DATA PRIVACY AND DATA PROTECTION IN E-COMMERCE IN VIETNAM

Mr. Duong Hoang Minh
Vietnam e-Commerce and Information Technology Agency (VECITA)

APEC ECSG Data Privacy Seminar
Peru, Lima
February 18, 2008

CONTENT

- Data privacy and personal data protection in the world
- Data privacy and personal data protection in Vietnam
- Legal framework on data privacy and personal data protection in Vietnam
- Privacy policy of Vietnamese websites
- Recent personal data leakage cases
- Approaches to enhance personal data protection in Vietnam

Data privacy and personal data protection in the world

Data privacy and personal data protection in the world

- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980).
- EC's Directive 95/46/EC in Oct. 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- APEC Data Privacy Framework (2004).
- In USA, Canada, Japan,... Legal Frameworks on Data Privacy are already in place.

The issue of data privacy and personal data protection in Vietnam

- The concepts of personal information protection and data privacy are still new.
- Legal framework is still lack of regulations on data privacy and personal information protection.
- Knowledge and understanding of general public and businesses are limited.

Legal framework on data privacy and personal data protection in Vietnam

- Civil Code (2001): Article 38. Right on personal life confidentiality.

  This article stipulate that right on personal life confidentiality is to be respected and protected by law. The collection, disclose of private life of a person must be under his/her agreement or consent.

- Criminal Code (1999): Chapter III. Offences on the right on freedom and democracy of citizen

  Article 125. Offence on violation the confidentiality or safety of mail, telephone, facsimile of other people

Legal framework on data privacy and personal data protection in Vietnam (cont.)

- Law on E-Transactions: Article 46. Information confidentiality in e-transactions

  1. Agencies, organizations and individuals shall have the right to select security measures in accordance with the provisions of the law when conducting e-transactions.

  2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consents, unless otherwise provided for by law.

- Law on Information technology: Article 21 and Article 22.

  These two articles stipulate more detailed regulations regarding information protection in the environment such as regulations on collection, process, use, storage and provision of personal information.

Privacy policy of Vietnamese websites

- From the total of 290 websites surveyed by VECITA in 2007, only 75 websites (26%) publish their privacy policies, the remaining 215 websites are still lack of specific commitments on the collection and use of personal information.

Awareness of Vietnamese people on privacy and personal data protection

- In 2006: the safety and security of personal data was voted No. 3 in the top 7 obstacles to the e-commerce development.
- In 2007: this issue was voted obstacle No 1
- These results show that the public and businesses are concerned and worried about safety and security of their information when involving in e-commerce.

Recent personal data leakage cases

- A case of stealing credit card accounts to buy and sell around 100 air-tickets of Tiger Airways.
- Another case of stealing credit card accounts and use money from these accounts to buy goods through the internet with the amount reaching more than 440 million VND (around 30.000 USD).
- A case involving the posting on the internet intimate footage of a young television actress, which drew the great attention of the general public.

Approaches to enhance personal data protection in Vietnam

- Educating the public and businesses on the issues related to privacy and data protection in e-commece.
- Stepping up the development of domestic approaches to privacy protection:
  - Perfecting the legal framework on data privacy.
  - Developing National Trustmark Organization (TrustVn) with international recognition.

Approaches to enhance personal data protection in Vietnam (cont.)

- Enhancing international cooperation, especially with APEC member economies.
- Actively participate in the APEC's programs and projects on data privacy.

Thank you!

A Japanese Culture of Privacy

Session Ⅰ: The Asian Culture of Privacy

Hiroshi Miyashita
Cabinet Office, Government of Japan

APEC ECSG Data Privacy Seminar
Peru, Lima
February 18, 2008

Topics of A Japanese Culture of Privacy

Cabinet Office

1. Privacy Conceptions in Japan

(1) *What is Privacy?*
(2) *Public Opinion Polls*
(3) *Court Cases*

2. The Japanese Act and its implementation

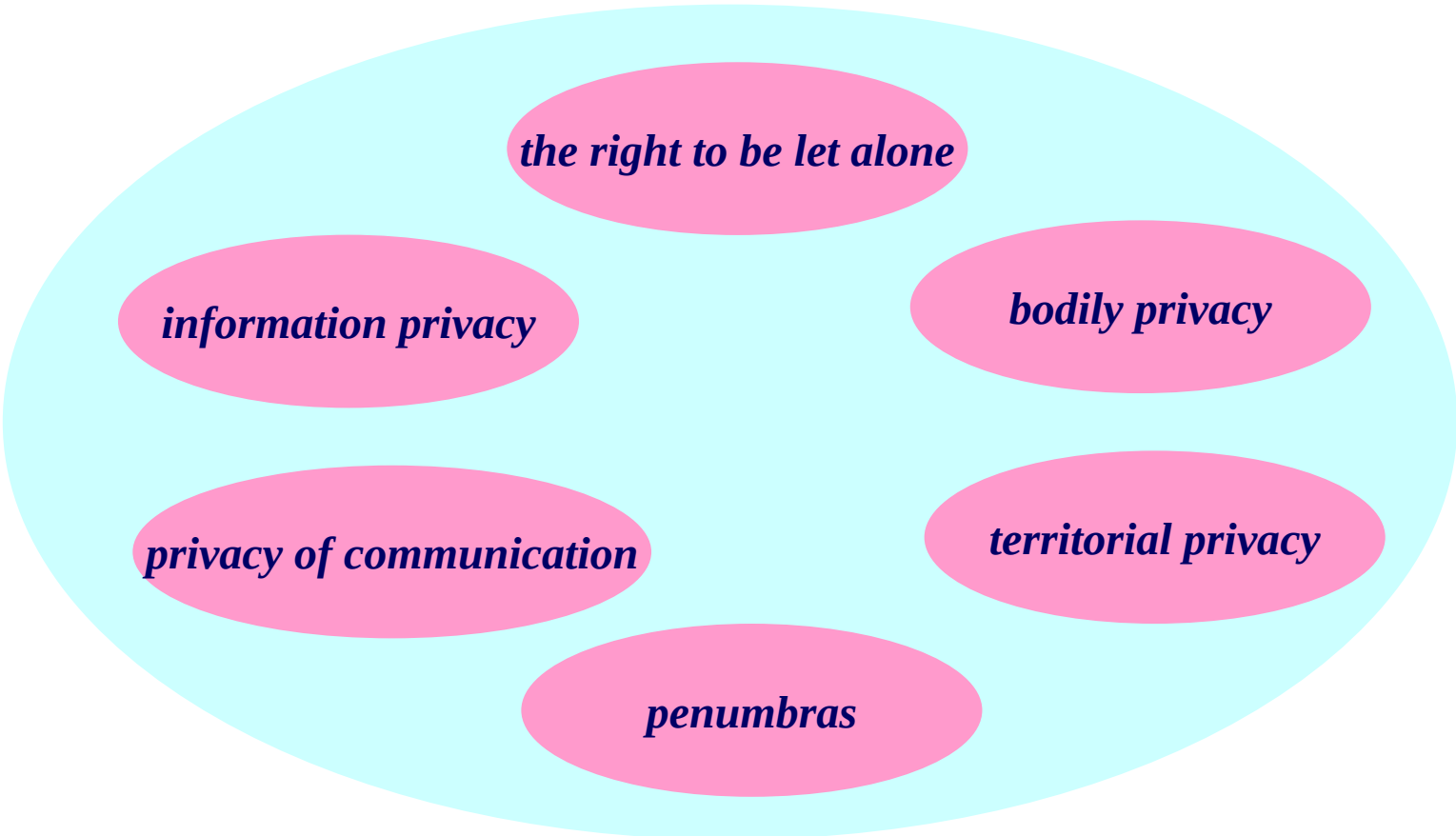
(1) History of Privacy Laws
(2) Outline of the Acts on the Protection of Personal Information
(3) Implementation Status of Act

3. Beyond A Privacy Culture

1. *Privacy Conceptions in Japan*

(1) *What is Privacy?*

Cabinet Office



1. *Privacy Conceptions in Japan*

(1) *What is Privacy?*

Cabinet Office

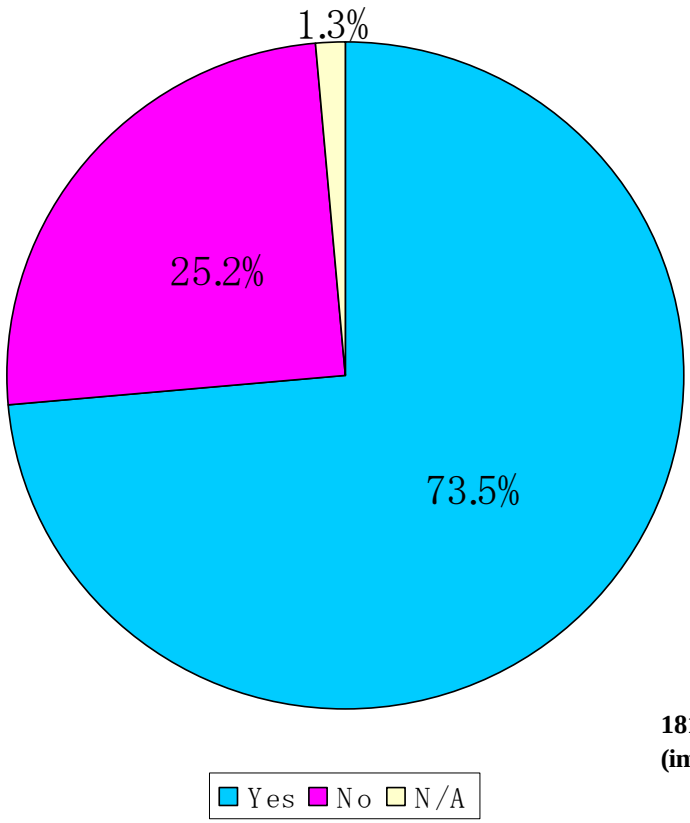
European Privacy	Asian Privacy	American Privacy
dignity	?	liberty values

1. Privacy Conceptions in Japan

(2) *Public Opinion Polls*

Cabinet Office

Interest in Personal Information Protection



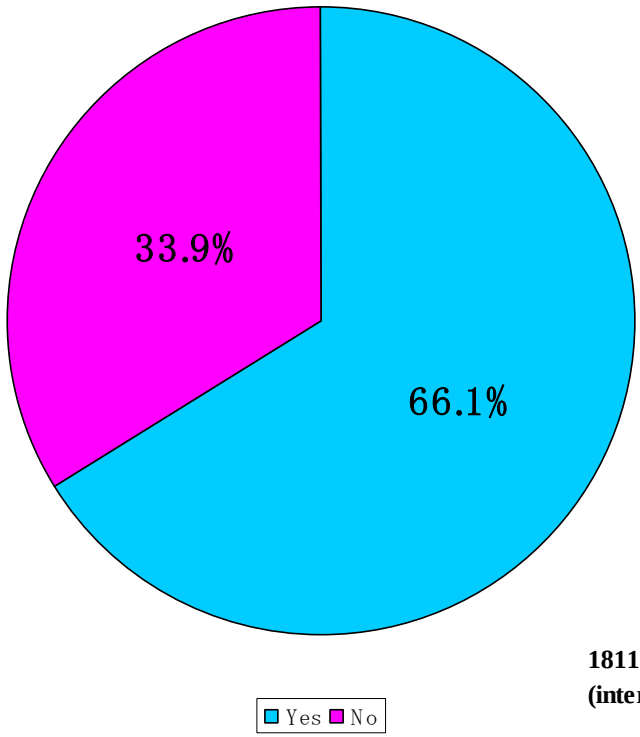
1811 valid answers
(interviewed in Sep. 2006 by Cabinet Office)

