Unclassified **DSTI/ICCP/REG(2002)5/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

12-Feb-2003

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2002)5/FINAL
Unclassified

Cancels & replaces the same document of 21 January 2003

Working Party on Information Security and Privacy

REPORT ON COMPLIANCE WITH, AND ENFORCEMENT OF, PRIVACY PROTECTION ONLINE

JT00139173

English - Or. English

PREFACE

This report presents and analyses enforcement mechanisms that are available in OECD member countries both to address non-compliance with privacy principles and policies and to ensure access to redress. It is intended to form the basis for assessing the practical application of available compliance and enforcement instruments in a networked environment and their ability to meet the objectives of the OECD Privacy Guidelines, including effectiveness and coverage across jurisdictions.

The report was prepared, based on contributions received from OECD member countries, by Chris Kuner, a consultant to the OECD, under the supervision of the secretariat. Chris Kuner is a partner in the law firm Hunton & Williams.

TABLE OF CONTENTS

INTRODUCTION

Privacy compliance and enforcement are different topics, but are interrelated. They are different, since compliance refers to the level of adherence to legal requirements, while enforcement refers to the mechanisms which can be used to compel such adherence and to protect the rights of data subjects when violations occur. At the same time, the two are closely interrelated, since the higher the level of compliance, the less need there is for enforcement, and a strong level of enforcement may motivate actors to adopt a higher level of compliance. This report recognises the close interrelationship between these two topics, and thus deals with compliance and enforcement together, while still recognising the potential distinctions between them.

Background

On March 12, 2002, a Questionnaire on Compliance with and Enforcement of Privacy Protection in the Context of Business-to-Consumer Electronic Commerce was sent to OECD governments and private sector participants. It was developed as part of the work programme of the ICCP Working Party on Information Security and Privacy (WPISP) to fulfil the objectives of the OECD *Ministerial Declaration on the Protection of Privacy on Global Networks* issued at the OECD Ministerial Conference in Ottawa, Canada in October 1998. Responses were received from 20 member countries and three private organisations.

In the Declaration, Ministers declared that they will take steps to ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress. Moreover, the Declaration calls on the OECD "to promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks."

Compliance and enforcement have become central issues in privacy protection since the OECD Ministerial Conference was held. Considering the limitations of purely legalistic and regulatory approaches, both governments and the private sector have been developing alternative methods of compliance and enforcement which make use of self-regulation, market incentives, technological means, and other mechanisms which go beyond traditional regulatory approaches, and which can better cope with the borderless and fast-moving nature of electronic commerce. It was thus the appropriate time to take stock of compliance and enforcement mechanisms used in the OECD member countries and analyse whether they cope adequately with the requirements of electronic commerce.

Respondents were requested to provide basic information rather than detailed analysis. Governments were requested to answer the questions with regard to any "legal provisions", meaning any domestic laws or regulations, including court decisions (case law), or conventions, treaties or other international legal instruments. Information was solicited both about governmental agencies (such as a government ministry) and independent privacy regulators (such as a data protection authority); in this report, the term "government agency" refers to both types of entities.

Input was also solicited from the private sector, since the private sector can provide practical experience, highlighting the process it undertakes when implementing privacy safeguards. Thus, private sector participants were requested, in addition to providing information on legal provisions they are familiar with as described above, also to provide information on any self-regulatory solutions which they are aware of, such as trustmarks, seal programmes, the use of corporate privacy officers, private sector enforcement programmes, and the like, as described further in the questionnaire. This report gives a high-level overview of the subject. It is based on the responses received and is non-judgemental.

SUMMARY OF RESPONSES

Responses were received from the following OECD member countries and private sector entities: Australia, Austria, Belgium, Czech Republic, Finland, France, Germany, Italy, Japan, Korea, Mexico, Norway, the Netherlands, the Slovak Republic, Sweden, Switzerland, Turkey, United Kingdom, United States, Internet service providers (ISPs) from the Slovak Republic, US Council for International Business (USCIB) and the US Direct Marketing Association (DMA).

Norms and instruments

Privacy framework

Among the countries with omnibus privacy legislation are Australia, Austria, Belgium, the Czech Republic, Finland, France, Germany, Italy, Korea, Norway, the Slovak Republic, Sweden, Switzerland, and the United Kingdom. Countries without a single omnibus law include Japan, Mexico, Turkey, and the United States. Legislation is currently being considered in Japan and Turkey. Some countries have sector-specific laws as well. For instance, many European Union (EU) member States have sectoral legislation regarding telecommunications privacy, and Finland has laws on telecommunications, openness in government activities, employment privacy, police data files, and criminal records. The United States has laws that address privacy protection concerning various sectors, such as the privacy of children's information, and financial and medical information. Germany has specific acts relating to online services. Most respondents also have additional forms of legal regulation, such as decrees, ordinances, administrative rules, and case law (for instance, France, Germany, Italy, Sweden, and Switzerland have ordinances or decrees). Case law plays a differing role in various member countries: for example, in the United States it is a major source of law, while French law does not regard it as an independent source of law. In Japan there are various self-regulatory guidelines in place, while in the United Kingdom human rights legislation is of particular relevance. Administrative rules and regulations play an important role in the United States.

