OECD QUESTIONNAIRE ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS

Introduction

1. Twenty-five years after their adoption, the OECD Privacy Guidelines remain a fundamental statement of the international consensus for privacy protection. Known primarily for the baseline principles they establish for the collection and handling of personal data, the Guidelines also call on member countries to establish procedures for "information exchange and mutual assistance" in procedural and investigative matters. In 1998, OECD ministers reiterated the need for effective enforcement mechanisms to address non-compliance.[1] Ever-increasing global information flows have further intensified the importance of revisiting international co-operation issues.

2. In 2003, the OECD Working Party on Information Security and Privacy (WPISP) produced a report on compliance and enforcement of privacy online. Based on the responses to a questionnaire to member countries and the private sector, the report highlighted the need for further work on cross-border co-ordination of privacy compliance and enforcement mechanisms.[2]

3. Under its work programme for 2005-06, the WPISP is tasked with new work on the issue of cross-border enforcement, with the aim of possibly developing an instrument to facilitate cross-border co-operation.[3] In order to better understand the cross-border enforcement challenges, the Working Party agreed to begin with a questionnaire addressed to OECD countries. The information gathered through this questionnaire will form the basis of a report that will be presented to the WPISP and help inform the development of the potential co-operation instrument.

4. The current volumes and destinations of transborder data flow, suggest that enforcement co-operation will need to extend well beyond the boundaries of the OECD to be effective. Therefore, it is hoped that non-member economies will also wish to respond to this questionnaire, and find value in the expected report and co-operation instrument.

Related Initiatives

5. Work at the OECD on this topic will build upon work carried out in the past, and be co-ordinated with current work in other forums. In particular, past work by the Council of Europe and the European Union noted the need for cross-border enforcement co-operation and established a preliminary basis for co-operation by participating countries. Last year the EU's Article 29 Working Party issued a declaration on enforcement, in which it announced plans for EU-wide synchronised investigations on common issues.

6. In November 2005, APEC Ministers endorsed the International Implementation Section of the APEC Privacy Framework. This Section calls for APEC economies to designate public authorities responsible for facilitating cross-border co-operation in connection with privacy protection. It further

---

1 OECD Declaration on the Protection of Privacy on Global Networks (1998).

2 DSTI/ICCP/REG(2002)5/FINAL.

3 DSTI/ICCP/REG(2005)9.

encourages the development of co-operative arrangements covering: (*i*) notification; (*ii*) information sharing; (*iii*) investigative assistance; (*iv*) the establishment of co-operation priorities; and (*v*) the maintenance of confidentiality.

7. Finally, cross-border co-operation efforts are underway in related areas such as spam and consumer protection. In the case of spam, this co-operation is particularly relevant as it involves privacy enforcement authorities in some instances. The OECD is currently working on an instrument to improve anti-spam enforcement co-operation, and informal information exchange occurs through the London Action Plan.[4] In the consumer area, the OECD has also developed a set of Guidelines to facilitate enforcement to protect consumers against cross-border fraud.[5] Many of the issues addressed by these initiatives will be instructive for the work on privacy enforcement co-operation.

Request for Responses

8. Member countries are invited to complete the questionnaire on behalf of their privacy enforcement authorities and to send their responses to XXXXX and XXXX by **20 March 2006.**

4 www.londonactionplan.com.

5 www.oecd.org/sti/crossborderfraud.

OECD QUESTIONNAIRE ON THE CROSS-BORDER ENFORCEMENT OF PRIVACY LAWS

Scope and Definitions

The questionnaire aims to elicit information to (*i*) understand the basic mechanisms for privacy enforcement in each country; (*ii*) identify current challenges present in cross-border co-operation; and (*iii*) point towards promising directions to address those challenges.

The term **enforcement** as used in this context means efforts by government authorities to (*i*) secure legal remedies for individuals that have been harmed; (*ii*) carry out regulatory audits and inspections; and (*iii*) secure compliance by formal legal action of an administrative, civil, or criminal nature.