1. *Privacy Conceptions in Japan*

(2) *Public Opinion Polls*

Cabinet Office

Knowledge of difference between privacy and personal information



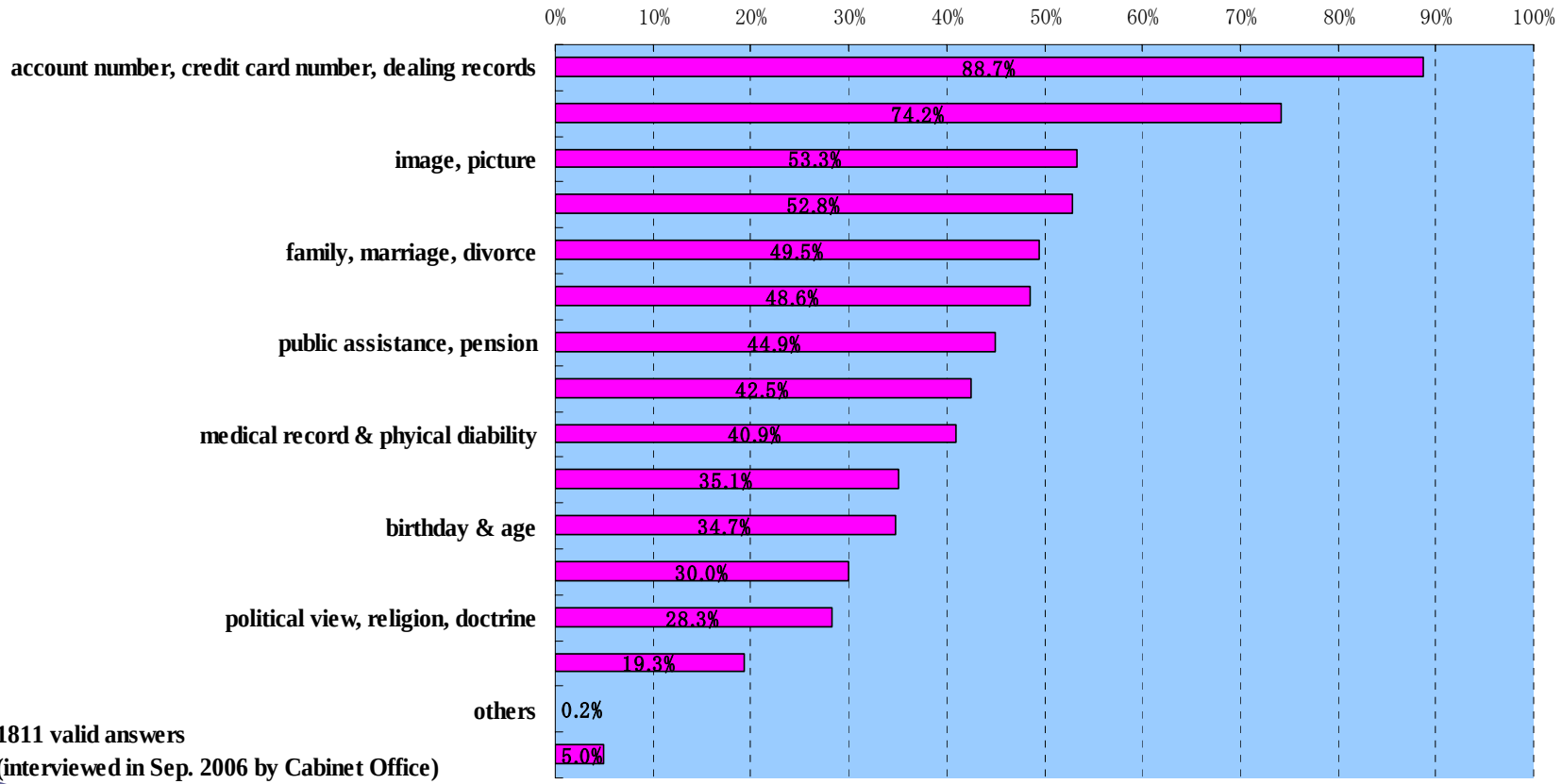
1811 valid answers
(interviewed in Sep. 2006 by Cabinet Office)

1. *Privacy Conceptions in Japan*

(2) *Public Opinion Polls*

Cabinet Office

Personal Infromation which One Does Not Wish to Disclose



1811 valid answers
(interviewed in Sep. 2006 by Cabinet Office)

1. *Privacy Conceptions in Japan*

(3) *Court Cases*

Cabinet Office

● **private life**

"The right to privacy is recognized as the legal protection or the right not to be disclosed of private life"

Utage-no-Ato Case (Tokyo District Court, 1964)

● **personal information**

"It is reasonable that one refuses disclosing such information to others with whom one does not connect, and his or her expectation should be legally protected."

Jiāng Zémín lecture Case (Supreme Court, 2003)

2. Japanese Act and its Implementation

(1) History of Privacy Laws

Cabinet Office

US (1974)
W.Germany(1977)
France (1978)

Canada (1982)
UK (1984)
Japan (1988)
Australia (1988)

New Zealand (1993)
South Korea (1994)
Hong Kong (1995)
Taiwan (1995)
Russia (1995)
Thailand (1998)
Chile (1999)

Peru (2001)

1970 1980 1990 2000

Additional law
Large Amendment

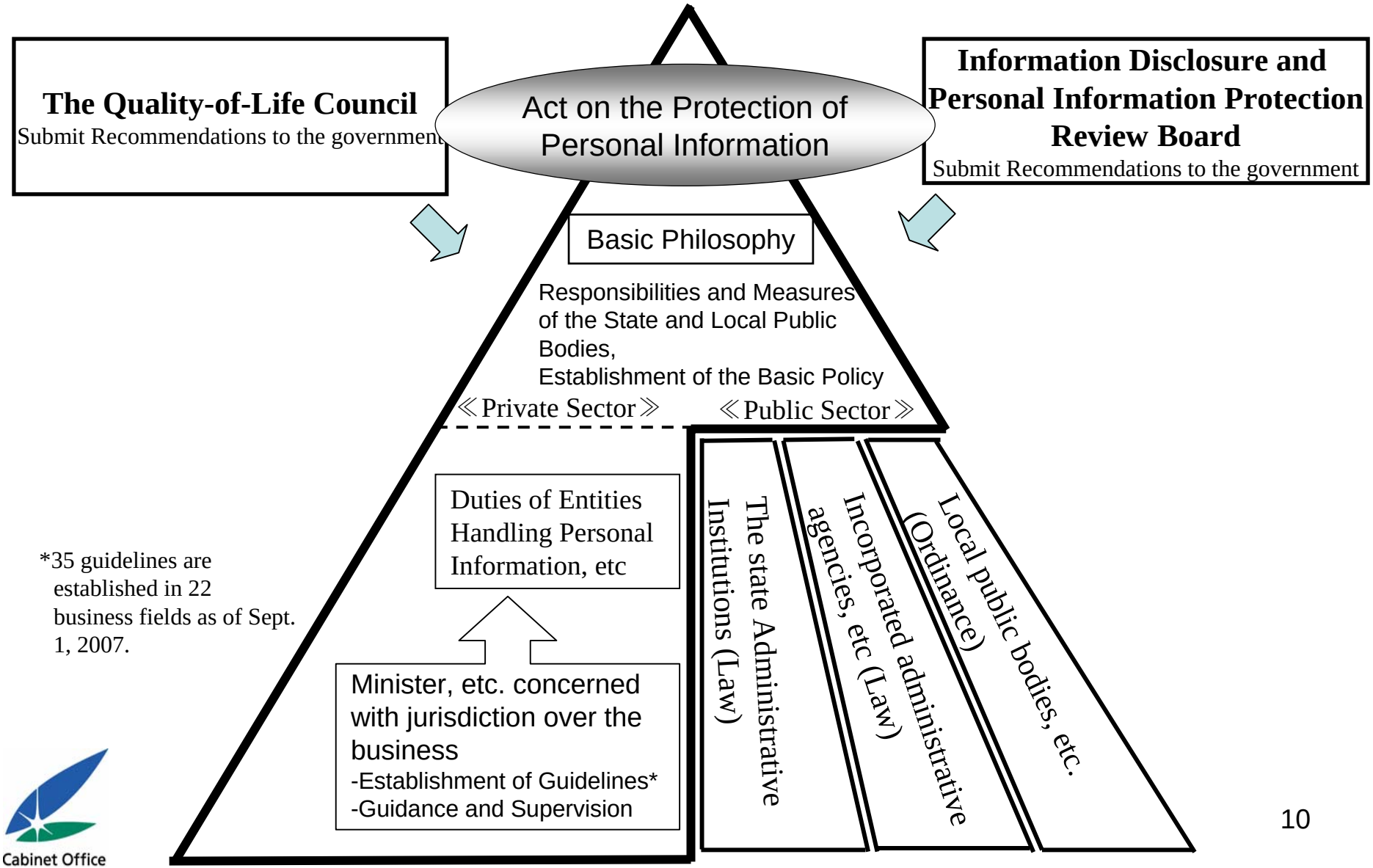
US (1988)

Germany (1990)
UK (1998)

Canada (2000)
Australia (2001)
Japan (2003)
France (2004)

