and does a better job of anticipating how to respond to emerging privacy challenges than the patchwork response in the U.S. I think the U.S. is in large measure in disarray – it doesn't have effective ways at present to deal with ID theft and security breaches, and it's clear that those problems are on the increase."

Some industry people, on the other hand, argued that the European system was rigid, while the U.S. system was flexible. One U.S. market player said: „I would not like to see a European Framework approach. Most people want to have their choice when it comes to privacy, they want to have their choice in respect to accessing their information any

time, anywhere, at their convenience, they might want to opt for better services. The European laws are far too limiting on how to use information."

Another U.S. respondent noted that the patchwork quilt of laws and regulation represented a significant burden for telecommunications service providers. „From the U.S. side, we have extensive regulation from the Federal Communications Commission (FCC) for our voice services, the Cable Privacy Act for our TV offering, we have Federal and State security laws, the Electronic Communications Privacy Act (ECPA) (those are more focused on existing law enforcement and limiting interception of any communication), and we have a variety of breach notification laws and limitations on the use of personal identifiable sensitive information. These regulations are not at all easy to deal with, they are all over the place, depending on where you are doing business (especially the ones that are state-specific), and each has so much regulation attached to it, so much so that it is quite complex, and quite a task to keep up with everything. As a communications provider, we not only have to deal with the law that is sector specific – a lot of the privacy laws don't govern our business, but they are very important to our customers, so we have to be aware of them and make sure we do what we need in order to protect the interest of our customers, such as the health care privacy laws and the financial services privacy laws. Within the Telecommunications Act, it is the CPNI rule that is focused on privacy, the Act itself is not focused on privacy."

Multiple U.S. respondents from the private sector and from government argued that it would be a mistake to equate the lack of a comprehensive data protection framework in the U.S. with a lack of data protection. They argued that there was, in fact, a range of measures in place, and that a great deal of enforcement takes place. A U.S.-based lawyer said: „It's untrue to say that there is no privacy law in the U.S. – this is a common misconception (even at high levels within the European Commission). There is no overarching framework law as in Europe, but a number of sectors (e.g. medical privacy, financial services, video records, telecoms records) all have laws relating to the use of personal information. It is true to say that there is nothing similar to the European Framework, but almost all the sectors that deal with large amounts of personal info have privacy law. … There is a tremendous amount of law and enforcement in the United States around privacy and security, it's just that it is not comparable to the European system." A U.S. government respondent made similar points.

The study team's research suggests that this perception of enforcement in the U.S. may possibly be inaccurate inasmuch as enforcement actions for the misuse of personal information in electronic communications are in fact quite rare.[289] The disparity between actual practice and the perception of many of our U.S. respondents might suggest that fear of enforcement continues to have significant deterrent effect. We would note, however, that it can be difficult to interpret the significance of the number of enforcement actions – a low number might indicate ineffective enforcement, or it might indicate a

289 See Section 3.5.1.

high degree of voluntary compliance.[290] Our data provide no basis on which to independently verify or refute the perceptions of the experts that we polled.

Two consumer advocates (neither U.S.-based) were asked about the degree to which legislative, self-regulatory and technical / organizational measures work together to ensure an effective level of data protection at the local / national level. The German consumer advocate said: „They work together better where the legal basis is more binding and clear, and where it is internationally harmonized." The South Korean respondent said: „Poorly. An integrated law is needed." Given the differences in their respective national systems, the differences in their responses is striking.

9.6 Perceived impact of differences between countries in data protection

A number of respondents remarked on the costs implicit in differences in privacy practices between the European Union, the United States, and other regions of the world. Many of these comments relate to trans-border data flows, a complex topic that was not an explicit objective of this study. Nonetheless, a number of the comments were illuminating.

A U.S.-based consumer advocate articulated the general issues between the U.S. and the EU in this way: „I think today as opposed to 10 years ago, people working on privacy in the United States (and I am thinking specifically of chief privacy officers of major corporations in the United States) are more familiar with the EU Data Directive and the OECD Privacy Guidelines. Today, for a U.S. company, it is virtually impossible if you are working on privacy issues to be unfamiliar with the Directive and the Guidelines. To a large extent, the U.S. tends to be very parochial, and it does not see itself participating in a global privacy framework. U.S. courts have only just grudgingly recognized the authority of foreign law, and these cases are very rare. In this respect, we only talk about privacy in the United States in terms of national or even state law. (… [A] lot of states have individual privacy laws.) … Privacy experts now are familiar with international legal frameworks, ten years ago that was not the case. So we are making some progress, but there is a lot more that still needs to be done. The discussion on whether we have convergence or divergence (with international privacy frameworks …) has been viewed in the context of *exceptionalism* (the US puts itself apart from other countries basically with a view that it isn't bound by any other laws)."

One respondent spoke of the need for progress toward a common understanding of the goals and the legal basis for privacy arrangements in the US and EU: „The best opportunity for improvement would be for the US and the EU to continue to understand or come to grips with the basis for their own legal regimes regarding privacy. For example,

---

290 Cf. Bennett and Raab, op. cit.

we know what the foundations for the Data Protection Directive in the EU have been, and most [of that] comes from cultural and historical issues. We know that the industry-focused approach in the US has developed from a very uncertain treatment of privacy under the US constitution. As we get further down the line, and many international businesses try to comply with scopes of laws in the EU and US that are very different, the best case for improvement is for EU and US legislators and businesses to come closer and closer to a meeting of the minds [about] what it is they want to protect, and what sort of consumer data is at risk most, and [that understanding] needs to have some kind of compliance mechanism around it."

Two U.S. respondents commented at length on trans-border issues. One discussed the implications for the multi-national firm for which he works: „Industry has gotten smart in a number of ways to help facilitate the compliance mechanism at the end of the day it does what the spirit of the EC directive was looking for, but doesn't necessarily break the back of the industry in trying to accomplish it and trying to get the consumer and customer a service that is quicker and cheaper as a result. … Recent history (last 8 years) … has seen the development of Safe Harbour for compliance with the European Commission Privacy Directive … A few industries including the telecom industry were left out of Safe Harbour, as well as financial services and transportation. The telecom industry had to look at and use other options – Inter Company Agreements (ICAs) and Binding Corporate Rules (BCRs). Binding Corporate Rules are an EU approved (since 2003) alternative to Safe Harbour … Safe Harbour works by companies signing up to a statement as to what they do with data, what they have done with personal data, and then action is taken under the remit of the FTC's authority in the US. … BCRs and ICAs are obligations companies make not only to their customers but amongst themselves by agreement, whereas the Safe Harbour arrangement was constructed that companies could say something publicly that a regulatory body could then field complaints from and take action against … (see http://www.export.gov/safeharbor/sh_overview.html for more information). This means [that the use of BCRs] is just different – not 'better or worse' [than Safe Harbour]. One model is based on a body of law that is contractual, and the other is based on a statute."

Yet another U.S. industry respondent said:

> We are exempt from safe harbour as a telecommunications provider, so we use inter-company agreements based on the ICC standard contractual clauses to signify the adequacy requirement signed by each of our entities throughout Europe, Asia, Pacific and America, basically stating which systems are transferring data to the US and how the data are be dealt with. The ICC model standard contractual clauses have been approved by the European Commission; they are more or less the same as the EU standard contractual clauses, although some third party beneficiary rights that were slightly amended.

When the Directive was introduced, they had to find a method by which the EU Commission could be assured that if information was transferred outside European Economic Area, an appropriate safeguarding and security was in place in the country to which the data was sent (e.g. if financial data is transferred by a company from the UK to the US, as in the US … basically no privacy legislation is in place apart [from] the sectoral legislation). So the EC [asked] organisations to put into writing how they would go about transferring the information to their entities in the US in the appropriate manner in accordance with the requirements of the EU, and that's what the contracts do. We spent a lot of time negotiating contracts with large multinational companies, who we are going to be offering services to, and they ask the question how we are going to guarantee the adequate requirements and when we mention the contracts they are satisfied.

We have 'binding corporate rules' (BCRs), this is a new method by which a multinational organisations can work with a designated data protection regulator to have their policies, procedures, training (everything to do with how you deal with privacy and personal information) assessed to see if it is adequate for the purposes of the EU... It can take up to 2 years, but at that point the data protection regulator would state that your binding corporate rules are approved, which means that you could transfer the data wherever you want outside the European Economic Area within your entity. You are appointed as lead data protection regulator, it is normally where your biggest office or your European headquarters is … So we would work with the information commissioner and then they would send all the relevant documentation to each of the regulators of the countries where we operate and ask them to approve it.

10 Recommendations and observations

In this section, we present our recommendations and observations to the European Commission as regards the establishment and enforcement of privacy rights.

Inasmuch as our study was focused on the target countries, and not on Europe, our recommendations must necessarily be tentative. We have not attempted an impact assessment on specific initiatives. At the same time, our study of the target countries provides insight into mechanisms that are working well elsewhere and that potentially could serve well here in Europe.

10.1 Legal protection of privacy

Legal protection of privacy could in principle be (1) enshrined as a legal right in a country's constitution, (2) effectively crafted as a legal right through judicial interpretation of the constitution, (3) implemented through comprehensive privacy legislation, or (4) implemented through narrower and more targeted (e.g. sector-specific) legislation. Korea is an example of (1); India is an example of (2); Japan is an example of (3); and, the U.S. is an example of (2) and (4). Malaysia can not be said to fall clearly in any of these categories.