Following the OECD Privacy Guidelines, this questionnaire is intended to cover the enforcement of privacy laws for both the **public sector** and the **private sector**. It is recognised, however, that the enforcement of privacy laws for public sector data controllers may differ from that of the private sector. Where it would be helpful, separate responses could be provided for each sector.

While recognising the important role of **regional or local enforcement authorities**, the focus of the questionnaire is governmental enforcement authorities having nation-wide authority. However, where it would be helpful, responses on behalf of regional or local authorities are also welcome.

There is often an important role for **public prosecutors, the police, and judicial authorities** in privacy enforcement. Cross-border co-operation among these types of entities is typically governed by existing bilateral or multilateral arrangements and therefore a focus of this project. Nevertheless, responses may describe the role of these entities where it would help to provide a complete picture of privacy enforcement.

The **private sector** has a crucial role to play in privacy compliance overall, as well as useful information to convey regarding government enforcement of privacy laws. Its views, along with those of civil society, will be sought in preparing the report, though not by means of this questionnaire, which is directed to governments.

The term "**Privacy Enforcement Authority**" (or "Authority") refers to public authorities or agencies that have an enforcement role at the national level. It does not include criminal law enforcement agencies that have no jurisdiction over privacy enforcement issues. An enforcement role could include any of the following functions: receiving complaints, conducting investigations, and/or initiating (or referring) proceedings to a court or tribunal.

The term "**cross-border**" is used in a broad sense to include cases where the data subject is located in a different country from the data controller, the data itself has passed to a third country, or simply where important evidence is located in a third country.

Other terms in the questionnaire should be interpreted consistently with the OECD Privacy Guidelines.

Instructions

Please provide responses on behalf of your primary Privacy Enforcement Authority. Where you have more than one such Authority, please provide answers for each one, to the extent that such information is readily available. If you respond on behalf of multiple Authorities, please complete a separate copy of the questionnaire for each one. Your responses will be used for the preparation of a report, but will not themselves be made public.

Questions have been drafted in a YES/NO format where possible to minimise the burden in responding. However, mechanisms for privacy enforcement may differ significantly from country to country. Where the structure of the questions is not adequate to describe your enforcement system, **supplemental explanations** are welcomed.

QUESTIONS

Please complete a separate copy of the questionnaire for each of your primary Privacy Enforcement Authorities

Responding Country:

Name of Privacy Enforcement Authority:

Section I - Basic Enforcement Mechanisms for the Authority

1. Please identify the Privacy Enforcement Authority by providing the following information if available:
   a. A link to the Authority's Web site:
   b. Date of establishment:
   c. Annual budget:
   d. Total number of staff:
   e. Number of staff directly engaged on privacy enforcement-related activities:

A. Complaints handling

2. Is the Authority able to receive complaints from data subjects or individuals? YES/NO
   a. Does the data subject or individual filing a complaint have to be a citizen? YES/NO
   b. Does the data subject or individual have to be legally resident in the country? YES/NO

3. Can complaints be received by:
   a. Mail? YES/NO
   b. Telephone? YES/NO
   c. Online via email or through a Web-based complaint form? YES/NO

4. Is the Authority obligated to investigate all complaints? YES/NO
   If YES, please identify any important exceptions to this obligation:

B. Investigation/ audits/ inspection

5. Can the Authority initiate an investigation on its own initiative? YES/NO
   (*i.e.* without having received a complaint, e.g. based on a media report)
6. When conducting an investigation is the Authority able to:
   a. Compel testimony from data controllers? YES/NO
   b. Compel documents or files from data controllers? YES/NO
   c. Compel information from third parties? YES/NO
   d. Enter premises without consent? YES/NO
   e. Compel a temporary or permanent cessation of data processing activities? YES/NO

7. Does the Authority have the power to make on-site inspections or audits at the premises of a data controller? YES/NO

   If YES, which conditions apply:

   a. Need for reasonable grounds to believe that there has been non-compliance? YES/NO
   b. The data controller has to be informed in advance? YES/NO
   c. The consent of the data controller is required? YES/NO
   d. Other (please specify):