(2) *Outline of the Act on the Protection of Personal Information*

Scheme of the System－Multi-layer Measures & Relevant Sectoral Minister System

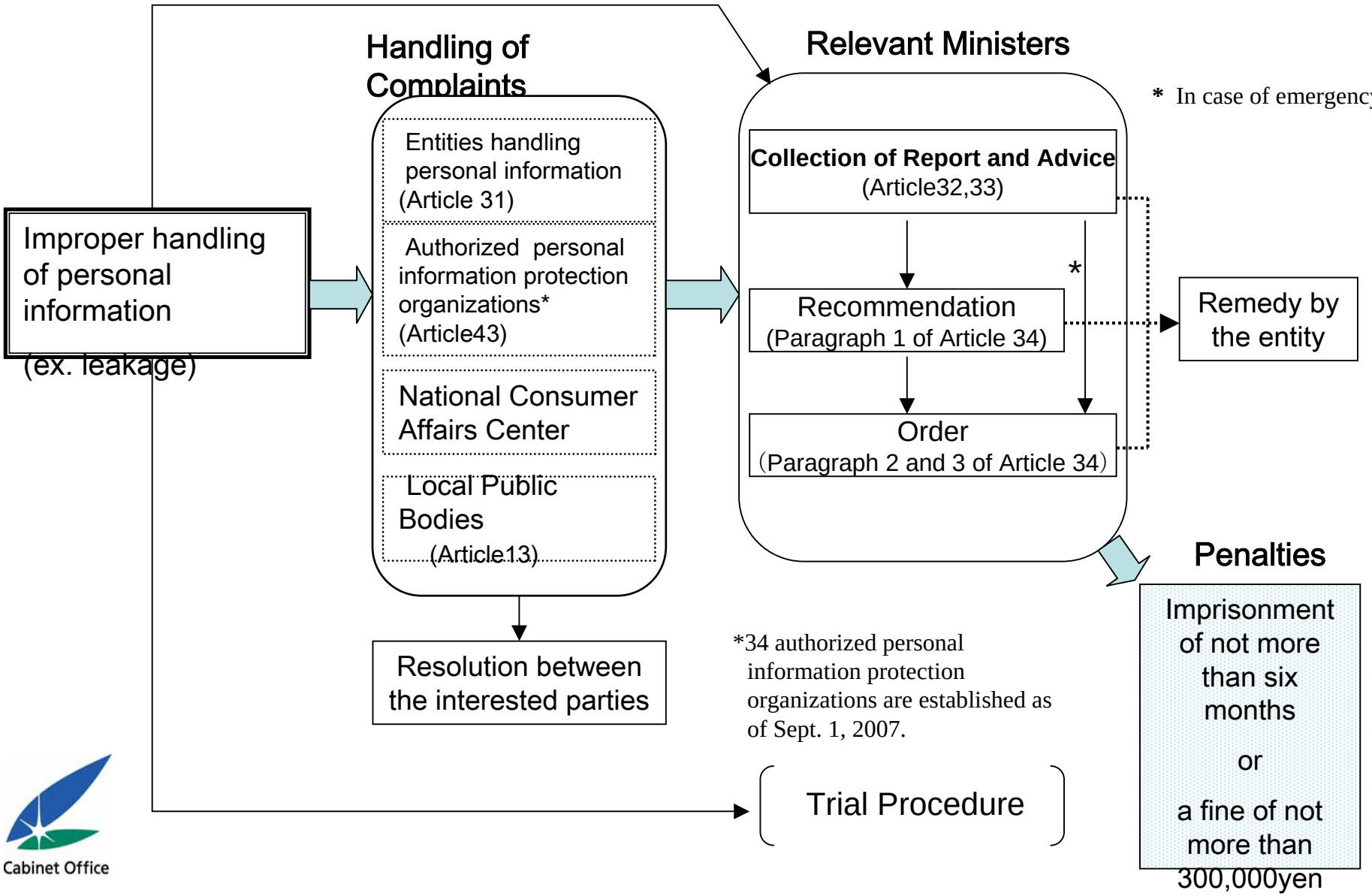


*35 guidelines are established in 22 business fields as of Sept. 1, 2007.

Cabinet Office

(2) *Outline of the Act: Mechanism of Ensuring Effectiveness*

- Autonomous approach; mechanism to encourage the business entities to protect personal information



Cabinet Office

2. Japanese Act and its Implementation
(3) Implementation Status of Act

Cabinet Office

- **893 cases of leakage* made public by entities in FY 2006.**

*Including "loss" or "damage" besides "leakage."

cf.) 1556 cases in FY2005.

- **Many cases relatively small as to number of persons affected by leakage.****

** Referred as "number of leakage-affected persons"

Table Number of Leakage-affected Persons (FY 2006)

	Fiscal 2006	
	Number of Cases	Percentage of Total
500 or less	683	76.5%
501 to 5,000	109	12.2%
5,001 to 50,000	60	6.7%
50,001 or more	36	4.0%
Unknown	5	0.6%
Total	893	100.0%

2. Japanese Act and its Implementation

(3) *Implementation Status of Act*

Cabinet Office

PrivacyMark

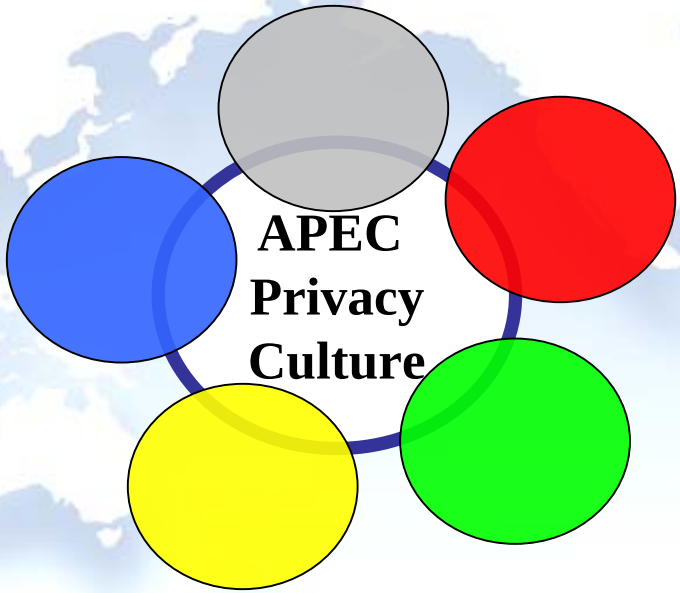
JIPDEC

(Japan Information Processing Development Corporation)

PD Mark

Kanagawa Prefecture

3. Beyond A Privacy Culture



Cabinet Office

INTERNATIONAL SEMINAR
IMPLEMENTATION OF THE GENERAL FRAMEWORK ON PRIVACY
APEC 2008

PERSONAL DATA PROTECTION:

DEVELOPMENT AND PERSPECTIVES IN PERU

Lima, 19 - 20 February 2008

TABLE OF CONTENTS

Part one:

Treatment of personal data and acknowledging the fundamental right to personal data protection. Development and perspectives in Peru.

Part two:

International data transfer and treatment of communication data. New regulatory challenges. State of the matter in Peru.

PART ONE

INFORMATION AND KNOWLEDGE SOCIETY.

Manuel Castells. Information society

- Network society: New social organization.
  The social model changes human relations, organizations and States.
- Information Economy: New Economic Model
  Prevailing of the value of information, knowledge: R+D.
- Information is the core of the New Model. Information is what adds value and support to economic development.
- Context: Economic globalization and economic blocks.

PERSONAL DATA TREATMENT

- Personal data is an asset.
  i.e. Data on patrimonial solvency, communications, and health matters.

- Technological development in the data treatment affects individual rights.

- A legal evolution of the concept of “privacy” is required to limit the personal data treatment.

Interests at stake:

The non regulated use of personal data v. the protection to individual rights.

INFORMATION ON PEOPLE (PERSONAL DATA)

- Can only “private” data be the object of protection?
  What about other type of information / data?

- Development of jurisprudence building the grounds for a new right. (Europe - early 90s)

- A new fundamental and autonomous right is consolidated apart from the right to privacy.

- Right to protection of personal data. Informative self-determination.

- Domestic laws acknowledging this right and setting its general principles are passed.

PERSONAL DATA PROTECTION

- European Community: Directive 95-46/CE on the protection of individuals with respect to personal data treatment and free circulation of this type of data.

- It is regarded as a fundamental right in Europe.

  Charter of fundamental rights of the European Union (2000)

- In Latin America:

  Personal data protection acts have been passed in countries such as Mexico, Argentina and Colombia.

PERSONAL DATA PROTECTION IN LATIN AMERICA

- XIII Ibero-American Summit of Chiefs of State and Government.
  Santa Cruz de la Sierra Declaration (14-15 November, 2003, Bolivia)

  … We are aware that the protection to personal data is a fundamental right of all persons and we highlight the importance of Ibero American regulatory initiatives for protecting the privacy of citizens contained in the La Antigua Declaration, creating the Ibero American Data Protection Network, open to all countries of our community ….

  The Declaration leads to outlining directives aiming at the uniformity of legal criteria for the protection of personal data at an economic block level.

  Evaluate APEC privacy framework for this purpose.

PERSONAL DATA PROTECTION IN PERU

1993 Political Constitution

Article 2°.- Every individual shall have the right to :
6) Expect that information services, whether in IT format or not, public or private, shall not provide information affecting the individual's personal and family privacy.
7) Honor and good reputation, to personal and family privacy, and the their own voice and image.

Article 200º.- Constitutional protection: Constitutional procedure to defend the right to the protection of personal data: Habeas data.

- So far, there is no law for the protection of personal data. This is a comparative disadvantage.
- Free trade agreements contain the need for personal data protection to favor international data transfers.
- There is a bill draft filed by the Ministry of Justice pending approval.

BILL DRAFT TIMELINE

Commission to file the bill draft	**Publication of the draft.**	**Revision of opinions.**	**The project is one of the goals of the development plan of information society in Peru.** **It is a government policy** **www.codesi.gob.pe**
R.M. 094-2002-JUS. **18 March, 2002**	**R.M. 331-2004-JUS.** **23 July, 2004**	**Presentation fora with the Spanish Data Protection Agency.** **May, 2006**	**Pending approval by the Council of Ministers** **January, 2008**

BILL DRAFT ON DATA PROTECTION

- ✓ Acknowledges general principles of personal data protection.
- ✓ General principles are applied to all data treatment.
- ✓ Submission to sectorial legislation.
- ✓ Includes databases of public and private nature.
- ✓ Outlines a summary administrative procedure enabling the owner of the data to exercise his/her rights.
- ✓ Foresees the existence of a National Authority.

- A) European Model: The data protection agency is an independent and autonomous institution.

- B) “Integrative” Model: The data protection agency is part of a national entity. I.e. In Argentina, the National Data Protection Directorate is part of the Ministry of Justice.

- The Peruvian draft adopts the second model: an entity that will be integrated to the Ministry of Justice.

PART TWO

INTERNATIONAL DATA TRANSFER

- Internet and Globalization: International Data Transfer
- Personal Data: *An asset for corporations.*
- Data Protection: A fundamental right

- Balance: *corporate interest and the individual right.*

- Reasons: *Less expensive costs.*

  - Services rendered by the same corporation abroad, labor costs, less demands and liabilities, etc.

  - Centralization of activities and human resources. Telephone marketing actions aiming at measuring customers' satisfaction degree.

  - Maintenance, technical support, management of the database (customers and suppliers).

  - Provision of administrative support services.

- Peru can offer comparative advantages for APEC economies in matters related to international data transfers.

INTERNATIONAL DATA TRANSFERS FROM THE EUROPEAN UNION.

1) Country of Destination with a satisfactory level of protection

Decision to adjust by the European Commission.

EEUU (Safe Harbor) and Canada (Canadian law)

Argentina (adequate level of data protection)

2) Authorization granted by the National Authority for the personal data protection.

Decision by each National Authority.