Among the countries which we studied, the choice among these options does not uniquely determine the effectiveness of privacy protection. Notably, an explicit constitutional right to privacy does not automatically translate to good protection of that right.

The presence of a comprehensive and coherent legal framework for privacy seems to correlate with more effective and consistent implementation and enforcement of individual privacy rights. Countries with a fragmented legal and regulatory framework seemed to experience more legal and regulatory asymmetries, more gaps in law and enforcement, and less predictability than jurisdictions with a comprehensive framework (notably Japan and Europe), even though the fragmented systems often implement considerable protection of privacy in specific, targeted areas.

We think that stakeholder input generally supports this view, although by no means unanimously.[291] A number of Asian respondents spoke of the need for a unified privacy framework in their respective countries. Market participants emphasized that law and regulation represent only one leg of an integrated system to maintain privacy, and one specifically opined that he considered a European-style system to be too inflexible; at the same time, a number of market participants felt that the fragmented system in the U.S. imposed needless cost on businesses. The comments from the U.S. tend to bear out the notion that enforcement is uneven, and that data protection overall may be quite strong in some sectors, but weak in others.

---

291 See Section 9.5.

These observations do not imply the need for a change of direction in Europe. If anything, they reinforce the value of Europe's comprehensive approach to data protection.

10.2 Self-regulatory and co-regulatory arrangements

Many of the countries studied make extensive use of self-regulation and of co-regulation.

Codes of conduct and privacy labels are prominent examples of self-regulatory arrangements. Many industry respondents were favourable to these arrangements. Consumer advocates and some other respondents were more sceptical, expressing the concern that sanctions for poor performance were insufficiently enforced and therefore ineffective. The sceptics often preferred co-regulatory arrangements, where the government plays a role, to purely self-regulatory arrangements.[292]

As an example of a co-regulatory arrangement, COPPA in the U.S. enables the FTC to approve specific trade association guidelines for the collection of personal information from children. Adherence to those guidelines then provides firms with a safe harbour for their data collection activities. As another example, CALEA in the U.S. provides firms with safe harbour for their deployment of network technology that complies with industry standards, and authorises the FCC to determine whether particular standards are adequate.[293]

These co-regulatory approaches seem to be used less often than they might be in Europe. Properly applied, they can empower industry to develop cost-effective standards and processes, while still enabling public policymakers to retain sufficient control and to intervene if the market is not offering privacy compliant products or services.

The Japanese „Ministerial Guidelines" described above are an example of industry establishing its guidelines within a framework established by government. This approach facilitates the uniform drafting of privacy policies in each sector, and thus mitigates the risk of consumers facing too many different privacy policies. It also creates the possibility of sector by sector negotiation between consumer groups and representatives of the companies in the sector. The Japanese system of „Authorized Personal Information Protection Organizations" is based on privacy guidelines voluntarily drafted by a group of companies or other organizations. Encouraging participants to draft solutions will in some cases be more effective than imposing top-down solutions.

---

292 For a discussion of stakeholder input as regards regulation, self-regulation, and co-regulation, see Section 9.1.

293 47 U.S.C. 1006.

10.3 Privacy labels / Trustmarks

Experience in a number of the countries studied suggests that privacy labels or Trustmarks (such as TRUSTe and BBBOnline) can serve a useful role by strengthening commercial incentives for firms to ensure the reliability and effectiveness of their privacy policies and procedures. Trustmarks are a relatively unintrusive approach that can serve as a useful complement to explicit legal and regulatory privacy protection.

Many respondents emphasized that the potential threat to a firm's reputation was in general a far more effective incentive for good performance than any likely legal or regulatory response.

Some respondents, as previously noted, were cautious about endorsing privacy labels that operate on a purely self-regulatory basis. Their perception, which is supported by our assessment, is that these systems are not necessarily aggressive in enforcing the conduct of their members.[294]

The JIPDEC system developed in Japan is an example of a successful co-regulatory privacy label approach.[295] Systems of this type merit further study, inasmuch as they could potentially ameliorate the concerns of respondents about lack of enforcement.

For a labelling system to be effective, the criteria used by the labelling authorities and the way in which compliance with those criteria is checked must be transparent and must be effectively applied.

The privacy label approach is not much used in Europe, but we see no reason in principle why the use of Trustmarks could not be expanded here. This topic merits further study.

10.4 Enforcement and deterrence

Without effective enforcement and deterrence measures, the right to privacy is all but moot.

It is difficult to quantify the level and efficacy of enforcement measures. Most enforcement statistics lend themselves to multiple interpretations. For example, it may be impossible to determine whether a greater number of enforcement actions over time is the evidence of a greater number of infractions, or simply stronger enforcement against a constant level of violation.

Fines can be a key enforcement mechanism. Fines primarily seek to constrain future conduct of companies, and only secondarily to compensate victims. In fact, fines often

---

294 See Sections 9.1 and 3.5.2.
295 See Section 4.2.2.1.

fail to provide adequate compensation for victims. In the U.S., for example, the FTC does not normally compensate victims. Normally, fines imposed go into Treasury or to funding the FTC and damages awarded to victims are salutary.

Oftentimes, the fines levied against violators may not be sufficient to deter violations. If a fine were too small, a firm might simply view it as a normal cost of doing business.[296]

Some countries such as the United States and Japan rely on a „shame and blame" approach as a complement to formal enforcement in order to guide the behaviour of firms. Shame and blame seeks to ensure that the reputation costs of a violation are sufficiently high so as to act as a deterrent. Yet, shame and blame depends first on consumer awareness of the practices of service providers and on whether awareness is a significantly strong consumer preference so as to have economic impacts on would be violators. It also may serve to chill the market for e-communication by making consumers 'hyper-aware' of privacy (but there is no data to support this). Furthermore, such public embarrassment of violators may be completely ineffective when the violator is unknown, as in the case of unsolicited email.

Differences in privacy litigation such as whether the suit is based on statutory provisions or breach of contract can impact the adequacy of privacy protection. For example, an ECNP could easily slip inadequate *de minimis* liquidated damages for a privacy violation into its service level agreements, which are largely unnegotiated, unread contracts of adhesion. A singular reliance on breach of contract law might thus provide insufficient protection against privacy breaches.

10.5 Breach notification

In the U.S., many states require ECSP, ECNP and Service Users to disclose any inappropriate release of consumers' personal data to public authorities, or to the impacted consumers, or both. In Japan, disclosure under these circumstances is encouraged, and in some sectors it is required.[297]

The disclosure obligation can be viewed as a positive contribution to transparency. Moreover, the risk of disclosure likely creates or reinforces appropriate economic incen-

---

296 This theme appeared repeatedly in our interviews. One respondent said: „[Fines] are better than the alternative – given the choice of having fines and sanctions, and not having fines and sanctions, I would prefer to have penalties because generally speaking if you establish a legal right it will not have much impact unless you have the force of enforcement behind it. One of the criticisms of fines is that they are not sufficient to match the scope of the benefit to the company of violating privacy, so if you think about these issues as economic concerns then (some firms might] be prepared to accept the fine – they will just factor this in as the cost of doing business."

297 See Section 4.1.5. In FY2005, a total of 1,556 cases of information breach were disclosed.

tives for service providers to take reasonable care with customer data and with network and service infrastructure. This is consistent with the views of multiple respondents.[298]

As part of the 2006 review of the European Regulatory Framework, the Commission has proposed to impose obligations of providers of publicly available ECS to disclose breaches of consumer personal data.[299] Some Member States already impose obligations, but there is no consistent breach disclosure obligation across the European Union. Experience in the U.S. and in Japan suggest that an obligation to disclose breaches can be a workable and appropriate policy instrument.

10.6 PETS and technology driven solutions

Privacy Enhancing Technologies (PETS) are a promising approach. We found significant interest in PETS, even though some respondents felt that there had been limited deployment to date. We found that some 40% of all market players in our expert survey claim that their firms use some form of PETS.[300] This seeming disparity (some respondents claiming to use PETS, others perceiving deployment as limited) may in part reflect very different understandings as to what constitutes PETS – the term PETS was not widely recognized by respondents in Korea, for instance, and not at all by respondents in Malaysia.

The awareness of PETs in Europe is relatively low – Eurobarometer data for 2003 indicates that 72% of EU citizens had not even heard of these technologies. Awareness, and also willingness to invest, appears to be greater for security software and services, which in some cases also serve to enhance privacy. For example, a 2005 Eurobarometer edition of *Statistics In Focus on Trust and Security* indicates that nearly 60% of all companies with 250 staff or more reported that they perform encryption of customer data.

RFIDs might possibly provide another opportunity for the development of privacy policies based on PETS. It is likely that solutions would be required not only data processing, but also for terminal equipment. In the case of terminal equipment, some mix of standardisation, guidelines, and required labelling of terminal equipment might be appropriate. We should note, however, that RFIDs have not been a focus of this study.

The European Commission might wish to fund more research into PETs, using research funding to determine the economic benefits of information security upon privacy.

---

298 For example, a U.S. respondent observed : „Sanctions/Fines are important, but there are various negatives associated with a compromise in personal information … [F]or companies that have significant brands, the reputational risk is much larger than everything else. We will do a lot to stay out of the newspapers for these issues."