International and regional instruments

The member countries of the EU are all bound by the Data Protection Directive,[1] and the various public law agreements and instruments which the European Commission has entered into (such as the Safe Harbour arrangement,[2] and the model contracts for data transfer[3]). Some European countries are also

1. Directive 95/46/EC of the European Parliament and of the Council of October 24 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, (1995) OJ L281 31.

2. Safe harbor is a self-regulatory privacy protection system in the United States which was the subject of a positive adequacy decision by the European Commission on 26 July 2000 regarding data transfers from the European Union to the United States. Full documentation concerning safe harbor is available at http://www.export.gov/safeharbor/sh_overview.html.

3. The European Commission has approved model contracts for data transfer both for controller to controller transfers [Commission Decision of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries, under Directive 95/46/EC, (2001) OJ L181/19] and for controller to processor transfers [Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC, (2002) OJ L6/52].

parties to other EU agreements that include data protection provisions, notably in the area of police co-operation.[4] The same countries and others are also members of the Council of Europe (COE), and are bound by the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[5] Mexico has signed an Economic Partnership, Political Consensus and Co-operation Agreement with the European Union and its member States which establishes commitments to promote the protection of personal data, among other aspects. The respondents also share a commitment to implement various other international instruments (such as the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the OECD Privacy Guidelines), the United Nations Guidelines on Computerised Personal Data Files, and others).

With regard specifically to model contracts for data transfer, the decisions of the European Commission on model contracts are applicable in the EU member States and have been implemented by them. The Czech Republic recommends the use of model contracts. The USCIB has participated in the drafting of the alternative model contracts that the International Chamber of Commerce (ICC) and other business organisations have recently presented to the European Commission for approval.[6] A set of model clauses has also been jointly published by the ICC, European Commission, and COE.[7]

Codes of conduct, trustmarks, etc.

Most countries do not have government-endorsed codes of conduct. In Australia, some industry codes of practice have been lodged with the Privacy Commissioner for approval. In the Slovak Republic, all technological norms are endorsed by a governmental entity, while in Sweden industry organisations may submit codes of conduct to the Data Inspection Board for an opinion and the Board has, so far, issued opinions on two such codes. Japan has created a model for guidelines to be set up by business organisations, and a number of companies have set up guidelines in conformance with the model. In many countries (such as Austria, France, Mexico, and the United States) the use of codes of conduct for privacy protection is encouraged.

The majority of respondents mentioned that they have private sector codes of conduct, best practices, seal or trustmark programmes that are either endorsed by a business federation, or widely used by the private sector either generally or in a specific sector. Most of the responses concerned codes of conduct, but some (Germany, Japan and the United States, for example) also mentioned that they had seal or trustmark programmes. The Korean Association of Information and Telecommunications mentioned that they award an "ePrivacy Mark" to qualified Internet sites that satisfy stringent data protection criteria.

---

4. Such agreements include, *inter alia*, the Convention on the Establishment of a European Police Office (Europol Convention), the Convention on the Use of Information Technology for Customs Purposes and the Convention implementing the Schengen Agreement on the gradual abolition of checks at the common borders (Schengen Convention). Furthermore, the EEA-agreement (European Economic Area) between the EU and 3 EFTA countries (European Free Trade Association) stipulates full implementation of the relevant EU data protection instruments in the EFTA-countries being party to the agreement. The EFTA countries are: Iceland, Liechtenstein, Norway and Switzerland.

5. A full list of Member States of the COE and the list of those Member States which ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data is available at: http://conventions.coe.int/Treaty/EN/cadreprincipal.htm. The Convention was opened to signature on 28 January 1981 and the full text is available at: http://www.coe.int/T/E/Legal%5Faffairs/Legal%5Fco%2Doperation/Data%5Fprotection/.

6. The final version of the clauses was submitted to the European Commission on August 9, 2002 and is available at http://www.iccwbo.org/home/electronic_commerce/word_documents/Final%20version%20July%202002%20Model%20contract%20clauses.pdf.

7. Council of Europe/European Commission/ICC, Model contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows of November 2, 1992, with Explanatory Memorandum.

Security

Nearly every respondent mentioned some form of government regulation applicable to the security of Web sites, although in many countries (*e.g.* Austria, Finland, France, Norway, and Sweden) there is no special legislation dealing solely with Web sites but general data protection or security legislation. In Japan private sector guidelines set forth security parameters for business, and guidelines have also been promulgated by governmental entities. In Mexico there are self-regulating measures in the financial sector that guarantee the security of online services. In the United States, a site's misrepresentation to consumers about its privacy and security practices could be a violation of federal consumer protection law. Additionally, there are statutory provisions and administrative rules on security safeguards applicable to the financial sector.