Fundamental Requirement: provision of accurate guaranties

Clauses between data importers and exporters

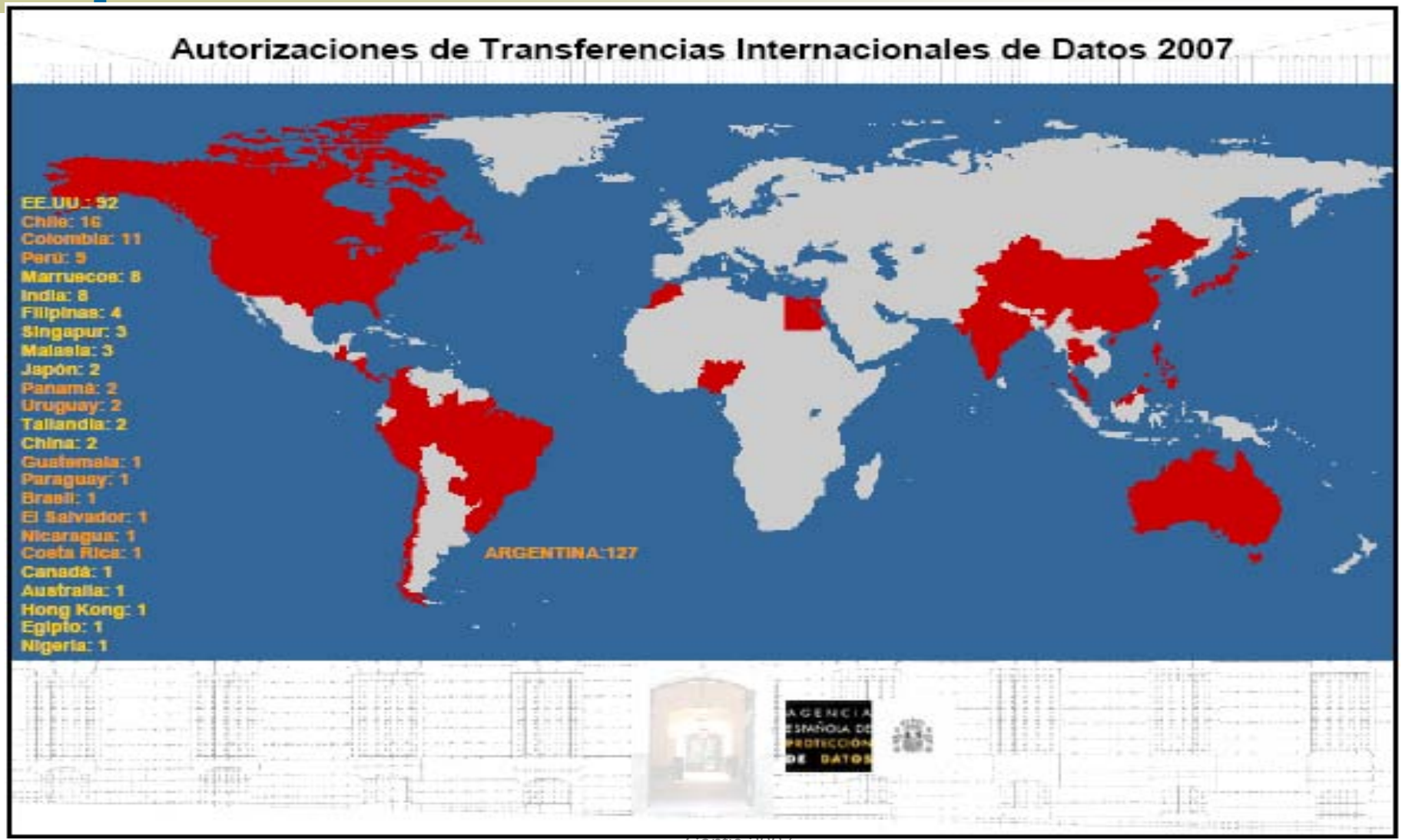
3) Exceptions.

Source: AEPD November 2007

Autorizaciones de Transferencias Internacionales de Datos 6-11-2007

	2000	2001	2002	2003	2004	2005	2006	2007		Total Autoriza-ciones
								Autori-zaciones	Otras solicitudes	
EEUU	1	9	2	6	40	9	16	9	7	92
Marruecos	1	-	-	-	2	2	2	1		8
India	-	-	-	-	4	-	3	1	5	8
Singapur	-	-	-	-	1	-	1	1	1	3
Japón	-	-	-	-	-	1	-	1	1	2
Panamá	-	-	-	-	-	2	-	-	-	2
Colombia	-	-	-	-	-	1	4	6	3	11
Malasia	-	-	-	-	-	1	1	1	-	3
Tailandia	-	-	-	-	-	1	-	1	-	2
Chile	-	-	-	-	-	1	7	8	2	16
Uruguay	-	-	-	-	-	1	1		1	2
Filipinas	-	-	-	-	-	-	3	1		4
Perú	-	-	-	-	-	-	4	5		9
China	-	-	-	-	-	-	1	1	1	2
Hong Kong	-	-	-	-	-	-	1	-	-	1
Guatemala	-	-	-	-	-	-	1	-	-	1
Paraguay							1		1	1
Australia								1	-	1
Brasil								1	-	1
Canadá								1	-	1
Egipto								1	-	1
El Salvador								1	-	1
Nicaragua								1	-	1
Nigeria								1	-	1
Emiratos Árabes								-	1	
Qatar								-	1	
Turquía								-		
Costa Rica								1		1
Túnez									1	
Solicitudes presentadas	2	9	2	19	56	45	54	85		268
Archivadas	-	-	-	13	6	16	17	37		89
En tramitación									20	
Total Autorizaciones	2	9	2	6	47	19		34		165

Source: AEPD November 2007



COMMUNICATIONS DATA

- Communication: information exchanged or handled by means of an electronic communication service.
- Data relating to names, numbers, addresses and general data provided by the sender.
- Traffic Data: Allow to carry out communications through a network such as: route, duration, time, terminal localization, protocol.
- Localization data: Place of the connection, location, tracing and terminal movement.

OBLIGATIONS AND RIGHTS RELATED TO COMMUNICATION DATA

- Forbids any type of intervention, treatment or surveillance of communications and traffic data.
- Imposes more advanced security measures to corporations.
- Users' Rights:
  Caller IDs, rejection of calls, block of the number called, call transfer (from fixed line to mobile line or fixed line to fixed line), not detailed invoicing.
- Restrictions to commercial promotions.
  These should be identified, should not cause a cost for the user and should bear the possibility of rejection by the user.
- Treatment and storing of traffic data only for purposes of invoicing, aggregated services rendered or commercial promotions (previously consented).
- Storing traffic data : Automatic, intermediate and transitory.
- **Europe:** Directive 2002-58/CE Orders confidentiality of communications and data traffic.

PERSONAL DATA PROTECTION
NEW CHALLENGES
WHAT HAPPENED ON SEPTEMBER 11, 2001?

- The States are authorized to adopt measures to limit some aspects of the directive to protect national security (State security, Public Security, Investigation of crimes)

- Measures related to data storage on communications. Appropriate and proportionate for a democratic society.

Interests at stake:

- Authorities: Investigation and fight against organized crime, terrorism. Retain communication data (more data in more time) context: terrorist attacks in Madrid 2004 and the United Kingdom 2005.

- Providers of communication services: Retention should be minimum, for a short period of time and reimburse of costs.

- Individuals: Preserve the effective protection of their fundamental rights (privacy, personal data protection and communications)

NEW LEGISLATION APPLICABLE TO COMMUNICATIONS DATA

Need to modify the legal framework on communications data

Need to preserve:

- Traffic and localization data.
- Data to identify the origin, destination, date, time or duration of a communication.
- Types of communication. Fixed, mobile or internet.

- Storage or retention of communications data would not affect the secrecy of communications. This does not include the content of electronic communications.

- EUROPE: Directive 2006-24/CE. Legal framework on data storage by the providers of electronic communication services.

  Term for preservation. Shall depend on the category of the data (Between six months and two years).

DATA RETENTION ON COMMUNICATIONS: DIRECTIVE 2006-24/CE

Objections to the European framework:

- It does not define the list of crimes that may cause the retention of communication data.
- The storage of communication data is general and it is not connected to a one specific investigation.
- High costs for telecommunication corporations.
- Total surveillance.

Adequate criteria on the treatment of communication data for purposes of criminal investigation among APEC member economies.

COMMUNICATION DATA IN PERU

Ministerial Resolution 622-96-MTC. Inspection procedure related to the secrecy of telecommunications and data protection.

- General prohibition to intercept telecommunications (Secrecy of telecommunications contained in the Constitution).
- Prohibition to deliver personal data provided by users.
- Obligation to inform with regard to all security measures in order to protect the secrecy of telecommunications and data protection.
- Favors the exchange of specific data among companies to improve competition (non reserved data). Resolution Nº 053-2004-CD/OSIPTEL.

OBSERVATION: So far, there has been no development of specific regulation with regard to traffic or localization issues

COMMUNICATION DATA IN PERU

- Directive draft prepared by the Ministry of Transportation and Communication (20 July, 2006)

- Includes, within the personal data protection, traffic and localization data.
- Foresees a demand for security measures.
- Foresees elements for the treatment of traffic data (cases of invoicing and fees between operators)
- Foresees a new scale of fines for infringement
- Includes the obligation to lift the secrecy of communications.

INTERVENTION AND CONTROL OF COMMUNICATIONS

Art. 2 numeral 10 of the Constitution.

Right to the secrecy and communications and private documents.

Communications, telecommunications and documents shall only be opened, captured, intercepted or intervened by express ruling of a Judge.

- Act Nº 27697 (2002) and Legislative Decree Nº 991 (2007).
  Act that grants the Prosecutor the attribution to intervene and control communications.

- Purpose: Regulate the attribution to intervene communications matter of a preliminary or jurisdictional investigation.

- Problem: There is no difference between a procedure to intercept the content of a communication and another to preserve or retain communication data.

- It grants the prosecutor both attributions, but a court order is required. It is not possible for the Prosecutor or the Police to request the retention.

- The operator shall facilitate the intervention.

INTERVENTION AND CONTROL OF COMMUNICATIONS

- In our country, intervention mechanisms may affect the storage of evidence prior to the preliminary investigation of the crime.
- It is possible review mechanisms from APEC economies.
- Retention :
  Decide whether a general retention should be adopted (Europe)
  Specific retention: To be requested by the authority in charge of the investigation (Prosecutor, Police)
- In our country delivery of information and intercepting always by court order.
- Level of liability of communication companies in cases of intervention.
- Crimes that are connected to the purposes of the intervention in communication data.

CRIMES FORESEEN WITHIN THE SCOPE OF THE INTERVENTION OF COMMUNICATIONS IN PERU

- Kidnapping
- Child trafficking. Act 28950. People trafficking
- Child pornography. Act 28950
- Theft
- Extortion Act 28950
- Drug trafficking
- People Trafficking – Immigrants. Act 28950
- Criminal Syndication
- Crimes against human kind
- National Security violations
- Embezzlement
- Corruption of public officials
- Terrorism
- Tax and customs crimes
- Asset laundering. Legislative Decree 991
- *Other crimes, whenever there are enough elements of judgement to enable the belief that the agent is part of a criminal organization.*

THANK YOU FOR YOUR ATTENTION

iferrando@osinerg.gob.pe

alfa - redi

http://alfa-redi.org

Latinamerican Culture of Privacy / Data Protection
What are we talking about?