299 See in particular the Commission Staff Working Document … on the Review of the EU Regulatory Framework for electronic communications networks and services: Proposed Changes, {COM(2006) 334 final}, 28 June 2006, SEC(2006) 816.

300 See Sections 2.2.2 and 9.3.

10.7 Liberty versus security

There is a significant interplay between national security interests and privacy protection. Across all of the countries we studied, each has tried to strike a balance between privacy and security; however, since the terrorist attacks of recent years in New York City, Washington DC, Madrid and London, policymakers in several countries have tipped that balance in favour of national security over individual privacy. In this new security environment, hard choices need to be made, and it is all too easy to go too far in sacrificing privacy protection in order to facilitate the needs of national security.

The varied experiences in the countries that we studied serve as a reminder that this issue will require the ongoing attention of policymakers. They also serve as a note of caution to Europe. They do not necessarily indicate a preferred direction, nor do they imply that Europe needs to change direction in any particular way.

10.8 The Relationship of Cultural Attitudes and Development Issues

Cultural and development aspects can have as great an impact on the protection of privacy as the legal rights do themselves. Separating out where differences in privacy are related to culture or development is not always easy.

For example, in India, the absence of good privacy protections appears to reflect both societal attitudes and competing priorities (development issues). Existing cultural norms help to shape consumer and business attitudes towards privacy concerns. Our interviews found high awareness of the need for protection of privacy in conjunction with business out-sourcing for European clients, but little interest in privacy protection on behalf of Indian consumers. In a country which has an estimated 20 to 65 million bonded labourers,[301] 23.3 million people living in hunger,[302] and 40 million children who do not attend primary school,[303] it is easy to see how privacy concerns may go unattended. Competing priorities can thus lead to an underinvestment in enforcement of consumer privacy rights.

The willingness and ability of industry to support consumer privacy presumably reflects both the perceived benefits, and the availability of resources. In a country like India, perceived benefits may be relatively low, and available resources more limited, so both the willingness and the ability to invest in the protection of consumer privacy as a domestic matter may tend to receive only limited attention.

---

301 U.S. Dept. of State, Country Reports on Human Rights Practices- 2004, February 2005.
302 rediffnews.com, 2004
303 Ibid.

Malaysia exhibits similar characteristics. Since the mid-1990s, policies supporting the development of an advanced multimedia and communications sector have been the centre-piece of national economic policy. When these policies were first presented, the introduction of comprehensive data protection legislation was one of the features of the proposed constellation of „cyberlaws“ that would create the enabling environment for the new ICT sector; however, as new industries began to develop and to offer and use online services, they saw such new legislation as a potential barrier to expansion. It seems that lobbying by industry has to date been effective in preventing any comprehensive protection of privacy from emerging.

At the same time, users have not demanded that their personal data be protected. This should perhaps not be surprising in a country where freedom of expression is not well guaranteed overall. Nonetheless, the electronic communications market is becoming more sophisticated and competitive, and some industry respondents said they saw protection of privacy as a service that could help differentiate them from their competitors.

Malaysia is also culturally important as an Islamic country. Islamic teaching defines strong rights to the protection of privacy, yet these traditions are not as yet reflected in legislation for privacy and data protection[304].

South Korea is a somewhat different example. In the 50 years since the end of the Korean War, the country has developed from one of the poorest in Asia to one of the world’s wealthiest, and is certainly among the most advanced in the use of advanced communications technologies and services. Economic growth has been rapid, and has been driven by the very active hand of government in developing and promoting major industries. This industrial policy tradition can be seen in even in quite recent legislation about data protection, where the intent of the law is as much to promote the industry or the sector as it is to protect rights. It is clear that Korea is now an advanced economy, and that it no longer needs such strong intervention. It is a sign of this maturing society that respondents from all sectors agreed that comprehensive data protection legislation was necessary now for Korean society as a whole.

The importance of cultural and developmental norms indicates that more of a cross disciplinary approach may be needed when reviewing the arrangements for privacy and trust in the Member States of the European Union. Such an approach may flag to policymakers other issues which may have an impact upon attitudes to privacy, but might not otherwise be the direct focus of those in charge of policy intervention.

---

304 see Ida Madieha bt. Abdul Ghani Azmi ibid

Annex 1: Summary Comparison Matrix

	Europe	U.S.	Japan	South Korea	Malaysia	India
Laws and Regulation						
Explicit constitutional right to privacy	Yes	No	No	Yes	No	No
Statutory right to privacy	Yes		Yes	Yes	Yes	
Judicially crafted right to privacy	Yes	Yes	Yes	No	No	Yes
Comprehensive law	Yes	No	Yes	No	No	No
Sector-specific law on privacy of electronic communications for:						
ECSP	Yes	Yes	Yes	Yes	Yes	Yes
ECNP	Yes	Yes	Yes	Yes	Yes	Yes
Infrastructure Products	Yes[305]	Yes	Yes	Yes	No	N/A
Service Users	Yes	Yes[306]	Yes	Yes	Yes	N/A
Regional or local laws on privacy of electronic communications	Yes.[307]	Yes	No	No	No	Yes

305 According to Article 14 of Directive 2002/58/ECc, Member states may adopt measures which ensure terminal equipment is compatible with the user's right to privacy.
306 State laws govern protection the confidentiality of telephone and electronic communications and provide transparency in cases of breaches of data security.
307 Directives 95/46/EC and 2002/58/EC must be implemented by law in the 27 Member States. Due to their institutional framework, some Member States could have local laws which govern electronic privacy rights. In those cases these laws must respect the rules prescribed by the two privacy Directives.

	Europe	U.S.	Japan	South Korea	Malaysia	India
Enforcement measures						
Public Authority						
ECSP	Yes	Yes	Yes	Yes	Yes	None
ECNP	Yes	Yes	No	Yes	Yes	None unless Ministry of Commerce and Industry ISP licences
Infrastructure Products	Yes	No	Yes	Yes	No	None unless Ministry of Commerce and Industry ISP licences
Service Users	Yes	Yes	Yes	N/R	N/R	None
Private Litigation Right of Action						
ECSP	Statutory Liability	Statutory Liability	Civil Law and Administrative Complaint	N/R	N/R	Breach of Contract
ECNP	Statutory Liability	Statutory Liability	Civil Law and Administrative Complaint	N/R	N/R	Breach of Contract
Infrastructure Products	Breach of contract + Judicial claim for compensatory damages	Potential Tort Claim	N/R	N/R	N/R	
Service Users	Statutory liability	Statutory Liability	N/R	N/R	N/R	Breach of Contract?

	Europe	U.S.	Japan	South Korea	Malaysia	India
Measures other than law or regulation						
Co / Self - Regulation for:						
ECSP	Yes	Yes[308]	Yes	Yes	Yes	No
ECNP	Yes	Yes[309]	Yes	Yes	Yes	No
Marketing associations		Yes	Yes	No		Yes[310]
Consumer associations		No	Yes	No	No	No
	Europe	**US**	**Japan**	**South Korea**	**Malaysia**	**India**
Privacy Enhancing Technologies for:						
Vendors	Yes	Yes	No	No	No	No
S/W manuf			No	No	No	
S/W providers			No	No	No	
Standards for:						
Vendors	Yes	Yes	No	Yes	No	Yes[311]
S/W manuf			No	No	No	
S/W providers			No	No	No	

308 Company internal codes of conduct.
309 Company internal codes of conduct.
310 Do-not-call register.
311 As agreed with customer.

Annex 2: Individual Country Comparison Matrices

Europe

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	In the context of the Council of the Europe, article 8 of the European Convention on Human Rights (ECHR) explicitly enumerates Privacy as a fundamental Human Right, subject to possible interference by public authorities only under limited and highly circumscribed circumstances. A large body of case law has significantly extended the Right to Privacy by asserting a right of each individual to self-determination including vis-à-vis private companies. In the context of the European Union, the right to privacy (or 'to respect for the private and family life, the home and the communications') is enunciated by article 7 of the Charter of Fundamental Rights of the European Union in exactly the same wording as the first paragraph of Article 8 of the ECHR. Furthermore, Article 8 of the Charter provides for a new constitutional fundamental right: the right to data protection. According to that right, personal data must be processed fairly for specified purposes and on the basis of a legitimate basis laid down by law. Every person has a right of access and to rectification to data that has been collected concerning him or her. Compliance with these rules must be subject to control by an independent authority. Most of the European countries have enacted privacy as a constitutional liberty.
	Comprehensive law	The overall framework for the protection of personal data is set forth by Directive 95/46/EC which applies to any operation or set of operations which is performed upon personal data. The Directive provides for important data protection principles, main of which are the purpose limitation principle, the data quality and proportionality principles, the transparency principle, the security principle, the existence of rights of access, rectification and opposition and restrictions on onward transfers. These rules must be subject to control by an independent data protection authority.
	Sector-specific law on privacy of electronic communications	While Directive 95/46/EC sets forth the principles for the protection of personal data in general, Directive 2002/58/EC specifically regulates privacy in the sector of electronic communications as it applies to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks. <u>ECSP/ECNP</u> Directive 2002/58/EC applies to both ECSPs and ECNPs. As regards these actors, the Directive contains important rules such as confidentiality of communications, regulation of traffic and location data, additional security requirements, and rules

