



Asia-Pacific
Economic Cooperation

2007/SOM3/ECSG/SEM/011

Agenda Item: 1

Cross-Border Privacy Law Enforcement Co- Operation - The New OECD Recommendation

Purpose: Information

Submitted by: OECD



**2nd Technical Assistance Seminar on the
International Implementation of the
APEC Privacy Framework
Cairns, Australia
25-26 June 2007**



Cross-border Privacy Law Enforcement Co-operation

The New OECD Recommendation

APEC Data Privacy Seminar

Cairns, 25 – 26 June 2007

Overview of the project

- Working Party on Information Security and Privacy
 - expert group, chaired by the Privacy Commissioner of Canada
 - includes privacy officials, EC, Council of Europe.
 - consultation with Business, Civil Society, other int'l groups
- The fact-finding (October 2006)
 - Questionnaire and Report on Privacy Enforcement
 - describes existing enforcement authorities and systems
 - identifies cross-border challenges needing further work
- The policy response (June 2007)
 - New OECD Recommendation + practical tools



Why work on improved enforcement co-op?

need for this work is a recurring theme for OECD . . .

- **OECD Privacy Guidelines (1980)**
 - *facilitate mutual assistance in procedural & investigative matters.*
- **Ottawa Ministerial Declaration (1998)**
 - *ensure effective enforcement mechanisms for non-compliance and redress*
- **Report on Privacy Online (2003)**
 - *establish mechanisms for cross-border co-operation between public agencies in procedural and investigative matters*



and in line with a broader trend . . .

- APEC Data Privacy Subgroup
- Int'l Commissioners Conference (Montreux Declaration)
- Council of Europe, EU Art. 29 Working Party

3



The evolving climate for data flows and privacy risks

Technology and Data flows

- Fast, cheap connections
- Efficient storage and processing
- Data and voice converge via IP
- Data flows with a mouse “click”

Changing Business Processes

- Global distribution of tasks
- Int'l data transfers are increasingly integral to the economy
- Human resources, financial services, customer service, education, e-commerce





The evolving climate for data flows and privacy risks

Privacy risk environment

- Data breach
- Secondary usage
- Identity theft

Changing user perceptions

- Data breach reports → consumers go elsewhere
- Increasing fears of data misuse → online banking interest declines
- Online users mobilise fast (e.g. Facebook)



How are privacy laws enforced?

- Privacy enforcement authorities are commonplace
 - 1980: about 1/3 had authorities → today: nearly all OECD countries
 - Varied structures
 - individual complaint resolution vs. regulatory compliance
 - independent authorities, commissions, government departments
 - public sphere, private sphere, particular economic sectors
 - Varied powers and enforcement processes
 - information gathering powers (onsite inspections, production of documents, audits)
 - sanctions, remedies, outcomes (declare violations, publicity, enforceable orders, fines, compensation for individuals)
 - administrative vs. civil vs. criminal
- To what degree do these variations impact enforcement co-operation?



Cross-border challenges

- **Mutual assistance**
 - notification
 - information sharing
 - investigative assistance
- **Enforcement powers**
 - foreign data controllers or data subjects
 - sanctions and remedies: do they provide adequate deterrence?
- **Identifying common enforcement priorities**
- **Need for continued information gathering**
 - cross-border complaint and case trends
 - role of informal or regional networks



Existing activities and initiatives

- **Enforcement activities**
 - cross-border cases: only a handful
 - cross-border audits/inspections: on the increase
- **International instruments (with an enforcement component)**
 - CoE Convention 108, EU Directive 95/46/EC, APEC Privacy Framework
 - EU-US Safe Harbor, AUS-NZL, ESP-USA
- **Less formal networks (without an enforcement focus)**
 - Int'l Commissioner's Conference, IWGDPT, APPA, Iberoamerican
- **Examples from other areas**
 - spam and consumer protection



The Policy Framework

- OECD Council Recommendation
 - non-binding, but represents a serious commitment
 - co-operation occurs within existing legal framework
 - approval at level of ambassadors sends an important signal
- Blends:
 - high-level policy objectives with key elements for good co-operation
 - while articulating some limits to co-operation
 - leaving the implementation details to MCs and their authorities
 - inviting non-OECD economies to collaborate with OECD members
- Follows OECD precedents on enforcement co-operation
 - consumer protection, spam, competition law
- Grounded in the 1980 Privacy Guidelines