APEC ECSG Data Privacy Seminar
Lima, Perú
February 19th, 2008

Preliminary Notes

a. Privacy / Data Protection
b. Independent Development / Harmonic Development
c. Information Access / Data Protection
d. Content Access / Don´t care about protection?
e. Privacy against Government Transparency
f. Regulatory Minimum Issues (RMI)

How is it going LAC region?

What have countries achieved?

alfa - redi

Constitutional Level, all the region (San Jose Pact)

Specifical Law Level: Argentina, Chile, Uruguay, Panama

Habeas Data Regulatory Framework Level: Perú, Panama, Brasil, Colombia, Uruguay

SPAM Regulatory Framework: Perú, Chile

Other Law levels: Ecuador, Perú, Venezuela; Mexico, Uruguay, Surinam

How is it going LAC region?

Ongoing efforts

Ongoing Efforts

- eLAC 25 – eLAC 78
- Iberoamerican Data Protection Network
- APEC Framework of Privacy
- Heredia Rulesa

Issue: Working together / Efforts harmonization

One step forward...
eLAC 2007

eLAC 25 – Preliminary Conclusions

See: http://www.cepal.org/socinfo/noticias/noticias/2/32222/GdT_eLAC_meta_25.pdf

Group Goals

The group had as a basic goal to generate rgulatory harmonization tools (not neccesarily harmonized regulations), which allow inter-operation in information society regulation among countries which already have a regulation and to generate regulation for those which don´t.

This is to be understood in a framework of a regional policy strategy on Information Society, where regulatory tools are useful to achieve the development policies goals, regarding ICT components.

Priority Issues

Two main critical issues and two secondary ones. The main ones were Regulation on Privacy and Data Protection in the region and Situation Status on Regulation regarding Cybercrimes in the region.

Secondary critical issues were Digital Signature Use and application for everyday activities of citizens in government environment for e-government; and Legal and Technical Solutions to SPAM.

Personal Data Protection – Principles

- *Principio de Legalidad y Licitud*
- *Principio de Calidad de los Datos de Carácter Personal*
- *Principio de Seguridad*
- *Principio de Nivel de Protección Adecuado*

Personal Data Protection – Control Mechanism

9.1. La garantía del cumplimiento de estas directrices deberá quedar sujeto al control de una o varias autoridades de protección de datos. Las autoridades podrán tener personalidad propia o encontrarse integradas en la Administración Pública o en un Organismo Público preexistente. Igualmente podrán tener como función exclusiva el cumplimiento de las normas de protección de datos o ejercer tal competencia junto con otras atribuidas por su legislación.

La organización territorial del Estado no podrá suponer un obstáculo para que las garantías derivadas de la existencia de la o las autoridades de protección de datos sean reales y efectivas en relación con todos los tratamientos llevados a cabo tanto por el sector público como por el privado.

Personal Data Protection – Control Mechanism

9.2. Las autoridades de protección de datos deberán actuar con plena independencia e imparcialidad, no pudiendo estar sometidas en el ejercicio de sus funciones al mandato de ninguna autoridad pública. Deberán establecerse mecanismos que garanticen la independencia e inamovilidad de las personas a cuyo cargo se encuentre la dirección de dichas autoridades.

9.3 Las autoridades deberá tener como mínimo las siguientes competencias:

- Conocer de las reclamaciones que les sean dirigidas por los ciudadanos, en particular en cuanto al ejercicio de los derechos a los que se refiere el apartado 5 de estas directrices.

- Realizar las averiguaciones e investigaciones que resulten necesarias para el cumplimiento de las directrices, pudiendo acceder a los datos que sean objeto de un tratamiento y recabar toda la información necesaria para el cumplimiento de su misión de control.

- Adoptar las medidas que resulten necesarias para evitar la persistencia en el incumplimiento de las directrices.

Personal Data Protection – Control Mechanism

- *Mantener un registro de los tratamientos llevados a cabo por los sectores público y privado, al que puedan acceder los interesados, a fin de poder ejercer los derechos reconocidos en las presentes directrices. La solicitud de inscripción se realizará mediante modelos simplificados y basados en estándares técnicos, respetando el principio de neutralidad tecnológica, utilizándose siempre que ello sea posible técnicas o medios electrónicos.*
- *Autorizar, cuando sea preciso, las transferencias internacionales de datos a Estados cuya legislación no recoja lo dispuesto en las presentes directrices.*
- *Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.*

Personal Data Protection – Control Mechanism

- *Promover el uso de mecanismos de autorregulación como instrumento complementario de protección de datos personales que: (i) represente un valor añadido en su contenido respecto de lo dispuesto en las leyes, (ii) contenga o esté acompañado de elementos que permitan medir su nivel de eficacia en cuanto al cumplimiento y el grado de protección de los datos personales y (iii) consagre medidas efectivas en caso de su incumplimiento.*
- *Dictaminar los proyectos de disposiciones normativas que puedan afectar al derecho fundamental a la protección de datos personales de los ciudadanos.*
- *Divulgar a los ciudadanos y a los poderes públicos el contenido del derecho fundamental a la protección de datos personales.*
- *Cooperar con las autoridades de protección de datos para el cumplimiento de sus competencias y generar los mecanismos de cooperación bilateral y multilateral para asistirse entre si y prestarse el debido auxilio mutuo cuando se requiera."*

Personal Data Protection – Pending Tasks

Tarea Pendiente 1: Fomento de la implementación de Agencias de Protección de Datos (Argentina es el único país que cuenta con este tipo de organización), de un alto nivel en la estructura gubernamental. Estas oficinas deben velar por la adecuada protección de los datos personales, en relación a su uso, manejo, manipulación, traspaso y/o venta. Asimismo debe implementarse una red regional que coordine los esfuerzos de estas Agencias Nacionales. De esta manera es tarea el desarrollo de manuales operativos y de requisitos mínimos para la implementación de dichas oficinas.

Tarea Pendiente 2: Es necesario establecer los mínimos necesarios para una adecuada Política y Regulación en Protección de Datos Personales en todos los ámbitos sociales: política, religiosa, económica, cultural, médica, judicial (siendo de especial interés para el último caso la adhesión abierta y aplicación de los Reglas de Heredia). Estos mínimos deben servir de sustento al desarrollo de políticas y normas de protección de datos ínter operables a nivel de los países región.

Personal Data Protection – Pending Tasks

Tarea Pendiente 3: Siendo un subtema específico pero que ha desarrollado implicancias comerciales y sociales especiales, la temática del SPAM tiene que ser considerada en el análisis de políticas y normativas, desde las perspectiva técnica, comercial, jurídica y política, siendo una tarea pendiente el establecer un espacio de monitoreo sobre el particular, así como un trabajo en base a la normativa existente y las propuestas que se puedan realizar, para limitar sino eliminar el SPAM.

Another step forward...
eLAC 2010

eLAC 78

See: http://www.elac2007.org.sv/docs/compromisodesansalvador-8feb2008.pdf

Data Protection and Health

Goal 35. Link up national health portals with a view to establishing a regional network that can be used to share experiences, exchange content and promote their development,
adaptation and relevance, taking into account the need for appropriate data protection..

Information Access

Goal 77. Promote the greatest possible access for citizens to public information on a timely basis while respecting cultural, linguistic, disability and other differences in accordance with international standards.

Legal Framework

Goal 78. Renew the mandate of the working group on the information society's legal framework to facilitate dialogue and the coordination of various regulatory initiatives at the regional and local levels that may contribute to the region's regulatory harmonization.

Note: Coordination of this group continues on charge of Peru

alfa - redi

Further information

Erick Iriarte Ahon

eiriarte@alfa-redi.org

Alfa-Redi

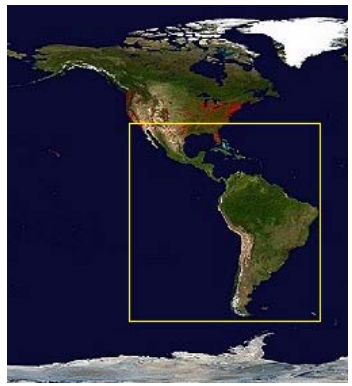
http://www.alfa-redi.org

Asia-Pacific Economic Cooperation

The Latin-American Culture of Privacy

Jorge Navarro, Esq.

Mexico



APEC ECSG Data Privacy Seminar

Peru, Lima

February 18, 2008

ITC Law Consultant

Agenda

I. Privacy & Data Protection - Spanish/European Influence

II. Global Consensus for Privacy and Data Protection Standards

III. Latin-American Economies

IV. Regional Harmonization

V. Challenges

ITC Law Consultant

Asia-Pacific Economic Cooperation

. Prviacy and Data Protection - Spanish/European Influence

- Same cultural roots
- V Centuries-Colonial-Heritage
- Language, Religion & Legal System
- Laws of Indias (1861) - Napoleon Codes
- Civil Wars & Military Regimes – XIX - XX Centuries
- Human Rights – Sensitive concern