Section	Sub-section	
		concerning the use of cookies and spyware. Directive 2004/24/EC specifies the ECNP obligation to retain data for public security and Law enforcement purposes. Infrastructure products Article 14 of Directive 2002/58/ECc regulates „terminal equipment". According to this provision Member states may - where necessary - adopt measures which ensure that terminal equipment is compatible with the right of the users under the Directive. More recently, notably as regards the new threats linked with the development of RFID systems, the Article 29 Working Group has pointed out the necessity for terminal equipment producers to implement in the design of their systems the means to ensure the full respect of the privacy requirements by the companies who would like to use their systems. Service users Article 13 of Directive 2002/58 deals with the question of unsolicited communications. The idea is to provide safeguards for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, fax machines, emails or SMS messages.
	Regional or local laws on privacy of electronic communications	Given the nature of the European Union construction, Directives 95/46/EC and 2002/58/EC must be implemented by law in the 27 Member States. As a consequence, even if some differences occur between the national laws, a considerable general convergence can be observed. The Article 29 Working Party has played an important role in the harmonization of these laws.
	Effectiveness	Directive 95/46/EC a. awareness According to the results of a 2003 Euro barometer, on average, more than two-thirds of EU citizens (70%) tended to agree that awareness of personal data protection in their home country was low. Moreover, one-third of those polled (34%) did not know whether their national legislation could cope with the issue of personal information on the Internet. On average, only 32% of citizens of the EU had heard of the existence of rights of access, rectification and erasure. Finally it should be emphasized that the level of knowledge about the existence of a data protection authority was low since two-thirds (68%) of EU citizens were not aware of their existence. More recent results of 2007 tend to confirm that, on average, 60% of all EU citizens are concerned to a greater or lesser degree, about the issue of the protection of privacy. b. effectiveness As the results of the 2003 Euro barometer show, a clear major-

Section	*Sub-section*	
		ity of data controllers throughout the European Union rate the level of protection offered by their respective national data protection laws as 'medium'. When observing the different types of information that companies make available to data subjects, we can note that for none of the required information to be provided does a clear majority of respondents throughout the EU indicate making its availability to data subjects. A relative majority of respondents throughout the European Union (49%) indicate that their company received fewer than ten access requests during the year 2002. As for the complaints companies have received from people whose data is being currently processed, a huge majority of respondents in all of the Member States (96%) indicates that their company has not received any such complaints. Art. 29 W.G has taken different initiatives in order to increase the effectiveness of the Privacy legislation by launching different investigations in peculiar sector and by harmonizing throughout Europe, certain Data controllers' obligations. See also the declaration of this W.G. dated from the 25th of Nov 2004 about the enforcement of the DP Directive provisions and national legislation by the different national DPA. <u>Directive 2002/58/EC</u> No information yet about the effectiveness of this Directive.
Enforcement measures **Public Authority**		The Directives 95/46/EC and 2002/58/EC require both a data protection authority with appropriate powers to supervise the information privacy principles, and individual (no class action) rights of enforcement before judicial authorities (criminal but also commercial (through unfair competition) and civil jurisdictions) with certain facilities as regards the onus probandi and the taking into account of pure moral damages. The European enforcement mechanisms are therefore quite strong. In its „Strategy Document", adopted on 29 September 2004(WP 98), the Working Party stated that the promotion of harmonised compliance is a strategic and permanent goal of the Working Party. It also stated that it is convinced of the necessity of moving forward in the direction of promoting better compliance with data protection laws throughout the European Union and that, in this respect, it will make a joint effort to improve the situation.
Private Litigation		Article 22 of Directive 95/46 provides that an individual must have rights to seek a judicial remedy for any breach of the national law. Furthermore, the Directive provides for a right to recover compensatory damages (Art. 23). ADR or ODR systems even if their creation is encouraged by the European Commission and in certain cases are financed in the context of EU programme (see ECODIR and CCFORM) are still in their infancy. Till now it does not seem that any ADR has been in position to solve a litigation in the Privacy field.

Section	*Sub-section*	
Other extra-legal measures		
	Co / Self - Regulation	General position The 2003' Inter-institutional Agreement on Better Law-making contains the overall principle regarding alternative regulation mechanisms (Point 16), the limits of their use (Point 17) and precise definitions of what is meant by 'co-regulation' (Point 18) and 'self-regulation (Point 22). Self/co-regulation in the context of transborder data flows In the context of Transborder Data Flows (TBDF), self-regulation is considered by the Article 29 Working Party as a mean to ensure an adequate data protection (see the famous Working Paper number 12 issued by the Article 29 Working Group which has been taken as a reference by the Commission in its Safe Harbour decision and the opinions of the same Working Group as regards the appropriate guarantees offered by Contractual Clauses and Binding Corporate Rules. Codes of Conduct Article 27 of Directive 95/46/EC explicitly encourages the drawing up of codes of conduct intended to contribute to the proper implementation of the national provisions adopted by the Member States. This provision puts the accent on two types of codes: on one hand, national codes (new ones or the adaptation of existing ones) that can be submitted to the National data protection authority, and, on the other hand, Community Codes (new ones or the adaptation of existing ones) that can be submitted to the Article 29 Working Party. As regards the second type of code, it should be underlined that up to now, only two codes of conducts have been approved in this context: the FEDMA and the IATA codes. PETS The incorporation of Privacy Enhancing Technologies (PETs) into strategies for privacy receives some encouragement from Article 17 of Directive 95/46/EC, which requires data controllers to implement *„appropriate technical and organisational measures"* to protect personal data, especially in network transmissions. On 2 may 2007, the Commission has adopted a Communication with the purpose of identifying the benefits of PETs and laying down the Commission's objectives in this field, to be achieved by a number of specific actions supporting the development of PETs and their use by data controllers and consumers.
	Standards	The Article 29 Working Party has always followed with great interest the developments concerning standardisation in the data protection field. In its opinion 1/2002 „on the CEN/ISSS Report on Privacy Standardisation in Europe", the Working Party „takes note of the work undertaken by CEN/ISSS in the field of privacy standardisation. A technical Committee on „Se-

Section	Sub-section	
		curity and Privacy" has been created at the CEN level and first norms have been approved. In 2004, at the 26th International Conference of Privacy and personal data protection, held at Krakow, the final resolution emphasised the need for Data Protection Commissioners to work jointly with standardisation organisations to develop privacy related technical and organisational standards. Moreover, Article 14 of the Directive 2002/58/EC states that, where required, the Commission may adopt measures to ensure that terminal equipment is compatible with data protection rules. In other words, standardising terminal equipment is another, admittedly subsidiary way, of protecting personal data from the risks of unlawful processing, risks that have been created by the new technological options.
	Effectiveness	<u>General position</u> The Strategic review of better regulation in the European Union presented by the European Commission in November 2006 shows that real and substantial progress has been achieved regarding a better regulation and sets out plans for taking the process forward. It is however remarkable that the document does not mention progress regarding self- and co-regulation. The 'regulation' part of the 2003 Inter-institutional Agreement seems not to be part of the first high level priorities for making better regulation. The next steps are indeed oriented towards a simplification of legislation, reducing administrative burden, impact assessments, screening and withdrawal of pending proposals. <u>Self/co-regulation in the context of transborder data flows</u> The recent assessment of the adequacy of protection offered by the U.S. Safe Harbour provisions demonstrate that in the case of this self-regulatory system settled upon without a legal framework, the absence of the legitimacy (no source, for example, is identified as the publisher of this policy, it is for the data subject to check the protection offered) and of the conformity criteria (no minimum content principles) leads to difficulties. Secondly, even if the use of contractual clauses and binding corporate rules are being legally recognized as adequate self-regulatory instruments, these are still in the infancy and some barriers are still to be overcome (easier negotiation with the national DPAs, sharing best practices,…) . <u>Codes of conduct</u> In practical terms, the procedure foreseen for promoting European Codes of conduct, with approval from the Article 29 Working Group, has been rarely followed even though clearly encouraged by the European Commission. Up to now, only two codes of conduct have been approved in that context and, at national level, big disparities have been noticed. Thereby, some existent alternative regulation systems (e.g. trust-marks/labelling), though they can already help to enhance

Section	*Sub-section*	
		confidence in e-commerce, are still in their infancy. As regards trustmarks, clear distortions exist as regards the critical criteria they should fulfil to be actually effective. PETs As the results of a 2003 Euro barometer shows, the level of awareness of citizens as regards the use of PETs was low four years ago: 72% of EU citizens had never heard of these tools or technologies. The level of awareness of companies was not much better. Indeed, results showed that a clear majority, representing 66% of respondents in the European Union, do not use any such technologies or software products to enhance privacy protection of databases. However, since 2003, the level of awareness of the citizens as regards PETs is raising year after year. Indeed, according to the results of the 2007' „E-Communications household" survey, 81% of respondents had installed antivirus programs while 60% had antispam software in their computer.