Key Actors

- “*Privacy Enforcement Authorities*”
 - Public bodies
 - Enforcement responsibility for “*Laws Protecting Privacy*”
 - Power to investigate or pursue enforcement proceedings
- Other stakeholders
 - Criminal law enforcement bodies
 - Privacy officers in organisations
 - Private sector oversight groups
- Don’t forget governments



Scope and Related Issues

- Would cover enforcement of “*Laws Protecting Privacy*”
 - national laws, the enforcement of which, has the effect of protecting personal data consistent with the OECD Privacy Guidelines
- Focus of Recommendation is:
 - violations most serious in nature
 - primarily aimed at private sector (but can include public sector)
 - and is not intended to interfere with government activities related to sovereignty, security, public policy
- Role of Discretion
 - Authorities may decline or limit assistance, where the request is outside the scope or otherwise inconsistent with national laws, important interests or priorities



Domestic Measures

- Recognises that you need to have the right domestic arrangements to co-operation internationally
- Effective Powers and Authority
 - Sanctions and deterrence
 - Investigations
 - Corrective action
- Ability to co-operate
 - To share information
 - To provide assistance (e.g., obtain documents or statements)
- Calls for a review of laws, procedures -- and adjustments if needed!



International Co-operation

- **Mutual Assistance**
 - Notifications, referral of complaints
 - Requests for assistance
 - Preserve the confidentiality of non-public information
 - Respect the purpose specified when information exchanged
 - Co-ordinate investigations to avoid interference
- **Collective initiatives in support of mutual assistance**
 - Contact points, information about laws
 - Sharing information about outcomes
 - Foster the establishment of an informal network of authorities
- **Co-operation with other stakeholders**
 - Criminal authorities, privacy officers, civil society, business



OECD and APEC frameworks: common elements

Provision	OECD	APEC
Notification	¶17	¶45(a)
Information sharing	¶12(a)	¶45(b)
Investigative assistance	¶12(b)	¶45(c)
Preserving confidentiality	¶18(b)	¶45(e)
Discretion to decline or limit co-op	¶15	¶44
Bilateral or multilateral MOUs	¶13	¶44



Practical Tools

- **Contact List**
 - Single national point of contact via a designation form
 - Internal list (with complete contact information)
 - Public list (can exclude personal contact information)
 - Co-ordinate with contact lists in APEC, elsewhere?
- **Request for Assistance Form**
 - Identifies key categories of information to be provided
 - Ensure careful preparation: helps ensure that preliminary investigation has been conducted
 - Flexible: can be adopted to fit the situation (referral, audit, etc.)
 - Not Duplicative: doesn't ask for what is readily available elsewhere
- **Restricted-Access Web site**
 - Access restricted to privacy enforcement authorities
 - To permit discussion on actual cases, general issues
 - Could be supplemented by a public section



Privacy Law Enforcement Co-operation Project

Contact Point Designation Form

Country Name: _____ Date of Last Update: _____

Internal Contact Point

Please provide information for each category.
This information will be maintained in a non-public list.

Authority	
Name	
Address	
Telephone	
Fax	
E-mail	
Web site address	

Public Contact Point

Countries may also provide a public contact point, and should only indicate information appropriate for public disclosure below. (e.g. you may not wish to include an individual's name, phone, or email)



Request for Assistance Form

Please see the instructions on page 4

Date of the request:

1. Case name

2. Authority contact details

From:

Requesting Authority, Country	
Contact Person, Title	
Telephone	
Email Address	

To:

Receiving Authority, Country	
Contact Person, Title	
Telephone	
Email Address	

3. Confidentiality requirements



9. Type of Privacy Principles at Issue

You may add explanation under each principle if necessary.

	Yes	No
Openness/Transparency: <i>e.g.</i> notification of, and information on, the existence of data processing		
Data quality: <i>e.g.</i> accurate, up to date, relevant, not excessive data		
Collection and Use: <i>e.g.</i> fair and lawful collection and processing; purpose specification; disclosure; consent; cross-border data transfer		
Security Safeguards: <i>e.g.</i> administrative, technical or procedural mechanisms for insuring the confidentiality, integrity, and protection of data		
Subject Access: <i>e.g.</i> knowledge that your data is being processed; the ability to see that data and to correct or delete it if it is incorrect, some means of redress if needed		
Transborder Data Flows: <i>e.g.</i> special protections for the transmission of personal data across borders		

10. Possible law violations and potential sanctions



Michael Donohue

michael.donohue@oecd.org

+33 1 4524 1479

www.oecd.org/sti/privacycooperation

www.oecd.org/sti/security-privacy