ITC Law Consultant

I. Privacy and Data Protection - Spanish/European Influence

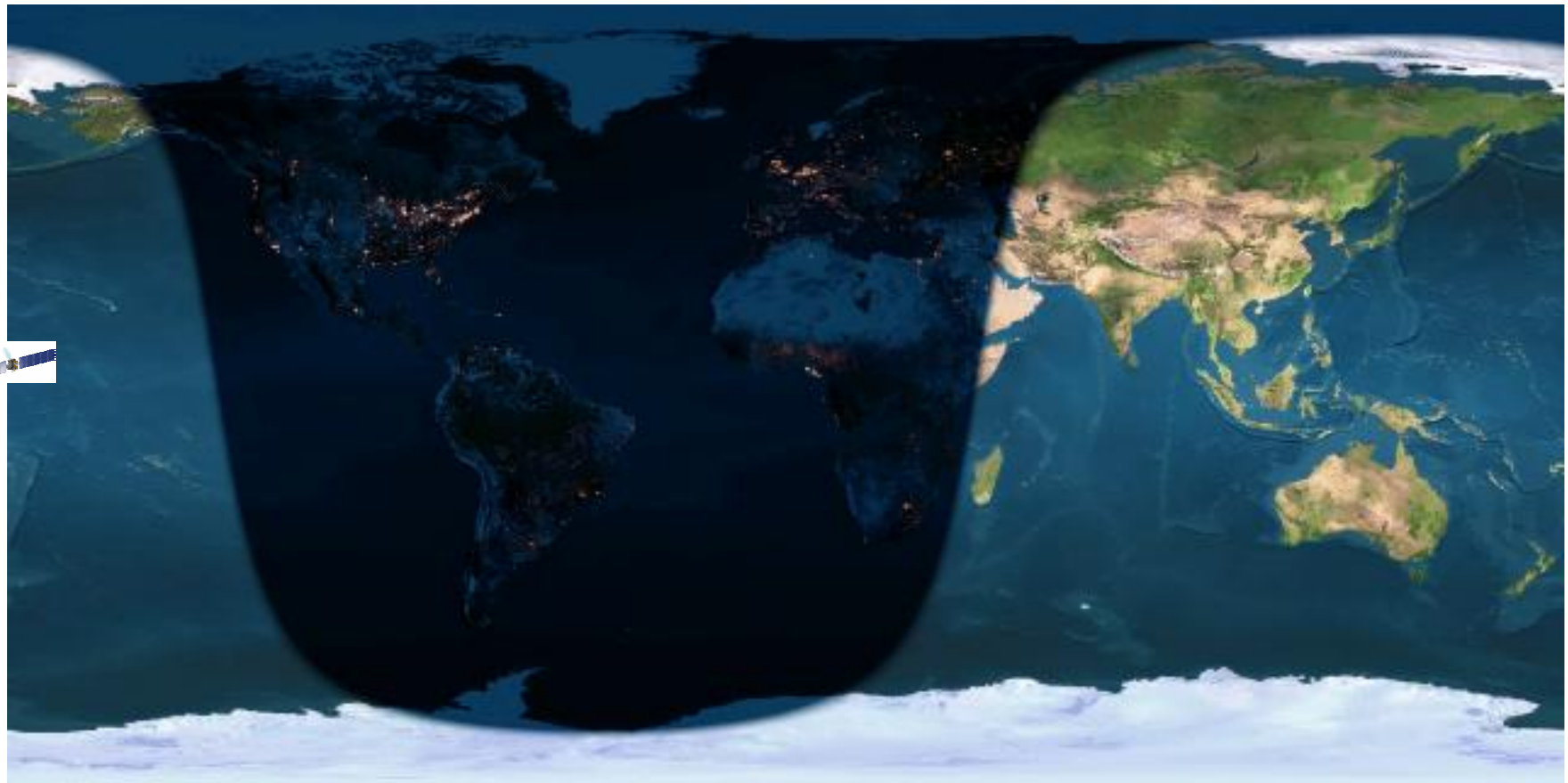
Latin- American Economies

- Similar social and political problems
- Developing economies - poverty
- Democratic systems - transparency
- **Privacy protection** – National Constitution / States - Provinces Constitutions
- Universal Declaration on Human Rights
- International Covenant on Civil and Political Rights
- American Convention on Human Rights

ITC Law Consultant

Asia-Pacific Economic Cooperation

II. Global Consensus for Privacy and Data Protection Standards



Source: www.fourmilab.ch

ITC Law Consultant

II. Global Consensus for Privacy and Data Protection Standards

OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)	Directive 95/46/CE 	APEC Privacy Framework
Collection Limitation	Collection Limitation	Collection Limitation
Data Quality	Data Quality	Integrity of Personal Information
Purpose Specification	Purpose Specification	
Use Limitation	Use Limitation	Uses of Personal Information
Security Safeguards	Security Safeguards	Security Safeguards
Openess	Openess	
Individual Participation (Habeas data)	Individual Participation	Access and Correction
Accountability	Accountability	Accountability

II. Global Consensus for Privacy and Data Protection Standards

OECD Privacy Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)	Directive 95/46/CE 	APEC Privacy Framework
International Data Transfer guaranty if compliance with principles	International transfers only to countries with adequate data protection level – Safe Harbor Unambiguous Consent (Evidence – complex) Databases Registration Opt-in Sanctions for any infringement	Notice (Evidence – T&C) Opt-out Preventing Harm Sanctions in there is a harm
Sanctions and redresses		Choice

Asia-Pacific Economic Cooperation

III. Latin-American Economies

Mexico

- Federal Constitution:

Privacy & Data Protection (Government)

- Sector Laws and diverse authorities
  - Government (G2C - IFAI)
  - Financial Sector (B2B- B2C - CONDUSEF; CNBV)
  - Consumer Protection (B2C - SE/PROFECO)
  - Health Sector (G2C - SS)
  - Telecommunications Sector (SCT/Cofetel – B2B-B2C)

- 32 States – Constitution and local laws

- Colima
- Jalisco
- Tlaxcala
- Federal District

III. Latin-American Economies
Mexico

- Privacy - evolving concept – Administrative and Judicial Courts

  - Supreme Court of Justice of the Nation/Amparo 402/2007

  "Private life is understood to be that part of human life that happens in view of few people or which is the personal and particular life."

- **Not an absolute concept** and must be defined over a case to case basis and it challenges other principles:
  - Freedom of speech
  - Transparency and access to information
  - Public interest
  - Fight against terrorism
  - Public security
  - Market development

- Public Sector and Private Sector relationships to enhance privacy and data protection
  - IFAI – Privacy Subgroup – Draft Project – 2 years
  - **Ministry of Economy** - AMIPCI Trust Mark

ITC Law Consultant

III. Latin-American Economies

Mexico

AMIPCI Trust Mark

- Released in February 2007; **Self regulatory scheme** supported by the Ministry of Economy and the Office of the Attorney General for Consumer Protection.

- The Trust Mark seeks to **enhance security** of e-commerce transactions and represents an acknowledgment that institutions and business adhering to AMIPCI´s Trust Mark:

  i) are **legally established** in Mexico

  ii) their **websites are trustworthy** and ethical responsible

  iii) **comply** with provision on protection of personal data contained in the **Federal Consumer Protection Act**, as well as with the privacy and information principles of **APEC´s Privacy Framework**

  iv) **Memorandum of Understanding** with ATA – **Asia Trust Mark Alliance**

  Thailand Department of Business Development, Ministry of Commerce; Korea Institute for Electronic Commerce; Consumers Association of Singapore; Commercenet Singapore Limited; Secure Online Shopping Association; Trusted Universal Standards in Electronic Transactions, Inc.; Ec network; Tradesafe Inc.

  iv) **ALADI-UNCTAD** support as a basis for a regional Trust Mark for Latin-America.

ITC Law Consultant

III. Latin-American Economies

- Chile
- Constitutional right
- Law No. 19,628 for the Protection of Private Life

  - Omnibus Law (1999)

- No special data protection authority

- Peru
- Constitutional right
  - Art. 2. 6) – Data Protection
- Constitutional Court - recognizes the self informative determination right as a relational right different than privacy and self image rights.
- Data Protection Law – Draft
- Omnibus law

Asia-Pacific Economic Cooperation

IV. Regional Harmonization

- APEC
- Data Protection Ibero-American Network
- Security and Prosperity Partnership of North America – SSP
- ALADI
- Mercosur

IV. Regional Harmonization

APEC

- Australia
- Brunei Darussalam
- Canada
- **Chile**
- People's Republic of China
- Hong Kong, China
- Indonesia
- Japan
- Republic of Korea
- Malaysia
- **Mexico**
- New Zealand
- Papua New Guinea
- **Peru**
- The Republic of the Philippines
- The Russian Federation
- Singapore
- Chinese Taipei
- Thailand
- United States of America
- Viet Nam

Asia-Pacific Economic Cooperation

IV. Regional Harmonization

Data Protection Ibero-American Network

Data protection authorities of

- Argentina
- Brazil
- **Chile**
- Colombia
- Costa Rica
- El Salvador
- Guatemala
- **Mexico**
- Nicaragua
- **Peru**
- Portugal
- Spain

- Directives to Harmonize Data Protection in the Ibero-America Community
- Seminario de Cartagena de Indias, Colombia, May 2007
- OCDE
- UN-Resolution 45/95
- Directive 95/46 EC – European Model
- Resolution 4/2002, Argentina adequate level on data protection legislation

Asia-Pacific Economic Cooperation

IV. Regional Harmonization

Data Protection Ibero-American Network

- Economic Partnership, Political Coordination and Cooperation Agreement of the European Community and its Member States and Mexico

  – Article 41.- Both parties " agree to **cooperate** on the protection of personal data in order to **improve the level of protection** and **avoid obstacles to trade** that requires transfers of personal data. Cooperation on personal data protection may include technical assistance in the form of exchange of information and experts and the establishment of join programs and projects."

- **BPO Services** and **Call Center industry** – concerns about the regulatory burden if domestic legislation adopts the European Model.

IV. Regional Harmonization

Security and Prosperity Partnership of North America – SSP
Canada - USA - Mexico

- North American Free Trade Agreement – NAFTA (1994)
- Article 904 Section 4 of NAFTA-

  "No Party may prepare, adopt, maintain or apply any standards-related measure with a view to or with the effect of creating unnecessary obstacle to trade between Parties".

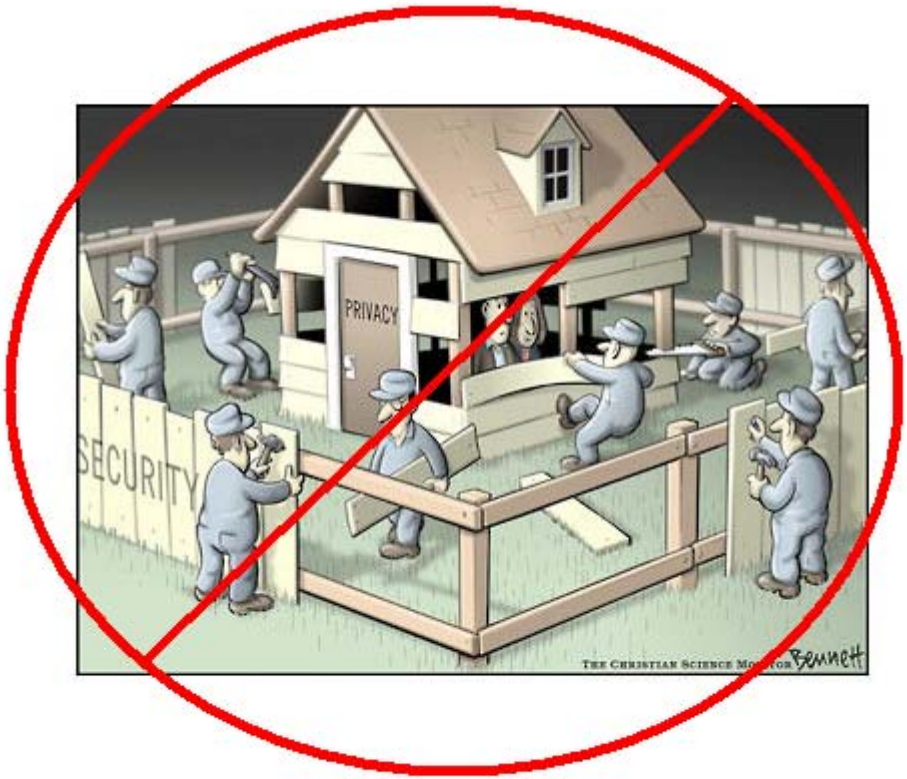
- Framework of Common Principles for Electronic Commerce (2005)
- Statement on the Free Flow of Information and Trade in North America
  - Parties agree that all possible steps should be taken to ensure that electronic information flows freely in support of a growing and efficient North American market, within a framework of security and privacy protection.
- Trilateral Sub-group on Transborder Data Flows.