United States

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	The U.S. Constitution does not contain an explicit right to privacy, though a „penumbra of rights" is interpreted to include protection for privacy that also covers electronic communications. These rights apply to protect the citizen from the government. Several state constitutions contain explicit protections for privacy that may apply to both government and private sector actors and may apply to telecommunications services. Narrowly drawn statutes protect privacy in electronic communications.
	Comprehensive law	Not applicable
	Sector-specific law on privacy of electronic communications	*ECSPs* Various statutes including the Electronic Communications Privacy Act and Telephone Records and Privacy Protection Act of 2006 seek to protect the confidentiality of the contents of electronic communications and information associated with the use of telecommunications services with respect to law enforcement and third parties. These statutes do not each address the full range of data protection principles. *ECNPs* Various statutes including the Telecommunications Act of 1996, the Electronic Communications Privacy Act, and the Computer Assistance for Law Enforcement Act regulate the confidentiality of electronic communications and the access to communications and traffic data by law enforcement and third parties. These statutes do not each address the full range of data protection principles. *Infrastructure Products* The Computer Assistance for Law Enforcement Act, though not addressed to product developers, requires that infrastructure products for electronic communications networks be technologically enabled for legally authorized monitoring of communications. *Service Users* Various statutes including CAN-SPAM and the Children's Online Privacy Protection Act Impose privacy obligations on users of telecommunications services.
	Regional or local laws on privacy of electronic communications	Laws at the state level exist to protection the confidentiality of telephone and electronic communications and to provide transparency of breaches of data security. According to the National Conference on State Legislatures, as of January 2007, 35 states have passed 'Security Breach Disclosure laws'.

Section	*Sub-section*	
	Effectiveness	*ECSP* Statutory rules offer clear protection for targeting activities by specific actors, but they do not provide comprehensive data privacy addressing issues such as data retention or data subject access and correction. *ECNP* Statutory rules offer clear protection for targeting activities by specific actors, but they do not provide comprehensive data privacy addressing issues such as data retention or data subject access and correction. *Infrastructure Products* Statutory rights generally do not impose any obligations on developers of infrastructure products *Service Users* Statutory rules seem ineffective in particular areas such as spam and data collection from children.
Enforcement measures Public Authority		*ECSPs* Statutes confer enforcement powers on federal and state authorities and provide penalties for violations. *ECNP* Statutes confer enforcement powers on federal and state authorities and provide penalties for violations. *Infrastructure Products* No specific enforcement measures are available against product manufacturers *Service Users* Statutes confer enforcement powers on federal and state authorities and provide penalties for violations. Public enforcement by any of the authorities faces a number of important obstacles. Industry representatives recognize that the work of government agencies is characterised by limited funding.
Private Litigation		Although there is a perceived ability to undertake private litigation the costs for private individuals act as a deterrent to doing so. ECNP Private rights of action exist against the illegal release of electronic and stored communications ECSP Private rights of action exist against service providers who illegally release electronic communications to law enforcement Infrastructure Products Explicit private rights of action against infrastructure product developers do not generally exist.

Section	*Sub-section*	
		Service Users Private rights of action exist against users of electronic communications services who use those services to illegally access protected communications and traffic data.
Other extra-legal measures		
	Co / Self - Regulation	The Better Business Bureau's OnLine Privacy programme (BBBOnLine Privacy program) was developed to support business websites in addressing key concern of online shoppers in respect to the use of their personal data. Currently 714 web sites are covered, and (depending on total annual sales) fees range from $200-7,000. The seal is available for companies based in the U.S., Canada and Japan, and is safe harbour certified. TRUSTe is an independent, non-profit organisation providing one of the foremost labelling schemes in evidence. TRUSTe certifies and monitors web site privacy and email policies, monitor practices, and resolves consumer privacy problems. Currently 2940 websites are participating. The fee for a TRUSTe seal varies between $599-25,000. It is available for English websites and companies in Japan.
		Amongst corporations, there is wide awareness and in representatives we interviewed, interest in Binding Corporate Rules (BCRs) and use of Inter-Company Agreements (ICAs) and the International Chamber of Commerce (ICC) standard contractual clauses for international data flows.
		There are a number of significant consumer groups active in this area. These include the Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF). The Privacy Rights Clearing House (PRCH) collects data on security breaches and identity theft and maintains a capability to receive direct complaints from concerned citizens.
		U.S. PIRG (Federation of State Public Interest Research Groups) runs awareness campaigns on privacy matters.
	Standards	Awareness of ISO 27001 is high but only in larger companies and perhaps only those that have to trade internationally (particularly with Europe). Even in larger companies not all of the organization will be accredited. Efforts to develop privacy-protective standards for web sites such as the Platform for Privacy Preferences (P3P) have been unsuccessful. Industry development tends to be slow and adoption is very limited.
	Effectiveness	Industry representatives commented that there is a vigorous personal protection landscape in the United States. The TRUSTe labelling scheme was seen to be the most effective, allowing the consumer to simply review the compliance of a site. Similarly the BBBOnline has been actively promoting its privacy seal under a general campaign of consumer awareness. Privacy experts and survey results, however, indicate a very different perspective. TRUSTe enforcement appears to be negligible. TRUSTe has only revoked its seal of approval in one instance.

Section	*Sub-section*	
		Awareness of and use of varying information security technologies was high. But recent surveys and the need for an FCC ruling on security for customer records indicates that deployment of encryption security is deficient. Anti-virus, firewall and access control technologies are the most widely deployed across the public and private sectors and many other technologies such as Intrusion Detection Systems, cryptography and spyware detection systems are also used. Difficult to implement or complex technologies such as Public Key Infrastructure or PETs were deployed less widely. Some companies, whilst at the forefront of the research into PETs had not yet deployed them internally which is a telling statement on the usefulness of these technologies. There is limited use reported of specific PETs like the Platform for Privacy Preferences (P3P) and there is ongoing research into certain technologies that have important privacy implications for example Radio Frequency Identification Tags (RFID)s, techniques to manage data mining in a privacy friendly way and also medical databases compatible with healthcare ethics. In general, the private sector sees a focus on Information Security measures where, although there is a lack of data, investment can be made with more 'certainty' than with regard to privacy measures. The appearance of the post of Chief Privacy Officer (CPO) in some major companies is increasing. In the public sector, the federal government is still progressing on the learning curve and the annual General Accounting Office (GAO) Information Security Report cards show slow improvement year on year. Industry has not, however, generally implemented data protection principles for the use of log data collected from electronic communications services.

Japan

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	Privacy is not defined as such in Japanese legal environment although historically a number of court decisions have been made in order to protect the nature of privacy. Privacy as a self-determination right is construed by a number of articles in the Constitution of Japan, such as Articles 13, 19, 21 (2), 23, 31, 33, 35 and 38 (1). This aspect of privacy is not restricted to the privacy of information. However, there is no statutory provision of privacy in Japan, and currently no rule-making is in order to legislate privacy.
	Comprehensive law	The overall framework for the protection of personal information is set forth by the Act on the Protection of Personal Information (Act No. 57 of 2003). The Act, which took effect in April 2005, outlines the principle and objectives for the protection of personal information and how personal information should be protected in the private sector. The Act holds the principle of 'protection' and 'use' of personal information, mentioning that personal information should be handled in a cautious and appropriate manner with respect to individuals' personal information. The law imposes legal obligations for the protection of personal information on businesses which fall under certain criteria. The Act is accompanied by two other acts which regulate the protection of personal information in public administrations and incorporated administrative agencies (quasi-government agencies).
	Sector-specific law on privacy of electronic communications	Privacy and personal information protection in telecommunications are subject to general regulation by the Act on the Protection of Personal Information. It is also subject to regulation by the Telecommunications Business Act and ministerial guidelines (Guidelines on the Protection of Personal Information in Telecommunication Business). Telecommunications carriers are also requested by the Equipment Rules to install necessary technical measures to ensure the secrecy of communications is protected. Unsolicited commercial email is regulated by the Act on Specified Commercial Transactions and the Act on Regulation of Transmission of Specified Electronic Mail. Unsolicited phone call and facsimile transmission are not regulated by law, but automated calls may violate the service contract by telecommunications carriers. The Telecommunications Business Act has provisions on telecommunication carriers' obligation to protect subscribers' information. The Act also requires telecommunication carriers to install necessary equipment and measures to fulfil the obligation. Measures in the Act place great obligations on Telecommunications carriers to protect personal data than the general law on other sectors.