Compliance

Variety of systems

Respondents indicated that a wide variety of entities are consulted in their countries for information and advice on compliance with the norms identified above. Those with a public independent privacy authority (for instance, Australia, Austria, Belgium and the Czech Republic) indicated that they could be consulted. A number of respondents also mentioned private-sector lawyers and law firms (*e.g.* Finland). Some mentioned governmental bodies other than privacy commissioners: for instance, in Japan there are "Information Security Advisers" at each Prefectural Police Headquarters (Local Police Department) who give information and advice about "Unauthorised Computer Access Law" and computer crime.

Best practices, software tools, etc.

Respondents indicated that governmental authorities responsible for privacy protection can review privacy practices of businesses. This can be based on administrative procedures, reviews based on best practices, software tools, or other means for reviewing the privacy practices followed by businesses engaged in online activities, Japan indicated that there are standard practices in place (such as "JIS Q 15001") which provide for regular business audits, as well as for a "Privacy Mark System". Switzerland mentioned that there is an initiative in the private sector for a labelling and auditing project for e-commerce. In the United Kingdom, the British Standards Institute has published an audit manual for self-audit, and has included data protection in its suite of software legal compliance tools. Similar initiatives have been promulgated by industry groups such as the World Wide Web Consortium (W3C); this was mentioned by the United States, which indicated that software tools can help companies translate their privacy policies into a Platform for Privacy Preferences (P3P) machine-readable format and can allow a company to inventory all features on its Web site so it can track and control its privacy risks. In the German omnibus privacy act, there is a provision on privacy auditing which is to be implemented by more specific legislation.

Australia and the United States indicated that they encourage companies to voluntarily engage in self-assessment of their privacy practices. It was noted that, in the particular case of the "Safe Harbor" frameworks in the United States, participants must assess their practices, either by a third party or by self-assessment. In the Netherlands, the data protection authority has developed auditing tools in co-operation with private organisations (*e.g.* a self-evaluation method and a framework for privacy audits). In Mexico and Sweden, companies voluntarily engage in such self-assessment. Most countries indicated that self-assessments are not usually made publicly available, with the exception of the United States, where some (but not all) companies make them public. Only in the Slovak Republic is there a legal requirement for self-assessment.

Governmental agencies and private sector oversight entities

In countries with governmental data protection agencies, such authorities are competent to oversee compliance with norms. Other governmental agencies may also monitor compliance with norms in specific sectors (for instance, in Finland the Finnish Communications Regulatory Authority together with telecommunications operators, the telecommunications equipment industry, and user associations promote privacy protection and information security in telecommunications). In those countries where private sector compliance systems are active (such as Japan and the United States), the entities that run such systems also monitor compliance with them, together with competent governmental agencies.

The organisation and powers of governmental regulatory bodies are determined by appropriate legislation. Private sector oversight entities are usually set up based on agreements entered into by the participants in the system. Governmental bodies have oversight powers as granted to them by law, which typically include carrying out audits, issuing warnings and reporting breaches to the appropriate authorities (as in France). Private sector entities tend to have similar powers, which can include responding to complaints and enquiries and expelling offending organisations from the scheme, without, of course, the full panoply of powers available to governmental entities.

Company privacy officers

Responses indicated that there is an increasing trend on the part of companies to appoint internal Data Protection Officers; in a few countries, there is a legal obligation to do so. The USCIB and United States government noted that self-regulatory bodies can offer advice on policy and practices, that over 500 companies now have Chief Privacy Officers who are responsible for ensuring that their companies adhere to existing laws and follow sound privacy practices, and that there now exist umbrella organisations in the private sector to assist companies in developing practices and procedures. The United States also mentioned that entities covered under the Health Insurance Portability and Accountability Act (health plans, health care providers, and health care clearinghouses) will be required by law to appoint a privacy officer when the Act takes effect in April 2003. Also, in Korea, companies must appoint a company privacy officer who will safeguard information and deal with complaints from data subjects. In the Slovak Republic, if a controller of information systems employs more than five persons, he has to appoint a responsible person or several such persons to carry on the supervision of compliance with statutory provisions in personal data processing. Finally, in Germany, public and private entities with more than four employees have to appoint a data protection officer. Almost none of the other respondents indicated the presence of a legal requirement for companies to appoint a privacy officer in charge of compliance. However, in Finland, the Data Protection Ombudsman has recommended that companies appoint a privacy officer, as do various self-regulatory programs in Japan and the data protection authorities in Norway, Switzerland, and the United Kingdom. The law of some member countries (*e.g.* Germany, the Netherlands and Sweden) exempt companies that appoint a company privacy officer from certain legal obligations (such as notification of data processing to the data protection authority).