Asia-Pacific Economic Cooperation

IV. Regional Harmonization

Security and Prosperity Partnership of North America – SSP

Canada - USA - Mexico



ITC Law Consultant

Asia-Pacific Economic Cooperation

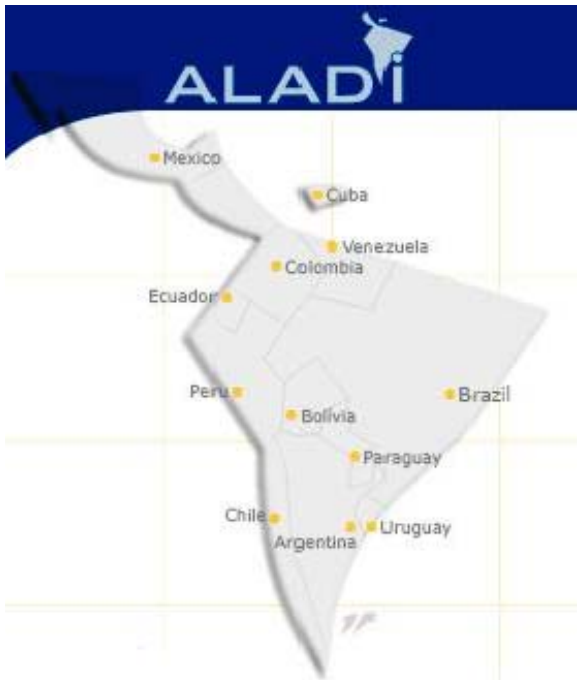
IV. Regional Harmonization

Security and Prosperity Partnership of North America – SSP
Canada - USA – Mexico

- Mexican exports to USA - $ 210,799 million dollars – **85%**
- Mexican exports to Canada $17,000 million dollars -5%
- Mexican exports to Europe $16,000 million dollars - 4%
- Mexican exports to Asia, Australia, New Zealand, Africa – 6%
- Canada exports to US $562,000 million dollars – 1st USA partner
- China exports to US $386,000 million dollars – 2nd USA partner
- Mexico – 3rd commercial partner
- Latin American Countries – not including Mexico – joint exports to USA $142,300 million dollars

Asia-Pacific Economic Cooperation

IV. Regional Harmonization



UNCTAD

United Nations Conference for Trade and Development

ALADI

Latin-American Integration Association

MERCOSUR

South Common Market

- Promotion of a Regional Trust Mark in Latin-America

ITC Law Consultant

Asia-Pacific Economic Cooperation

V. Challenges

- Regulatory Harmonization
    - International – APEC – Privacy Pathfinder
      - EU - Safe Harbor Agreements
    - Regional – ASEAN - Association of Southeast Asian Nations
    - Bilateral-Trilateral -National level – Federal; Provincial and States
- Promotion of Self Regulatory regimes – Regional Trust Marks
- Capacity building – Authorities, industry, legislators, courts.
- Inclusive law making process – Effective dialogue with Industry and competent authorities.
- Adequate inter-government agencies strategy to include main actors to reform laws or establish adequate regulations.
- Budget – Priority which is not included in budget – is not a priority!
- Political issues – federal vs. province/state autonomy.

Asia-Pacific
Economic Cooperation

Thank you!

Jorge Navarro, Esq.

ITC- Law Consultant

jnavarro@msda.com.mx

Tel. + (521) 55 5102 5244
+ (52) (55) 5595 4870

LATIN AMERICAN CULTURE OF PRIVACY

In México, there is no law on privacy or data protection

However there are several regulations aimed to protect private life -personal data information:
Constitution, Civil Codes, Banking and Tax laws, Intellectual Property law, Consumer Protection Law (Robinson Lists) and others.

Since 2002, the Federal Freedom of Information Act (FOIA) also protects personal data collected by government, and guarantees the related treatment, including access by individuals and the possibility to replace, rectify, complete or correct such information (habeas data).

Who is subject to Mexican FOIA?

Only the Federal public sector which has the most important data bases in the country
Executive -agencies-,
Legislative and Judicial branches, and
Autonomous entities created by Constitution

Purpose of Mexican FOIA

- *To guarantee the protection of personal data and to create a culture concerning its treatment*

- *To give access to personal data including the possibility to correct such information*

What is the Federal Institute of Access to Information (IFAI)

- It is the authority for the interpretation and application of FOIA -regulator of 5 commissioners-, whose competence is exclusively the Executive Branch

- More than 240 Federal public agencies

- IFAI has authority to make them comply with the law – regulation, supervision and dispute resolution-

IFAI's tasks

- Solves appeals presented by individuals when the required information – public or personal data- is not obtained from Federal public agencies
- Guarantees access to personal data, including the possibility to replace, rectify, complete or correct such information (habeas data)
- Enacts, implements and supervises regulations related to personal data protection
- Reports compliance and recommends actions to improve and correct practices; to sanction, IFAI works with to the Public Function Ministry

What type of personal data does the Mexican Government posses?

- Information related to the compliance of laws and regulations: tax collection, population census, permits, authorizations, subsidies and credits.

- Also, health, financial, education and social assistance services, among others.

Data bases in the Executive Branch

- There are **2,275** different personal data bases in possession of the Federal public agencies of the Executive Branch.

- The law requires to maintain an active list of all personal data bases which can be consulted in *"sistema persona"* by individuals in order to allow them to exercise their right to access personal data.

Main individual concerns under FOIA

- Individual requests to access their personal data: 30,611 (December 31st, 2007)

- IFAI has ruled **1,221** cases related to personal data, such as rectification of data, access to their own medical records, education and social assistance services.

- Requests and appeals have no cost.

Disputes resolutions and complaints

- Appeals concerning personal data are presented and solved by IFAI in 3 months maximun.

- IFAI supervises the compliance of regulation and rulings concerning personal data access, protection and security measures.

- Public servants that do not comply with IFAI's regulations or rulings, shall be subject to administrative, civil and/or criminal sanctions by the Public Function Ministry.

Constitutional amendments article 6

- Article 6 regulates the right of access to information in the government and includes the need to protect personal data

- The amendments to actual FOIA include a new chapter on data protection that foresees (access, rectification, cancel and objection rights) and international data transfers, national security and police data bases, etc.

Constitutional amendments still pending…

- Article 16, section II, recognizes data protection as a fundamental right and includes the right to access, rectify, cancel and object.

- Article 73 enables Congress to issue a law to regulate personal data protection in the private sector (only one national regulation for all federal states)

Constitutional amendments still pending…

- Congress is to decide if IFAI will be the authority in this regard; therefore, a new entity may be created for that purpose; given the experience, IFAI will be there to help in either way.

There is not an extended privacy culture

- Indivudual concerns about privacy have focused on telemarketing phone calls, and consumer's protection authority PROFECO have launched Robinson's lists.

- Commercial sector has given a step forward in order to protect their clients (trust marks-codes of ethics-privacy policies)

Opportunities...

- We have an opportunity to build a comprehensive privacy framewoork based on best practices around the world.

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

Outsourcing and Accountability

Martin Abrams
February 2008

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

Center For Information Policy Leadership & Hunton & Williams LLP

- Center is a think tank that develops balanced solutions to challenges presented to businesses in an information age
- Maintaining accountability in data flows between countries and regions is one of those challenges
- The outsourcing group at Hunton & Williams LLP represents many companies that outsource business processes

Outsourcing Transactions

- Very tough negotiations between outsourcer and vendor
- Define how risk is transferred
- Often we talk about this in terms of transfer of liability
- The actual issue is accountability

Liability and Accountability

- Liability: The state of being obligated according to law (or contract)
- Accountability: An obligation or willingness to accept responsibility or account for one's actions
- An organization may transfer liability – but never accountability

Basis in Law and Standards

- 1980 OECD Privacy Guidelines
  - Principle 8
- APEC Privacy Framework
  - Principle 9
- U.S. Safeguards rule
- Expansion to most US business via Section 5 FTC Act
- Canadian Federal Privacy Law

May 2004 Letter

FTC Chairman Muris to Congressman Ed Markey:

"....A company that is subject to U.S. laws is responsible for the use and maintenance of consumer information in accordance with those laws. Simply because a company chooses to outsource some of its data processing to a domestic or offshore service provider does not allow that company to escape liability for any failure to safeguard the information adequately."

APEC Privacy Framework Principle 9

"A personal information controller should be accountable for complying with the measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

Attributes An Outsourcer Should Be Looking For

- Vendor
  - An understanding of how to program the appropriate security safeguards and limitations on information use
  - A capacity to do so
  - The character to follow-through
- Economy
  - A legal structure that facilitates contracts being honored
  - An ability to hold employees accountable for their actions
  - Participation in global governance

Cross Border Privacy Rules

- Specifically referenced in the APEC Privacy Framework
- A self assertion that a company should be free to transfer information based on its ability and willingness to be accountable
  - Agreement to carry forward local requirements and promises made in the notice
- The company would match its policies to the principles using a guidance document
- Outsourcer – CBPRs create confidence that accountability is in place
- Vendor – CBPRs create confidence in the capacity and character to follow through

Summary

- A company may transfer the processing and the data may be processed offshore
- But organizations will be held accountable if there is a security or privacy breach
- Therefore:
  - Companies should do what is necessary to assure one's service provider is capable of maintaining promised standards
  - To be competitive a vendor and an economy must demonstrate the understanding, capacity, and willingness to meet the APEC standards

I Can Be Reached

➔mabrams@hunton.com

➔972.781.6667

Outsourcing:
A Citizen/Consumer Perspective

Philippa Lawson, Director
Canadian Internet Policy and Public Interest Clinic
University of Ottawa, Faculty of Law
Ottawa, Canada
www.cippic.ca

Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 2008
Lima, Peru
Feb.19 & 20, 2008

uOttawa
L'Université canadienne
Canada's university

Consumer Concerns

- vulnerability to unauthorized access
  - by ID thieves, fraudsters, org'd crime, disgruntled ee's
    - inadequate security
    - increased risk as a result of transfer
  - by foreign government agencies
    - foreign state surveillance activities
    - inadequate privacy laws
- secondary uses and disclosures
  - by foreign government agencies
  - by other businesses for their own purposes
    - inadequate privacy laws

Protecting Outsourced Data

- From unauthorized access:
  - Minimize amount/type of data transferred
  - Minimize retention of data by vendor
  - Encrypt, anonymize or pseudonymize data
  - Ensure technical security safeguards
  - Ensure business process/employee safeguards
- From fraudulent use:
  - security breach notification
- From secondary uses/new purposes
  - ensure informed consent (or don't do it)
- From foreign government surveillance
  - avoid jurisdictions that lack due process guarantees

Canadian Consumer Concerns

National survey - March 2006

- Transfer of personal data across borders:
  - B2B (customer data)
  - G2B (citizen data – outsourcing to USA)
  - G2G (“to protect national security”)
- Questions:
  - How concerned would you be if…?
  - How important is it for you to be notified?
  - How important is it that the individual’s consent be required (B2B transfers only)?