Section	*Sub-section*	
	Regional or local laws on privacy of electronic communications	There have been a number of efforts to regulate the electronic storage of personal information at the prefectural and municipal level in accordance with the state regulation. However, electronic communications is in the jurisdiction of the Ministry of Internal Affairs and Communications, and there is no prefectural and municipal regulation on privacy of electronic communications.
	Effectiveness	In general, legislation on personal information protection has worked out well in Japan. An opinion poll conducted by the Cabinet Office in September 2006 showed 80 percent of the respondents knew about the Act on the Protection of Personal Information, and that three-quarters of them considered public awareness and concern over personal data protection increasing. The polls also showed 70 percent of those who knew about the Act consider private and public entities have made progress in the protection of personal information. On the business side, another Cabinet Office-led survey on entities who handle personal information showed more than half of these entities have clarified who should be responsible for handling personal information and published a privacy policy. Serious information breaches occurred prior to the implementation of the Act on the Protection of Personal Information and still are occurring. As public awareness on personal information protection increases, and the Act on the Protection of Personal Information calling for voluntary disclosure of any data breaches, businesses now tend to disclose cases of information breaches immediately to avoid reputation risk.
Enforcement measures **Public Authority**		Although Japan's personal information protection regime assumes private entities will take primary efforts to protect personal information, the government has several enforcement measures to be used as the last resort when private efforts fail. When complaints concerning personal information protection are not settled between the concerned parties, the Minister who oversees the business area (also known as „Competent Minister") may require the company to report on the case, the Minister may then issue a notice of advice, make a recommendation or order depending on the seriousness of the case. Failure to provide a required report or to comply with the minister's order may result in criminal offences. The former may result in a fine up to 300,000 yen, and the latter may result in either imprisonment for up to six months or a fine up to 300,000 yen.
Private Litigation		Inquiries and complaints from citizens or consumers concerning personal information protection should primarily be dealt with the entity handling personal information, or one of the Authorized Personal Information Protection Organizations. However, when inquires and complaints are not settled at this level they can be brought to the Competent Minister who oversees the entity and take a necessary action. Little case law has been established in the area of personal information protection in Japan. However, businesses are starting to consider the mismanagement of personal information as both a financial risk and reputation risk. Companies that

Section	*Sub-section*	
		have experienced disclosures of personal information under their control may end up compensating for the possible damage with payments between 500 to a few thousand yen per person on a voluntary and pre-emptive basis. In one of the largest cases of personal information disclosure, Softbank, the third largest telecommunication carrier, leaked personal information of 4.5 million subscribers, which resulted in compensation of approximately 4 billion yen.
Other extra-legal measures		
	Co / Self - Regulation	Self-regulatory arrangements for the protection of personal information can be found in two streams. One is the self-regulatory framework set forth by the Act for the Protection of Personal Information. In the light of the objectives of the Act, protection of personal information should be pursued at the initiative of businesses and other entities handling personal information. In principle, the Act does not dictate how personal information should be protected and lets each player take necessary actions. Once the government has formulated the regulatory environment and provided necessary assistance to establish the system, industry self-regulation works out the details. In this stream of self-regulation, in addition to efforts by entities handling personal information, „Authorized Personal Information Protection Organizations“ also have a role to play. Authorized Personal Information Protection Organizations are an entity or group of entities which intend to ensure the proper handling of personal information in a particular industry sector, sub-sector or geographic region. They form voluntarily to perform duties handing complaints about the handling of personal information and to help resolve disputes following provisions of the Act on the Protection of Personal Information. They are authorized in this function by the Competent Minister. Private and semi-private labelling programmes have also been developed. Major programs include the Privacy Mark administered by the Japan Information Processing Development Corporation (JIPDEC) and TRUSTe. In addition, there are industry-specific programs such as Japan Accreditation Council for Healthcare Information (JACHI) and Campaign Privacy.
	Standards	Japan Industrial Standard (JIS) Q 15001:2006 defines the requirements for management systems for personal information protection. JIS Q 15001 outlines the processes that an organization should follow in protecting the personal information. It also requires that personal information protection should be conducted on a Plan-Do-Check-Act cycle, thus ensuring personal information protection is not a one-off activity.

Section	*Sub-section*	
	Effectiveness	As of 31 May 2007, a total of 34 organization in various sub-sectors such finance, health, telecommunications, and other smaller industry segments have been authorized as Authorized Personal Information Protection Organizations. Statistics from the Cabinet Office suggest they are active in handling personal information-related claims between consumers and businesses although the total number of claims filed with the Authorized Personal Information Protection Organizations are still relatively small. The effectiveness of privacy labelling in Japan is yet to be seen, because many Japanese companies began to formalize their efforts to protect personal data only after the Act on the Protection of Personal Information Protection took effect. A sharp rise in the number of companies participating in labelling schemes can be observed in FY2005: 553 new accreditations in 2005, 2,395 in 2006 and 2,283 new accreditations in 2007.

South Korea

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	The constitution provides an explicit right to privacy and South Korea is a signatory to the Universal Declaration of Human Rights, and of the International Covenant on Civil and Political Rights. These rights have often been denied in the name of national security. Under the National Human Rights Commission Act 2001, the National Human Rights Commission (NHRC) has competence to investigate and recommend action on any violation of Human Rights guaranteed by the constitution or international agreements entered into and ratified by the nation by any state agencies, local governments or detention or protective facilities. The commission's authority includes violations of the right to privacy, but only by public sector entities. Privacy law has been extended through recent recognition by the courts of a „right to publicity" which allows individuals to control commercial use of their identity.
	Comprehensive law	There is no comprehensive law protecting privacy[312]. The Act on the Protection of Personal Information Maintained by Public Agencies 1996 (enacted 1998) secures personal information held by public agencies and gives allows citizens rights to control that information.
	Sector-specific law on privacy of electronic communications	ECSP/ECNP The Act on Promotion of Information and Communications Network Utilization and Information Protection is the main legislation protecting of privacy in electronic communications, the Act's provisions apply to both ECSP and ECNP. The act has the purpose of both promoting the use of information and communication networks and protecting user's personal information when they use information and communication services. It is the companion sectoral act to the Act on the Protection of Personal Information Maintained by Public Agencies which secures personal information held by public agencies. The act embodies the OECD's eight privacy principles as the basis of policy approach to privacy protection. However the act is notable in that one of its primary purposes is the promotion of the information and communications sector, it is sector specific industrial policy more than policy for the protection of the right to privacy in electronic communications. But there are strong protections for the rights of juveniles. The Protection of Communications Secrets Act protects secrecy of communications and promotes freedom of communications. Administered by the Ministry of Information and Communications, the Act covers all communications under the Ministry's remit: postal mail services and all electronic communica-

312 New legislation addressing privacy protection for the private sector broadly is currently before the National Assembly. Three drafts are under consideration, each suggests different measures and degrees of protection, but all propose that the protection of privacy should become the responsibility of the Prime Minister's office, rather than industry specific ministries.

Section	*Sub-section*	
		tions, including Internet. The Act also describes broad arrangements under which communications can be monitored or intercepted.
	Regional or local laws on privacy of electronic communications	N/A (question not asked)
	Effectiveness	General comment from respondents from all sectors was that an omnibus data protection law was necessary and the current sectoral and industry-policy approach was not as effective as it should be. General lack of awareness of privacy was beginning to change, current legislation was inadequate. Particularly the potential for very significant abuse from extremely widespread use of the national ID number in many forms of online transaction should be addressed.
Enforcement measures **Public Authority**		The Korea Information Security Agency (KISA), operating as an agency of the Ministry of Information and Communications, has the duty to implement measures under the Act on Promotion of Information and Communications Network Utilization and Information Protection. KISA is also responsible for oversight of the Personal Information Dispute Mediation Committee (PICO) and related self-regulatory activities. KISA's role is somewhat equivalent to that of a data protection commissioner, but it is not independent of government, does not have full powers of investigation and enforcement, and only serves the information and communication sector. Ministry of Information and Communications administers the Protection of Communications Secrets Act, the Minister of Government Administration and Home Affairs administers the Act on the Protection of Personal Information Maintained by Public Agencies. Personal Information Dispute Mediation Committee (PICO), operated by KISA has been promoted as an industry self-regulatory measure, however given KISA's oversight and responsibility for PICO, it is better described as legislative action. PICO was created to protect personal information in the private sector and handle complaints regarding the infringement of personal information under the Act on Promotion and Communication Network Utilization and Information Protection. It monitors compliance with the information protection provisions of the Act and receives complaints from users. The dispute resolution system functions either online or offline. PICO investigates the facts of a complaint and advises corrections in the case of minor violations. Any person may file an application for the mediation of a personal information dispute involving a communication service providers, or any dispute involving personal information processes by a travel agency, airline carrier, department or discount store, hotel, or educational institution. As such PICO's influence extends to some in the ESCP sector. MIC also issues guidelines on a range of issue effecting privacy and security, the most influential being guidelines on

Section	*Sub-section*	
		technical and management protection of personal data. This guideline provides guidance mainly on standards for monitoring and protecting network operations.
Private Litigation		N/A
Other extra-legal measures		
	Co / Self - Regulation	Trustmarks: the „i-Safe“ security mark and „e-Privacy“ privacy mark, administered and implemented by the Korea Association of Information & Telecommunication (KAIT) are awarded to sites that meet a set of criteria for implementation of security standards and policies and the protection of consumer privacy. The marks are administered by a committee made up of members from MIC, Fair Trade Commission, Consumer Protection Board, lawyers and academic experts. The e-Privacy mark is designed to guarantee privacy protection, the i-Safe mark has two types: the first, guarantees privacy protection, system security, and safety for online shopping, the second guarantees privacy protection, system security, and consumer safety for online financial and medical services.
	Standards	ECSP and ECNP: In March 2005 „RFID Privacy Protection Guideline“ was published by the Telecommunications Technology Association as an industry standard. The standard does not carry the authority of enacted legislation, but has been adopted by the Korean telecommunications sector. The standard places limitations on the writing of personal information on RFIDs and the type of information that may be collected. Consumers should be notified when an RFID tag is attached to an object, they should be informed of the features and function of the RFID tag, and what information is recorded by the RFID tag. Mechanisms to stop the RFID functioning if used by the public should be provided. The standard also requires notification is made when RFID readers have been installed.
	Effectiveness (of legislation – NOTE PICO and mention of MIC guidelines have moved sections)	PICO was cited by many respondents as being effective as a mechanism for handling complaints, and later in its mediation and dispute resolution role. KAIT’s trustmark system is rigorous and well administered, but take-up among online providers is very low, less than 190 certified companies as of February 2007, compared to the large and vibrant online service market in Korea. MIC guidelines were commented on by respondents from ESCP and ESNP sectors as being appropriate and that MIC was responsive to industry requests for modifications and improvements to the guidelines. The RFID standard is addressing a new area where there is little commercial deployment, too early to tell if it will be effective, or if powers offered by legislation will be required.