Notification

Notification of data processing to an oversight entity is mandatory in Austria, Belgium, the Czech Republic, Finland, France, Italy, Norway, the Slovak Republic, Sweden, Switzerland, and the United Kingdom. However, even in such countries, certain exceptions apply, or notification may apply only to certain situations. For instance, in Sweden notification is not required if a personal data representative has been appointed or if the processing takes place with the individual's consent. Also, in Japan the TRUSTe

Japan seal program requires the notification of processing to an oversight department. Notification of data processing by banks may be required in Mexico under certain circumstances.

Technological solutions

Most respondents stated that technological solutions to protect privacy are implemented to a limited extent only, although some member countries (such as Japan, the United Kingdom, and the United States) indicated that the use of technical standards (such as P3P) to ensure compliance is expanding. The UK Information Commissioner promotes the use of privacy enhancing technologies, while in the United States there are many such tools widely available on the Internet (including P3P) but it is unclear how many businesses or consumers take advantage of them. The German Ministry of Economy and Technology has a programme to encourage the anonymous use of online technology. The Netherlands indicated that the Dutch government has committed itself to the use of privacy-enhancing-technologies in new public data processing systems. However, these initiatives remain exceptions. Otherwise, the use of technology to protect privacy was mentioned in the context of security. In Austria, as in other countries, the use of firewalls, anti-virus software and other safety precautions is standard, and the law requires certain data security measures but does not specify the exact techniques that are to be used. Finland indicated that the situation in companies varies to a great extent depending mainly on the size and partly on the field of the company. Japan stated that SSL and other encryption technologies are used to protect sensitive information such as credit card numbers, as is the case in Turkey.

Enforcement

Governmental authorities

Every member country has at least one government authority, which can enforce privacy norms (including the courts, the police, consumer protection agencies, data protection authorities, telecommunications regulatory authorities, unfair competition authorities, and others). Italy mentioned that under the law, data subjects can always turn to data controllers to exercise their rights in the event of a dispute. Japan, the United Kingdom, and the United States noted that data subjects may also be able to turn to a self-regulatory scheme, in cases where one is applicable.

Most respondents indicated the possibility of obtaining judicial or administrative relief based on a case brought in court or with governmental authorities, such as monetary compensation for damages, injunctive relief, erasure of data or blocking of processing. Austria noted that most privacy claims against private entities must be brought before the courts, but that many claims regarding privacy issues are resolved through other legal instruments (such as media law, unfair competition law, telecom law, and laws against libel and slander). The United States noted that the Federal Trade Commission (FTC) could sue companies who misrepresent their privacy policies, through administrative procedures or through the courts, and could obtain injunctions and monetary redress for consumers who are harmed. Most respondents indicated that administrative or penal fines are possible. Among those who may impose such fines are criminal authorities, data protection authorities, and consumer protection authorities. Most respondents stated that criminal penalties, including imprisonment and fines, are possible; however, Australia and Belgium stated that this is not the case, and the United States noted that such authority is narrowly prescribed. Most respondents indicated that monetary compensation for damages is possible. Most respondents stated also that either courts, data protection authorities, or both, could impose injunctive relief. In Belgium and France the data protection authorities may themselves not impose injunctive relief, but may apply to a court to do so.

Private sector entities

With regard to remedies that private sector entities can impose for violations, respondents mentioned withdrawal of seals and trustmarks, expulsions from self-regulatory schemes, and blacklists. Several also noted that in their countries (*e.g.* Finland, Norway, and the Slovak Republic) a private sector entity cannot itself impose a fine or take similar punitive action, but could bring a case in court or before a data protection authority against the offender. The USCIB said that loss of goodwill and reputation in the marketplace is important, and that in the United States, many alleged privacy incidents have been handled expeditiously by organisations so as to preserve their reputation. Japan indicated that a self-regulatory entity can direct participating companies to take certain measures, and punishment such as expelling the company from the scheme can be used to compel compliance.

Handling of complaints

There are a wide variety of procedures used for handling privacy complaints. In most member countries, complaints are brought before data protection or consumer protection authorities, which may then investigate the complaint and take appropriate action, which may include imposing penalties or referring the case to the courts or criminal authorities. In some countries (such as Italy) the data subject should first make an application to the data controller before applying for relief to the data protection authorities, whereas in others (Sweden, for example) the data subject may turn directly to the authorities or go first to the data controller. As Japan pointed out, self-regulatory bodies have their own procedures for handling complaints.

Online filing and ADR systems

Online filing of complaints is possible in a number of member countries (for example, Australia, Austria, France, Germany, Japan, Sweden, and the United States). Norway indicated that, while online filing was not formally provided for, it was used in practice (*i.e.* data subjects would often send complaints or inquiries to data protection authorities by e-mail). The United Kingdom is working on an online filing system. Mexico specifically noted that the Federal Consumer Protection Agency (Profeco) takes part in an international project conducted within the framework of the International Marketing Supervision Network (IMSN) which has resulted in the establishment of a Web site to gather and share complaints about cross-border electronic commerce.[8] In the United States, the FTC administers the IMSN website project and also maintains its own agency Web site[9] to allow consumers to report on privacy complaints, including those relating to Internet representations and e-commerce transactions.