C. Sanctions/remedies/outcomes/powers of intervention

8. After an investigation, what actions can the Authority take with respect to a data controller:

   a. Conduct voluntary mediation between the data controller and the complainant? YES/NO
   b. Conduct binding arbitration between the data controller and the complainant? YES/NO
   c. Assist the data subject in pursuing redress through the courts? YES/NO
   d. Reach a conclusion or determination that the law has been violated? (i.e. without the need to institute formal legal proceedings) YES/NO
   e. If YES, does the conclusion have legal force? YES/NO
   f. Publicise a violation? YES/NO
   g. Issue a warning or reprimand? YES/NO
   h. Negotiate a fine or other settlement? YES/NO
   i. Issue a legally enforceable order? YES/NO
      (e.g. to cease or alter a practice, provide access, or destroy/erase data)
   j. Order financial compensation? YES/NO
   k. Seek injunctions through the courts? YES/NO
   l. Seek redress, fines, imprisonment or other penalties on its own initiative or through the courts/legal system? YES/NO
   m. Initiate a criminal prosecution? YES/NO
   n. Other (please specify):

9. What sanctions or remedies other than those available to the Authority (described in Question 8) are available through the legal system (*e.g.*, through a public prosecutor):

   a. Orders? (e.g. to cease or alter a practice, provide access, destroy/erase data) YES/NO
   b. Compensation to the data subject? YES/NO
   c. Civil penalties? YES/NO
   d. Criminal fines? YES/NO
   e. Imprisonment following a criminal conviction? YES/NO
   f. Other (please specify):

10. If the sanction or remedy that is obtained by the Authority is not complied with by the data controller, what further steps are available to the Authority?

11. If a sanction obtained in court is not complied with, what further steps are possible?

Section II - Cross-border Aspects of Enforcement

A. Existing arrangements for facilitating cross-border co-operation

12. Does the Authority (or your country) have any bilateral or multilateral arrangements with other authorities or countries to co-operate in the enforcement of privacy laws?[6] YES/NO

    If YES, please provide copies or Web links to any relevant arrangements.

13. If a single national point of contact has been established to co-ordinate cross-border co-operation of privacy laws, please provide the contact information:

    If NO, would it be possible to establish a national point of contact? YES/NO

14. Does the Authority have priorities for enforcement?[7] YES/NO

    a. If YES, please describe those priorities.
    b. Please identify any differences for cases with a cross-border element.

B. Cross-border challenges

15. Can the Authority take action against a foreign data controller on the grounds that the privacy violation concerns domestic data subjects? YES/NO

    If YES, under what circumstances?

16. Can the Authority take action against a domestic data controller on the grounds that the privacy violation concerns foreign data subjects? YES/NO

    If YES, under what circumstances?

17. Please describe any other grounds for the Authority to take action against a foreign data controller:

18. Can the Authority notify authorities in other countries about investigations of possible privacy violations that affect those countries? YES/NO

    If YES, under what circumstances?

19. Can the Authority share information with, or otherwise provide investigation assistance to a foreign Authority? YES/NO

    If YES, under what circumstances?[8]

---

6 We already have information about the Council of Europe Convention 108, the European Union Directive 95/46/EC, the International Conference of Data Protection Commissioners, the EU Article 29 Working Party, the OECD Spam Task Force, and the London Action Plan, so responses need not refer to these arrangements.

7 For example, cases causing serious harm to an individual(s)? Cases harming a large number of individuals? Cases involving a particular type of privacy violation?

20. Are any of the following factors considered to be obstacles to effective cross-border enforcement of privacy laws:

    a. Lack of legal powers? YES/NO
    b. Incompatibility of legal regimes? YES/NO
    c. Restrictions on sharing information? YES/NO
    d. Inadequate resources? YES/NO
    e. Language/communication barriers? YES/NO
    f. Other (please specify):

21. Please describe or provide a Web link to any enforcement actions that could serve as case studies to illustrate cross-border enforcement challenges (there need not have been a successful outcome to the action):

Section III - Quantitative Information

To the degree that such information is readily available, please complete the following tables with information from 2004 and 2005. If your statistics are compiled in a different way, please share any relevant information you have on privacy complaints in a convenient format.