Malaysia

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	Malaysia has no explicit constitutional right to privacy. Article 10 of the Constitution of Malaysia recognizes the right to freedom of speech and expression, peaceable assembly and association, however these rights are subject to qualifying clauses in the same article giving government the power to restrict them in the interest of security of the nation. In 2001, a Malaysian civil court ruled there was no constitutional protection of privacy, and in addition that Malaysian common law should be based on the English common law prior to 1957 (Malaysian independence) and English law before 1957 had not recognized the infringement of privacy as a form of tort.
	Comprehensive law	There is no comprehensive privacy or data protection law. A comprehensive data protection act was proposed as a one of a new batch of „cyberlaws“ drawn-up in the mid-1990s intended to bring Malaysia's legal system up to date wrt Internet and online issues. However the data protection bill has remained in draft form and has not yet been brought before parliament.
	Sector-specific law on privacy of electronic communications	Overseen by the Ministry of Energy, Water and Communications, the Communications and Multimedia Act 1998, regulates the converging communications and multimedia industries: telecommunications, broadcasting and computing. The act attempts to encourage competition and reduce regulation through the adoption and promotion of industry codes of practice and self-regulation. As well as providing a legal framework for these multimedia industries the act also has a strong industrial policy role in promoting Malaysia as global hub for communications, multimedia and content services. The act has no direct provisions regarding privacy and trust but contains a number of sections related to privacy of communications. Under the act the interception and disclosure of communications is prohibited. „Communications“ refers to all Internet based communications, from an e-commerce transaction to e-mail. Network service providers have some obligations under the act to maintain the privacy and integrity of customer data. The act also grants law enforcement agencies powers to conduct searches of computer equipment, and the power to intercept or listen to communication transmitted or received by any communications without a warrant if the prosecutor believes the communications is likely to contain any information relevant to any investigation into an offence under the Act. The Digital Signature Act imposes an obligation of secrecy on any one who gains access to confidential information under the act. The Telemedicine act extends all existing medical confidentiality provisions to online medical practice, with specific provisions relating to the dissemination of patient information with-

Section	*Sub-section*	
		out their consent. The Banking and Financial Institutions Act (BAFIA) provides the financial and banking industry with by far the strongest protection of privacy and confidentiality of information of any sector. The provisions are with respect to information relating to transactions in this sector, not electronic information more broadly.
	Regional or local laws on privacy of electronic communications	N/A
	Effectiveness	Very limited effectiveness in terms of protection of privacy and data protection. People interviewed were generally of the opinion that the Malaysian ICT industry and ICT users did not find privacy a major concern. Users tend to lack awareness of their rights and are trusting of service providers. A comment „People not yet aware of privacy as an issue“ captures the situation. Non-profit advocacy organizations focus on fundamental rights to free speech rather than privacy. Service and network providers are beginning to be aware that the protection of privacy is valuable to the company, particularly in terms of reputation in the marketplace. There was a general sense from all respondents that improved data protection is now necessary as Malaysia's Internet and e-commerce sector continues to grow.
Enforcement measures **Public Authority**		The Ministry of Energy, Water and Communications has broad powers over communications providers under the Communications and Multimedia Act, questionnaire respondents often mentioning the potential for suspension of cancellation of operating licenses, for example if they failed to maintain privacy or integrity of their customer's data, or if that data was disclosed. Under the act a fine and/or prison sentence may be imposed for interception, inappropriate disclosure or use of information obtained though the interception of communications. Contravention of the Telemedicine Act through the disclosure of any image or information is punishable by a fine or possible imprisonment. The Banking and Financial Institutions Act addresses violations of privacy and confidentiality more directly and aggressively than any other piece of legislation: the disclosure of confidential information can lead to subject to fines of up to 3 million ringgit or to imprisonment for a term not exceeding five years.

Section	*Sub-section*	
Private Litigation		Under the General Consumer Code, if the complainant did not receive satisfaction from the Consumer Forum or Ministry then a civil suit could be brought for violation of privacy, loss of confidentiality etc. However, to date no such action has been brought, and if a case were brought it would be a lengthy process.
Other extra-legal measures		
	Co / Self - Regulation	Communications and Multimedia Act was intended to support a self-regulatory regime and encourages the adoption and promotion of industry codes of practice. The regime is administered by the Communications and Multimedia Consumer Forum of Malaysia, and established as a requirement of Communications and Multimedia Act. The Forum is responsible to the Malaysian Communications & Multimedia Commission. Membership of the forum is drawn from the communications sector broadly and these industry members are independent of the Commission, however they do report progress of the forum to the Commission and the forum's stated role is to promote the national policy objectives pursuant with the Communications and Multimedia Act 1998. The Forum developed the „General Consumer Code of Practice for the Communications and Multimedia Industry Malaysia", registered in October 2003. The protection of consumer information is one of eight objectives of the code requiring Service Providers to adopt and implement a „protection of consumer information policy" to protect the privacy of identifiable information. Compliance with the code is a requirement for all companies licensed to operate under the Communications and Multimedia Act. The code includes a section on „notice and disclosure" which requires the service provider to provide details about what information is being collected, how it will be used, any distribution to third parties, any choices that may be available to the individual regarding collection of their information, a statement of the organization's commitment to data security, and steps taken by the organization to ensure data quality and access. These policies on the protection of consumer information should be made available in the most accessible, easy to read and understood manner and should be disclosed each time individually identifiable information is collected.
	Standards	
	Effectiveness	Provisions of the General Consumer Code regarding the protection of consumer information are not being widely observed, very few websites carry privacy statements with the information the code requires. Notice and disclosure statements are often lacking. Only a small number of service providers meet the requirements of the code rules and principles. Industry representatives interviewed in the course of our research commented they were aware of the codes and some had participated in the forum that oversaw and developed them. However, none were able to mention specific instances when codes were directly considered in relation to privacy.

Section	*Sub-section*	
		They could only assume a code may apply to issues concerning the protection of privacy. Compliance with the voluntary code is not mandatory under the Act.

India

Section	*Sub-section*	
Laws and Regulation		
	Statutory or constitutional right to privacy	No explicit right to privacy but jurisdiction has developed case law deducing the right to privacy from other fundamental laws – especially the Constitution The Right to Information Act 2005 (Act No. 22) has introduced right for citizens to secure access to information controlled by public authorities, including access to information held about the citizen himself.
	Comprehensive law	No comprehensive law. Protection of personal data mainly achieved by contractual law. There are several laws that regulate aspects such as the ICT Act 2000, that deals with aspects of confidentiality of electronic communication. Certain sectors are regulated (e.g. public financial institutions and credit information companies) e.g. Credit Information Companies (Regulation) Act 2005 governing the activities of credit information companies incorporates certain data protection provisions including the requirement of accuracy, regular up-date, security, purpose limitation, right to access and to rectification etc. (scope very limited, no specific monitoring authority); also Public Financial Institutions Act 1993. Privacy breaches can be dealt with under civil, administrative and criminal law (e.g. Indian Penal Code, Contract Act, IT Act).
	Sector-specific law on privacy of electronic communications	ECSP/ECNP The current IT Act provides sanctions in case of confidentiality breaches in respect to data. Amendments in Parliament in 2007 may specify technological and organisational measures required to safeguard security of services and networks. These amendments foresee that „reasonable security practices and procedures" may be specified in the agreements between the parties by law, or may be prescribed by the Government in consultation with professional bodies or associations (the recently established Data Security Council could be recognised as such a body). The government has also secondary powers to impose data retention requirements (these powers are more flexible than the European Directive). Private arrangements between companies and government deal with data retention: Individual Privacy Act governs automated calling systems without human intervention. Infrastructure Products – no information available Service Users – no information available.
	Regional or local laws on privacy of electronic communications	There are initiatives in Kerala and Andhra Pradesh to develop state privacy laws. Central government does not see real effectiveness for multinationals without national legal framework.

Section	*Sub-section*	
	Effectiveness	Some known instances of litigation, recently a consumer court has fined Airtel, India's largest mobile company Rs 7.5m (about 50,000€) for intrusion of privacy of mobile users.
Enforcement measures **Public Authority**		There is no Data Protection oversight body in India. Acts establish specific bodies that deal with aspects of data protection e.g. Consumer Protection and National Consumer Disputes Redress Commission (according to interviewees this general body is not effective for individual privacy breaches). There is no requirement to notify any authorities of security breaches. Central Information Commission dealing with the Right to Information Act 2005 in respect to the citizen's right to access to information held by the public administration (including information on themselves). Consumer Advocacy interviewee mentioned problems with enforcement of the Right to Information Act. Authorities established by the IT Act competent in arbitration and adjudication of settlements of civil disputes under the act. The government and parliament in 2000 and 2007 rejected an Information Commission as too bureaucratic for India – and unnecessary in view of limited consumer demand for privacy protection as compared with other more basic human rights.
Private Litigation		ECSPs Data protection is in general governed by an individual contract or a Service Level Agreement with the client. Based on the contract BPOs may have to apply the client's national law (mostly US or EU), apply specific standards (e.g. ISO 27001), and even report privacy breaches to their client (contractual compliance with California 1357 breach notification law). Consequently breaches of data protection are normally dealt with under civil law, but remedies for privacy breaches may also be found in administrative and criminal law (e.g. Indian Penal Code, IT Act). Audits such as SAS 70 or to standards such as ISO 27001 can be required by contractual arrangement between companies based in Europe or North America and BPO providers. Furthermore, audits by companies' internal audit teams can also ensure data security. IT staff are authorised by the National Skills Registry that collects and checks credentials and – upon individual agreement – provides this information to potential employers.
Other extra-legal measures		
	Co / Self - Regulation	ECNPs Call register for mobile telephony telemarketing (supported by the Indian Banks Association and Indian Cards Council) requires banks to establish a DNC register, these are to be consolidated. The Telecom Regulatory Authority of India (TRAI) has initiated a consultative process for regulating unsolicited calls.