Alternative dispute resolution (ADR) mechanisms for privacy-related disputes, such as arbitration and mediation, are in use in only a few countries, such as Austria, Korea and the United States. France indicated that a number of such schemes are now being developed by the European Commission. Italy indicated that ADR schemes are used, but that they are not specifically focused on privacy disputes. Such mechanisms are now being developed in Japan. In Germany some trustmark providers may offer such schemes.

8. 17 member countries take part in this project. See: www.econsumer.gov.

9. www.ftc.gov

Auditing

Only a few countries indicated that auditing of privacy practices is used as a method of enforcement. In Finland the Data Protection Ombudsman has the right to audit personal data registers and the Finnish Communications Regulatory Authority has the right to audit telecom operators' activities. The French Data Protection Authority (CNIL) has also used online surveys to inventory the practices of Web sites. Auditing by self-regulatory bodies is used in Japan and the United States, and voluntary audits are used in Mexico. Auditing may also be a kind of mandatory enforcement mechanism used by governmental agencies, for example in Sweden and the United States. Some of the local data protection authorities in Germany are presently using software tools to conduct audits of Web sites. Many respondents mentioned that security audits are often used to review the security of information systems and computer networks.

Public awareness

Methods

Most countries stated that the public or private sectors had undertaken campaigns to educate the public as to their privacy rights. Among the methods used are speeches and meetings; media interviews; disseminating copies of publications; information on the Web sites of privacy authorities,[10] the publication of annual reports by privacy authorities; the creation of online "privacy toolboxes" by companies; and self-regulatory schemes which tell users how they can limit disclosure of their personal information, what choices they have about how such information is used and shared, and under what circumstances they can access it.

Privacy policies

No respondents have specific legal requirements to post online privacy policies. However, in many member countries data controllers (including operators of Web sites) have legal obligations to inform the data subject of the processing of his data (including such matters as access rights etc), and this obligation can be satisfied through an online privacy policy. Many government and private sector schemes also encourage companies to post online privacy policies. When a privacy policy is posted, it may need to include certain mandatory information, such as the identity of the data controller and the purpose of the processing. There is evidence from several respondents that the number of Web sites posting privacy policies is growing rapidly.

Contact persons

Only a couple of countries (*e.g.* Belgium and the Slovak Republic) legally require the appointment of a contact person who can provide information on privacy practices or to whom persons can turn with complaints or questions. However, most countries indicated that they provide for incentives for the appointment of such a person. For instance, in France the law encourages companies to appoint a contact person for the purpose of access and rectification rights, since notifications to the CNIL must give the name of the department to which requests for access to and correction of personal data should be addressed.

10. For the United Kingdom, see: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf.

Publication of violations

Respondents provided a wide variety of answers to the question of whether privacy violations are published, and if so how. Some respondents (*e.g.* Mexico and Turkey) stated unequivocally that violations are not published, while others (*e.g.* Italy) do publish them. Most member countries indicated some possibility for publication, however restricted in some way. For instance, in Austria decisions are published online, but in anonymised form; in Belgium only decisions with particularly serious implications for the public are published by means of press communiqués; in the Czech Republic the data protection authorities publish only general reports on cases in its annual reports but not the text of individual decisions; and in the Slovak Republic only serious violations are published. In the United States, FTC investigations of alleged privacy violations are non-public, but administrative or court actions are made public on the FTC's Web site. The US Direct Marketing Association also mentioned that their "Safe Harbor Enforcement Program contract" contains language empowering the DMA to issue public press releases about an enforcement decision. Several respondents indicated that publication of violations, whether by the government or in the scope of self-regulatory compliance schemes, could be a very effective means of privacy enforcement; indeed, France stated that courts may use publication as an additional punitive measure. However, France also indicated that the publication of privacy violations could have legal implications for libel and other types of civil liability, and so had to be carefully considered in each individual case. The UK Information Commissioner has recently conducted a study of Web site compliance, which is published on the Commissioner's Office Web site.[11]

11. The report is available under Guidance and Other Publications: Codes of Practice our Responses and other Papers: Related Papers: UMIST UK Website Compliance Study at: http://www.dataprotection. gov.uk/dpr/dpdoc.nsf.