22. For all complaints received by the Authority in 2004, please provide indications in Table 1 below about the percentage which related to each of the listed privacy requirements, the relevant sector implicated by the complaint, and the context in which the data was collected or processed:

Table 1: Complaints Received 2004

Privacy Requirements*	%	Relevant Sector	%	Context	%
Openness/transparency		Financial institutions		Direct marketing	
Data quality		Telecom/broadcasting		Spam	
Collection and use		Transportation		Ongoing customer relationships	
Security safeguards		Insurance		Conditions of sale/service	
Subject access		Retail/merchants		Employment	
Transborder data flows		Health care		Surveillance (video or other)	
Other		Professions		Other	
		Not-for profits/charities			
		Government			
		Other			

Note: *For a short description of each of these requirements, see the table attached to question 27.

[8] For example, does the practice in question have to be illegal in both countries as a condition to co-operation? Does it help if the complainant consents to sharing personal information with the other foreign Authority?

23. For all complaints received by the Authority in 2005, please provide indications in Table 2 below about the percentage which related to each of the listed privacy requirements, the relevant sector implicated by the complaint, and the context in which the data was collected or processed:

Table 2: Complaints Received 2005

Privacy Requirements	%	Relevant Sector	%	Context	%
Openness/transparency		Financial institutions		Direct marketing	
Data quality		Telecom/broadcasting		Spam	
Collection and use		Transportation		Ongoing customer relationships	
Security safeguards		Insurance		Conditions of sale/service	
Subject access		Retail/merchants		Employment	
Transborder data flows		Healthcare		Surveillance – video or other	
Other		Professions		Other	
		Not-for profits/charities			
		Government			
		Other			

24. For all complaints received in 2004 and 2005, please provide an indication in Table 3 below as to how the complaint was handled and the final outcomes (if known):

Table 3: Investigations/Outcomes 2004-05

	2004 (%)	2005 (%)
Of the complaints received, what percentage were investigated		
What percentage were settled/mediated without enforcement action		
In what percentage were determinations of wrongdoing made		
How often was binding compliance action taken by the Authority		
How often was binding compliance action taken by the courts		
How often were fines levied		
How often were criminal proceedings brought		

25. If fines were levied in 2004 or 2005, please identify:

    a. The maximum fine?
    b. The minimum fine?
    c. The average fine?

26. In what percentage of cases was the Authority unable to complete or enforce the results of an investigation because the evidence or the organization accused of violating the legislation was outside the Authority's jurisdiction?

    a. Percentage in 2004:
    b. Percentage in 2005:

Section IV - Privacy Law(s) enforced by the Authority

27. Please complete the attached Privacy Law Summary Table for each privacy law enforced by the Authority:

PRIVACY LAW SUMMARY TABLE

Title of Law:

Web link:

Name of Enforcement Authority:

Scope of Coverage:

- Nation-wide YES / NO
- Sub-national (*e.g.* regional, provincial, state, etc.) YES / NO
- Public sector YES / NO
- Private sector YES / NO

Principal Economic Sector:

Indicate the primary focus of a sectoral law according the key below. If the law applies generally to all sectors (i.e., an omnibus law) please respond with "GA".

- Generally applicable (GA)	*- Electronic communications (EC)*
- National number or identifier (NI)	*- Financial information (FI)*
- Credit referencing (CR)	*- Health information (HI)*
- Direct marketing (DM)	*- Other (please specify)*

Content:

Please indicate whether the law contains provisions addressing the following privacy principles:

Openness/Transparency: YES / NO
e.g. notification of, and information on, the existence of data processing.

Data quality: YES / NO
e.g. accurate, up to date, relevant, not excessive data

Collection and Use: YES / NO
e.g. fair and lawful collection and processing; purpose specification; disclosure; consent, cross-border data transfer

Security Safeguards YES / NO
e.g. administrative, technical or procedural mechanisms for insuring the confidentiality, integrity, and protection of data

Subject Access: YES / NO
e.g. knowledge that your data is being processed; the ability to see that information and to correct or delete it if it is incorrect; some means of redress if needed.

Transborder Data Flows YES / NO
e.g. special protections for the transmission of personal data across borders