Section	*Sub-section*	
		ECSPs Under the aegis of NASSCOM: 1) Data Security Council of India: aims at developing the best practices into a code of conduct, and introducing a kind of accreditation/label proving compliance with these best practices, which might also require the audits. Also education shall be promoted and NASSCOM aims at establishing local security fora of Chief Information Security Officers in cities with a large number of companies. 2) National Skills Registry initiative for individual vetting that checks the credentials of BPO staff by collecting demographic information, details of academic qualification etc. Management of this information is done on a contractual basis between the IT professional who is a member of the Registry and the company operating the system. 3) '4E Framework for Trusted Sourcing' includes the responsibility to report to its members on legislation affecting the industry. 4) NASSCOM members perform staff training and information about data protection as part of their security awareness training and data protection best practices. The Reserve Bank of India (Banking), Telecom Regulatory Authority of India (Telecom) and Securities Exchange Board of India (for securities trading) have issued guidance regarding privacy and trust for electronic communication.
		Marketing associations – see NASSCOM above
		Consumer associations – very under-represented in India – view that company-based 'Do Not Call' registries need to be replaced by national registry, and that effectiveness of sanctions is less with very small (easily dissolved) and very large (easily defended) companies than the mid-sized.
		Vendors – NA
	Standards	Data Security Council intended to drive the evolution of best practices into a code of conduct, for standards that foreign customers of BPOs expect and require.
	Effectiveness	Privacy awareness is very low in India, the concept in the way perceived by Western countries is mainly introduced by customer requirements, which are growing with penetration of mobile and fixed Internet (note that broadband penetration at roughly 3 million lines in a population of 1.3 billion is very low by international standards). Domestic data protection is seen to be separate from BPO as foreign customers drive the developments of data protection. The system is very reactive. Interviewees reported that there are few complaints or requests dealing with privacy issues. Privacy concerns – if they exist at all - are more in the area of the customer company. Awareness of foreign data protection regulation and standards as companies are required to adhere to them based on contractual obli-

Section	*Sub-section*	
		gations. Industry's own perception of the effectiveness of contractual data protection requirements is very good. Widely publicized cases such as HSBC, Bank of America and Citibank/ Infosys show that the contractual effectiveness for data protection requirements can be weak. Companies deploy a wide variety of the most popular information security products, including firewalls, antivirus, intrusion detection technologies and access control systems; however, there is no data regarding the effectiveness of these measures. Additionally, in personnel vetting NASSCOM has introduced the National Skills Registry initiative, with over 100,000 registered individuals. CERT-IN is to publish the results of an information security survey of its members indicating their views on the effectiveness of technical measures to enhance privacy and trust. NASSCOM also expected to publish survey of its members.

Annex 3: Glossary of Terms

A - B

BCR (Binding Corporate Rules) Binding Corporate Rules provide an alternative to the Save Harbour regime by take the concept of model contracts forward and allowing multinational companies to transfer data outside the EEA. An 'entry point data protection authority' is assigned to assess the rules against the requirements of the EU Directive and approve them. Once approved the same data protection authority is responsible for requesting approval from each regulator where the company operates.

BBBOnline (Better Business Bureau's OnLine Privacy): a privacy seal for web sites issued by the Better Business Bureau.

BPO (Business Process Outsourcing): is contracting of a specific business task (e.g. payroll, billing) to an external service provider.

B2B (Business to Business): services provided by one business to another business.

B2C (Business to Consumer): services provided by a business to the customer.

C

CALEA (Computer Assistance for Law Enforcement Act): a U.S. law which requires electronic communications services and infrastructure products to be technologically enabled for legally authorized monitoring of communications.

CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) :the U.S. law which seeks to reduce spam, 15 U.S.C. §§ 7701, et. seq.

CNPI (Customer proprietary network information): information about telecommunications network customers that is defined by U.S. law.

COPPA (Children's Online Privacy Protection Act): a U.S. law that requires parental consent to collect personal information from children over the internet.

D

DMA (The Direct Marketing Association): global trade association of business and non-profit organizations using and supporting direct marketing tools and techniques.

DMCA (Digital Millennium Copyright Act): U.S. law that strengthens copyright law by, *inter alia*, making it illegal to circumvent TPM. (17 U.S.C. §1201).

DRM (Digital Rights Management), see also TPM: measures used by copyright owners and publishers to control access and use of their digital data (e.g. encryption or digital watermarks).

DSL (Digital Subscriber Line): technologies providing digital data transmission over the local telephone network.

E

ECPA (Electronic Communications Privacy Act): U.S. law that protects the privacy of electronic and stored electronic communications.

ECSP (Electronic Communications Service Provider): a provider of electronic communications service (ECS). An ECS is a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks. (*Framework Directive*, Article 2).

ECNP (Electronic Communications Network Provider): a provider of an Electronic Communications Network (ECN). An ECN is a transmission system and, where applicable, switching or routing equipment and other resources which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed. (*Framework Directive*, Article 2).

EEA (European Economic Area): area established by an agreement between the European Union and the EFTA (European Free Trade Association) providing for the participation of the EFTA countries in the European Single Market.

EFF (The Electronic Frontier Foundation): non-profit organization focusing at defending individual's rights in relation to the use of communication technologies.

EPIC (Electronic Privacy Information Center): EPIC is a public interest research centre in Washington, D.C. The focus of EPIC is drawing public awareness to emerging civil liberties issues, privacy protection protect privacy, the First Amendment, and constitutional values.

F

FBI (Federal Bureau of Investigation): the U.S. federal law enforcement agency.

FCC (Federal Communications Commission): the U.S. regulatory authority for telecommunications

FTC (Federal Trade Commission): the U.S. regulatory authority charged with consumer protection and anti-trust enforcement.

G - I

ICA (Inter Company Agreements): agreements based on standard contractual clauses from the International Chamber of Commerce (ICC) signalling the adoption of adequate measures guaranteeing data protection for data transferred outside of Europe. These agreements are signed by entities in the organisation and indicate which systems are transferring data outside of Europe and how this data is dealt with and managed.

ICT (information and communication systems): technologies designed to support the exchange and management of information.

ISP (Internet Service Provider) A firm which enables other organizations to connect to the global internet.

J - K

KISA (Korea Information Security Agency): operating as an agency of the Ministry of Information and Communications, with the duty to implement measures necessary to protect information and for the secure distribution information.

L - N

NSL (National Security Letters): a letter issued by U.S. Government Agencies (in particular the United States Federal Bureau of Investigation) demanding an organisation to turn over data pertaining to individuals.

O - P

Patriot Act, see USA PATRIOT Act.

PETs (Privacy enhancing technologies) Technologies which enable information and communication systems to minimise the collection and use of; hinder any unlawful use; and prevent the possible destruction, alteration or disclosure personal data.

PICO (Personal Information Dispute Mediation Committee): committee operated by KISA (Korea Information Security Agency). PICO was created to protect personal infor-

mation in the private sector and handle complaints regarding the infringement of personal information under the Act on Promotion and Communication Network Utilization and Information Protection.

Privacy: the right of the individual to determine his own destiny without hindrance, especially from government.

P3P (Platform for Privacy Preferences): protocol developed by the World Web Consortium to give users more control on the use of their personal information allow websites to declare their intended use of information they collect about browsing users. Designed to give users more control of their personal information when browsing, P3P was developed by the World Wide Web Consortium (W3C) and officially recommended on April 16, 2002.

Q - S

Security The protection against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and against all other forms of unlawful processing of data.

spam (Single Post Addressed to Multiple lists): unsolicited email sent indiscriminately and in bulk.

SPI (Sensitive Personal Information)

S/W (Software) The set of ordered instructions which enables a computer to perform specific tasks.

T

TBDF (Transborder Data Flows)

TPM (Technical Protection Measures), see also DRM.

TRPPA (Telephone Records and Privacy Protection Act): a U.S. law that protects against impersonation to obtain telephone records.

Trust is the perceived security of the networked environment.

TRUSTe: an independent, non-profit organisation enabling trust based on privacy for personal information on the internet.

U - Z

USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001): the U.S. law intended to help law enforcement agencies pursue terrorism suspects by lowering the thresholds for

obtaining legal access to electronic communications to search the records of individuals purportedly involved in terrorist or other clandestine intelligence activities, Pub. L. No. 107-56.