ANALYSIS

The OECD Privacy Guidelines

The 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data contain two types of provisions relevant to compliance and enforcement: *i)* provisions setting forth general principles of data processing (such as collection limitation, data quality, use limitation etc., and *ii)* provisions dealing with the interests of individuals concerning their personal information (such as individual participation, accountability, and national implementation). The first set of provisions, although formulated in the nature of conditions for the processing of personal data, are relevant to compliance and enforcement, since they set forth the practices which entities processing personal data should observe. The second set of provisions deals more directly with the recommendations for rights which individuals should have with regard to their personal data (Part 2. Basic Principles for National Application, Paragraph 13), and the recommendations to member countries to provide mechanisms for accountability (Part 2. Basic Principles for National Application, Paragraph 14) and to implement such principles by endeavouring to adopt appropriate domestic legislation, encouraging and supporting self-regulation, in the form of codes of conduct or otherwise, provide for reasonable means for individuals to exercise their rights, provide adequate sanctions and remedies in the case of failures to comply with measures that implement the principles, and ensure that there is no unfair discrimination against data subject (Part Four. National Implementation. Paragraph 19).

The 1980 Guidelines thus provide that individuals should be given certain rights in personal data relating to them; that the data controller should be accountable for complying with measures which give effect to such rights; and that member countries should implement certain legal, administrative, or other procedures to protect privacy and individual liberties in respect of personal data. At the same time, the Guidelines do not set forth in detail the mechanisms by which such protections are to be effected, and only provide certain suggestions for member countries to implement the OECD principles relating to privacy compliance and enforcement (see Paragraph 19 mentioned above). The Guidelines contemplate a flexible mixture between government regulation and private-sector self-regulation as the best way to ensure effective compliance and enforcement.

Shift in national frameworks for privacy protection

The legal frameworks for privacy compliance and enforcement which were initially created in most member countries concentrated on ensuring a good level of compliance and the rights of data subjects by creating a basic legal framework within which data subjects could exercise their rights, and focused on "traditional" enforcement mechanisms such as making complaints to data protection authorities and other governmental bodies, bringing suits in court, and ensuring that adequate penalties existed with which infractions of the law could be punished.

However, several significant developments since the passage of initial privacy legislation and regulation have complicated compliance with and enforcement of privacy rules:

- The world's economy is now much more globalised than was the case 20 or 30 years ago, and it has become routine for data subjects in one country to enter into transactions via electronic communications networks with entities in other countries.

- The use of computer equipment to process personal data has increased exponentially in a way that would have been unimaginable just a few years ago.
- Online systems such as portals, marketplaces, and communities have sprung up, which, while still subject to privacy law, function mainly based on self-imposed rules and terms and conditions agreed upon with users.
- The concept of privacy enhancing technologies (PETs) has been developed, to provide for before-the-fact compliance with privacy laws.
- The number of cross-border jurisdictional disputes based on online interactions has been continually increasing.[12]

These trends have fundamentally changed the legal landscape for privacy compliance and enforcement as borne out by the results of the questionnaire. While the principle that the government must pursue violations of the law remains the foundation upon which individual user trust in the area of privacy is based, traditional compliance and enforcement mechanisms (such as fines, investigations by data protection authorities, and court actions) are increasingly supplemented by alternative and complementary means of ensuring compliance with and enforcement of privacy protection.

As the responses to the questionnaire demonstrate, OECD member countries and private sector entities have developed and continue to develop alternative means to ensure compliance with and enforcement of privacy law which go beyond traditional governmental regulations and sanctions. Such alternative methods demonstrate a number of characteristics:

- They tend to make use of market-based incentives and punishments to ensure compliance with norms. For instance, many trustmark and privacy seal programs have been developed which require participating Web sites to adhere to certain privacy practices. If they do not, then the seal or trustmark may be taken away from them, which fact may be made public, thus exerting pressure on participants to comply with the scheme.
- They tend to use technical means as a way of ensuring compliance. Both member countries and private sector entities have been encouraging the use of privacy-enhancing technologies, technical standards for privacy protection (such as P3P), audits, and other compliance mechanisms to ensure that computer and online systems process personal data in compliance with applicable privacy principles. By encouraging compliance before the fact, the need for enforcement after the fact can be reduced.
- Businesses have come to see the commercial benefits which can accrue from offering privacy protection to customers, and have thus been offering many tools, mechanisms, and systems for privacy protection. These self-regulatory systems include trustmark programs, seals, PETs, company privacy officers, online privacy policies, and others.
- There is considerable potential for taking existing mechanisms for privacy compliance and enforcement and adapting them to the online environment. For instance, some member countries and commercial entities have made it possible to file privacy-related complaints online, and there are also a number of alternative dispute resolution (ADR) mechanisms for privacy disputes under development.

12. This is indicated by government reporting on numbers of complaints received through the use of www.econsumer.gov.

- Ensuring security is seen more and more as an essential element of privacy protection. It is therefore not surprising that both governments and private entities have been promoting technical standards, audits, security policies, and other mechanisms for ensuring the security of data processing online.

These developments demonstrate the changing face of privacy compliance and enforcement. Whereas these topics were previously seen with a legalistic, regulatory focus, attention has shifted to viewing them more holistically, so that government regulation is part of ensuring compliance and enforcement, but must be combined with technical, organisational, and self-regulatory mechanisms in order to attain maximum effectiveness in a cross-border online environment. Moreover, it is critical that privacy protection be viewed in a global perspective, rather than in a purely national one, in order to better facilitate redress for privacy violations that cross national borders. Ensuring compliance before the fact is less expensive, and imposes less burden on data subjects than having to pursue enforcement actions in court or otherwise. Many such initiatives are now underway, and there is every sign that their use will grow rapidly in the coming years.

Further steps

At the same time, more needs to be done in the member countries to encourage use of alternative mechanisms for privacy compliance and enforcement at the cross-border level. Progress needs to be made in particular in the following areas:

- The international and cross-border co-ordination of compliance and enforcement mechanisms is critical, both to protect the privacy of data subjects and to avoid putting data controllers in the position of being subject to varying requirements for the same conduct. Member countries should thus do everything possible to co-ordinate their compliance and enforcement activity to protect data subjects while minimising excessive burdens on data controllers, and providing for sufficiently flexible solutions to ensure effective privacy protection and continued transborder data flows, as recommended in the OECD Guidelines (see, for example, paragraph 7 of the Explanatory Memorandum to the Guidelines). At present, too many mechanisms seem to operate on a national or regional, rather than at a global, level; Member countries should work together to promote effective global co-operation with regard to privacy compliance and enforcement. In particular, member countries could take steps such as further sharing resources for handling complaints and educating individual users and businesses about privacy regulations and best practices, and fostering the development and use of online ADR and PETs. As a further step, member countries could strengthen enforcement against companies misrepresenting compliance with privacy policies or promises, particularly when those misrepresentations have adverse consequences that could cause harm to consumers.
- It seems that not enough is being done to encourage the implementation of technical solutions for privacy compliance and enforcement (such as P3P), since only a few member countries mentioned this as an area with much activity. Member countries should educate and raise awareness about such technical solutions and encourage their development and use. In particular, the use of PETs should be encouraged in order to provide data subjects with increased privacy protection.
- At present use of some self-regulatory mechanisms which hold particular promise for the protection of privacy online seems somewhat haphazard and is concentrated in a few member countries. For instance, from responses it seems that, in some countries, mechanisms such as encouraging companies to engage in voluntary self-assessment of privacy practices are not used as often as they could be.

- More member countries should encourage the appointment of company privacy officers. For example, member countries could consider providing a legal basis for them and/or granting companies legal incentives for their use. At present, in some countries the appointment by companies of a privacy compliance officer to oversee data processing is foreseen in the law, while in others it is implemented by companies on a purely voluntary or self-regulatory basis.
- While much thought is currently being devoted to the development of online ADR mechanisms for privacy disputes, few member countries have such mechanisms actually in operation. The development of ADR systems could be crucial for improving the legal situation for data subjects regarding enforcement, and more needs to be done in this regard. It is particularly important that such systems be constructed to take into account the global nature of electronic commerce (*e.g.* they should function in multiple languages), and that they are able to cope with transborder disputes.
- Given the likely increase in privacy complaints and the limitations on government resources to address them, member countries should focus on areas where individual users suffer the most harm as a consequence of misuse of their personal data.

Member countries are currently making good progress toward providing an effective regime for privacy compliance and enforcement for the online environment, but further work remains to be done. The key for the coming years will be to make traditional means of regulatory enforcement even more efficient, while at the same time encouraging the growth of self-regulatory mechanisms, since a mixture of these two systems is likely to best protect the interests of both data subjects and data controllers. Moreover, it is critical that any mechanisms developed are able to operate on a transborder basis.

ANNEX

QUESTIONNAIRE ON COMPLIANCE WITH AND ENFORCEMENT OF PRIVACY PROTECTION IN THE CONTEXT OF BUSINESS-TO-CONSUMER ELECTRONIC COMMERCE

1. When answering the questions below, please:

- Focus on their application to online activities. You may give information that is not specifically targeted to online activities, but if so, please indicate how such information is applied to the online world.
- Focus on the business-to-consumer (B2C) realm. At the discretion of member countries, information related to the public sector may also be included.
- Provide broad coverage regarding the information requested. In particular, your responses should cover not only regulatory approaches, but also self-regulatory schemes such as corporate privacy officers, privacy seals, auditing procedures, industry bodies, technologies (such as privacy-enhancing technologies), and the like.
- Distinguish, where appropriate, among regulatory and non-regulatory approaches addressing privacy compliance and enforcement generally, and on a sectoral basis. You should also mention legal provisions and self-regulatory schemes that may not be specifically designed for privacy protection, but which could nonetheless impact it.
- Indicate any differences between mechanisms used in a domestic context, as opposed to those with a cross-border element. Provide information on domestic schemes, but focus on their application at the cross-border level.
- Indicate any co-operative mechanisms or efforts for ensuring compliance with and enforcement of privacy protection at the global level (whether bilateral or multilateral formal or informal cross-border co-operation).

In addition, please recall from the introduction section of this document that we use the terms "legal provisions", "non-regulatory", and "self-regulatory" in a generic, general and inclusive sense.

2. Norms and instruments

These questions are designed to determine the standards and reference points for online privacy compliance and enforcement at the domestic level. Please provide references of these norms and instruments, and also indicate which provisions are directed at cross-border and international issues.

Do you have any of the following that may be the basis for legal rights and obligations in the area of privacy:

2.1 Do you have a law or laws on the protection of privacy and personal data? If so, please indicate if it is a single omnibus law, or a collection of sectoral laws, or both.

2.2 Do you have other forms of relevant legal regulation (such as decrees, ordinances, administrative rules, case law (*jurisprudence*), or the like?

2.3 Is your country a party to public law agreements or instruments in the privacy sphere (for example, the Safe Harbour)?

2.4 Has your country implemented other private law agreements or instruments which may be the basis for data protection (*e.g.* model contracts for data transfer)?

2.5* Do you have any industry codes of conduct endorsed by a government entity?

2.6* Do you have any private sector codes of conduct, best practices, seal or trustmark programs which are either endorsed by a business federation, or widely used by the private sector either generally or in a specific sector?

2.7* Do you have any government regulation or applicable private sector practices requiring Web sites to have security policies, rules or technical measures in place to protect the personal data of visitors from unauthorised access, improper use or disclosure, and the like?

3. Compliance

Keeping in mind the norms identified above, please explain how compliance with these is ensured at both the national and cross-border levels with regard to online activities.

3.1* Where do companies obtain information and advice on compliance with the norms identified above? For instance, do they consult with a lawyer (either external or internal), make use of internal privacy compliance officers (whether because of legal requirements or business practice), use consultants, or consult with data protection or consumer regulators?

3.2* Are there administrative procedures, reviews based on best practices, software tools (whether used for privacy protection or privacy auditing), or other means for reviewing the privacy practices followed by businesses engaged in online activities?

3.3* Do oversight entities exist which are competent to review compliance with the norms mentioned above? For instance, are such entities government agencies, independent data protection authorities, or private sector bodies?

3.4* How are such oversight entities set up, and what powers do they have?

3.5* Do companies voluntarily engage in self-assessment of their privacy practices? Are such self-assessments made publicly available?

3.6* Are companies encouraged or required to appoint a company privacy officer in charge of privacy compliance?

3.7 Are companies required to notify their data processing to an oversight entity?

3.8* To what extent are technological solutions for privacy protection used in your country?

3.9* Are there any other compliance procedures or processes used which are not mentioned above?

4. Enforcement

Please explain how the norms identified above are enforced.

4.1* To which organisations, entities, or persons may parties or data subjects turn to obtain enforcement of the norms?

4.2 What remedies are available to injured parties, and how can infringing data controllers be forced to comply with the applicable privacy norms?

4.3* What kind of remedies can private sector entities impose for violations? For example, withdrawing a seal or trustmark, blacklisting a company, or bringing the case to court?

4.4 Are administrative or penal fines available to deter or punish violations, and who is authorised to request such fines (*amendes*)?

4.5 Can a court order other criminal penalties, such as imprisonment?

4.6 Can injured parties obtain monetary compensation for damage caused to them by violations (*dommages-intérêts*)?

4.7* Can an oversight entity (whether in the public or private sector), authority or court impose injunctive relief (*exécution d'un droit*), such as ordering that access be granted to personal data, or prohibiting a data transfer?

4.8* What sorts of procedures exist for handling complaints?

4.9* Is it possible to file complaints online, or are there other possibilities for making use of Internet or online technologies for the resolution of disputes?

4.10* Are third party dispute resolution mechanisms, such as alternative dispute resolution (ADR) proceedings (whether in the public or private sector), used for the resolution of privacy-related disputes?

4.11* Is auditing of privacy practices used as a method of enforcement? If so, is auditing voluntary, or is there an obligation to be audited? Note that "auditing" in this sense is to be understood widely, and includes, for example, not only auditing of practices by professionals, but also auditing of online practices using software tools (such as software robots to evaluate Web site compliance or to find out where a seal or trustmark is being displayed).

4.12* Are technical standards used to ensure compliance (for example, P3P)? Are there any legal incentives for using such standards?

5. Public awareness

Please explain how members of the public are made aware of their privacy rights and of privacy violations in the online environment.

5.1* Are companies required or encouraged to post privacy policies or to make any reference to notification to an oversight entity, or both?

5.2* Are companies encouraged to appoint a contact person who can provide information on privacy practices or to whom persons can turn with complaints or questions?

5.3* Are violations of privacy norms publicised, and if so how (for example, by posting information on the Internet, or publicity to the press)? Who publicises such violations?

5.4* Does the public or the private sector undertake campaigns to educate the public as to their privacy rights, and if so, how is this done? Is this done through special campaigns or by continual and regular activities?