Canadian Consumer Concerns

CdnCo transfers customer data to ForeignCo:

- Level of concern:
  - 65% - high
  - 32% - moderate
  - 6% - low
- Customers should be notified:
  - 75% - very important
  - 5% - not important
- Customer consent should be required:
  - 84% - very important
  - 2% - not important

Canadian Consumer Concerns

CdnGov transfers customer data to ForeignCo:

- Level of concern:
  - 65% - high
  - 28% - moderate
  - 6% - low
- Customers should be notified:
  - 72% - very important
  - 6% - not important

Canadian Consumer Concerns

CdnGov transfers customer data to ForeignGov "to protect national security":

- Level of concern:
  - 51% - high
  - 36% - moderate
  - 11% - low

- Customers should be notified:
  - 70% - very important
  - 8% - not important

International Consumer Concerns

- 2006 International Survey
  - Canada, USA, Mexico, Brazil, France, Spain, Hungary
  - Ispos-Reid, for Queen's University Surveillance Project

Q: "Is it appropriate for companies to share or sell customer data with third parties such as:
  - foreign governments?"
    - 39%-53%: No (never)
    - 19%-25%: Yes, with express consent
    - 19%-27%: Yes, if customer suspected of wrongdoing
    - 4%-12%: Yes, under all circumstances

“Country Risk”

- Citizens/consumers don’t want their data made available to foreign governments with less oversight/due process:
  - Cdn complaints to Privacy Commissioner:
    - bank, ISP outsourcing to USA
    - SWIFT
  - when given choice, many opt out of foreign outsourcing
    - Cdn security system provider
  - BC govt, Cdn census outsourcing issues

Cdn. Legislative Response

- Some Cdn laws amended to “block” disclosures of citizen data to foreign govts without Cdn govt authorization:
  - if govt outsourcing to foreign-based vendor:
    - data must be housed in and accessed from Canada
    - no disclosure in response to foreign ct orders/subpoenas
    - notice of any such requests
    - substantial fines for non-compliance
    - whistleblower protection

Responsibility of Outsourcers

- Canadian law:

  "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

Responsibility of Outsourcers

APEC IX. Accountability

A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Comparison: Responsibility

– responsibility/due diligence obligation applies to all outsourcing orgs in Canada

– under APEC, outsourcing orgs may choose to rely on consent instead of taking responsibility for the data
  - meaningfulness of consent?

Comparison: “Country Risk”

- PIPEDA:
  - requires “a comparable level of protection”; doesn’t exclude protection from foreign govt access under foreign laws
- APEC:

  “in cases where disclosures are required by domestic law, the personal information controller would be relieved of any due diligence or consent obligations”

Notice of Foreign Outsourcing

- Canadian law:

  "An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information."

  - outsourcing orgs must notify customers of foreign outsourcing (but consent not required)
- Quebec privacy law:
  - data collector must inform individual of location where personal data is being kept

- APEC:
  - no notice of foreign outsourcing required

Data Minimization

- Canada:
  - collect only what is necessary
  - retain only as long as necessary
- APEC:
  - collect only what is relevant
  - no rule limiting retention

Breach Notification

- Security Breach Notification laws:
  - must notify affected individuals in case of security breach exposing personal data
    - most US states
    - being considered in Canada
    - arguably required under APEC “Preventing Harm” principle
- Dual purpose of law:
  - creates stronger incentives for effective security + data minimization (esp. if via public registry)
  - allows affected individuals to take mitigating action

Consumer Risk Management

- Consumers should be able to select service providers based in part on exposure to foreign "country risk" + on record of data security
  - notice of foreign outsourcing
  - public notice of security breaches

- Consumers should be able to prevent ID fraud by taking action when their data is exposed
  - individual notice of data security breaches

Enforceability

- Consumers should be able to enforce data privacy laws and commitments against:

  (a) companies whose data processors fail to protect customer data, and/or

  (b) data processors who fail to protect the data.

  – Adequacy of trustmark schemes in providing consumer remedies?

www.cippic.ca

Processing, Privacy and Progress in India

Joseph Alhadeff
VP Global Public Policy
Chief Privacy Officer

APEC 2008 – Lima, Peru

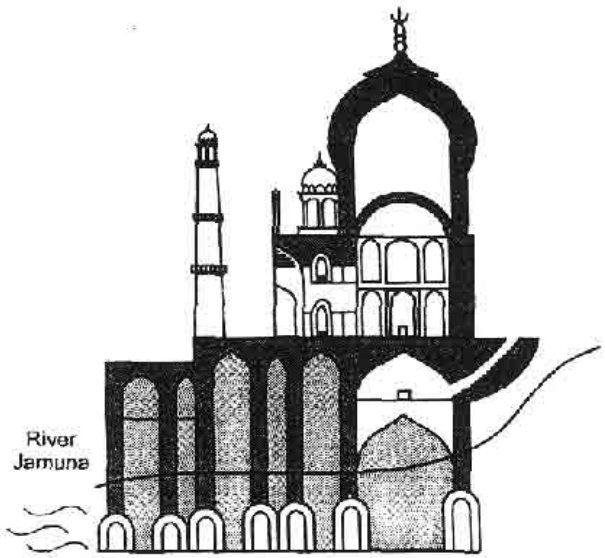
The Current Context: Perception and Reality

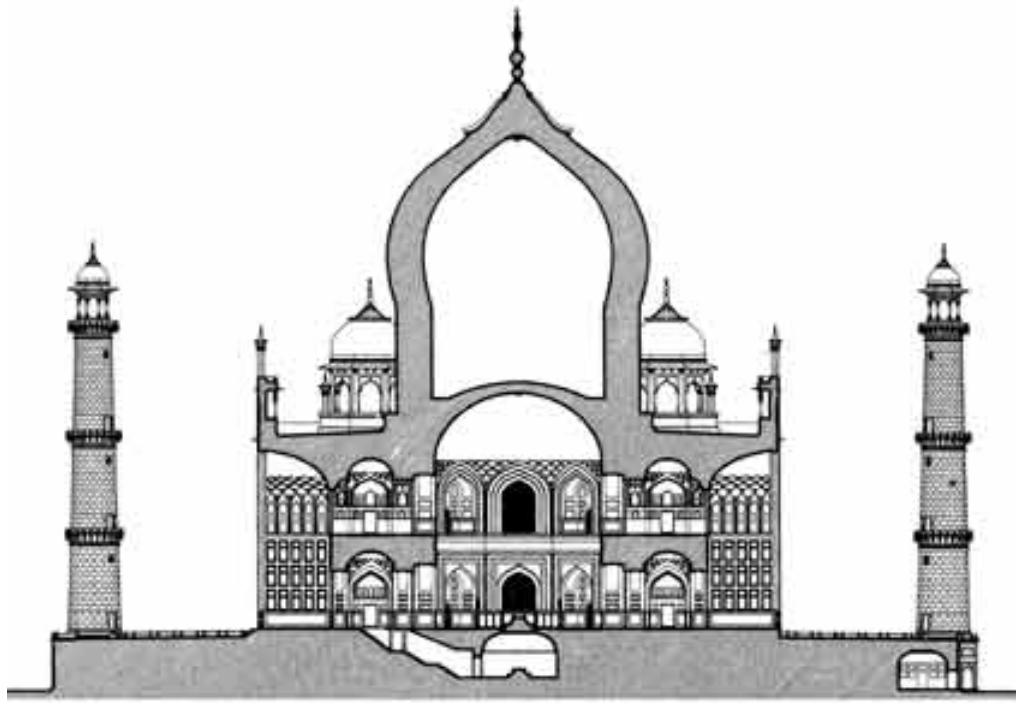
- Increased public concern over ID theft, privacy and security as they relate to personal data
- India is not immune from breaches
- Lack of consumer/legislator familiarity with the Indian legal system and technology companies.
- The “over there” and “them” factors
- Relative quality of processor/call center job
- More Indian companies are ISO 17799 certified than North American companies
- Good track record of breach remediation
- Established practices related to contracts date back to 1870’s

What are local drivers

- Maintain and increase India's reputation as on the cutting edge of IT
- Genuine concerns over BPO data and possible foreign misperceptions about commitment
- Continued growth and investment in the Indian IT and Services sector
- Concern is shared by public and private
- How to tailor a solution that meet both Indian and foreign needs

Architecture Elements





Risk Management. Privacy and Security in a BPO Context

- Contracts
  - Chain of accountability
  - Uses – privacy limits
  - Security – levels, technology…
  - Jurisdiction – where litigated
- Business Confidence
  - Practices & Policies
  - Local assistance
  - Credible response
- Enforcement
  - Investigatory resources
  - Legal/Judicial expertise
- Local law
  - enforcement of obligations/contracts
  - injunctive relief
  - prosecution of offences

Concepts for Privacy Approaches

- Consistent with need for and benefits of global information flows
- Protection as appropriate to type and use of information – business directory, for instance
- Private sector role
  - Innovative policy instruments and mechanisms
  - Recognition of value of private sector bodies, mediation/dispute resolution
- Flexible approach across different legal frameworks
- Cooperation in cross-border transfer and responsibility
  - Not adequacy, but accountability

Process Steps:

- Focus on rationale and objective
- Review existing laws and processes (including Contract Law and other related laws and processes)
- Review current state of the data processing and global sourcing industry re: privacy and security
- Gap analysis to relevant international instruments and norms considering all compliance vehicles
- Selective amendment / revision of existing laws and processes as needed to achieve objectives
- The need for more, better and targeted information to address gaps in perception

Contracting Paradigms

- Information flows are governed by contract
  - With large players, jurisdiction is in home country
  - Concerns arise over downstream players and supporting organizations
- What relief is available under Indian law?
  - IT Act
  - Contracts Law
  - Penal Code
  - Consumer Protection Act

Current Solution Framework

- Focus is on transborder information flows
- Provide appropriate security
  - Better specification of actionable offenses
  - Credible remedies
- Empower incident investigation
- Raise the level of practice
  - Cooperation with the Private Sector
  - Capacity Building

Supporting Elements

- Data Security Council of India (DSCI)
  - Initial focus on promoting a culture of privacy and security through education and outreach.
  - Evolve from capacity building to certification and compliance
- Develop ways of defining appropriate roles for business and government and enhancing cooperation
- Training of police investigators and legal professionals (judges, prosecutors…)
- Developing voluntary IT employee registration and reference system – to better clear backgrounds and facilitate streamlined employment processes (win/win)

The End Game…

- Exploring the thought-leadership role that India could play building on its long-established legal frameworks, cutting edge technology players, entrepreneurial expertise and increasingly important role in global data transfers
  - The are looking at the APEC model to help guide their process
  - APEC may wish to consider whether there are ways to extend opportunities for participation to non-APEC economies

Outsourcing:

The perspective of a Data Processor

Scott Taylor, Chief Privacy Officer

Presentation Outline

- HP Overview
- Outsourcing Trends
- Data Controller & Processor Responsibilities
- Managing Assurance & Compliance
- How APEC Will Help

Hewlett-Packard Company

$104 Billion	387,000	178	#1 or #2	$4.5 Billion	World's Largest
Revenues	Professionals	Countries with operations	In markets served	Annual R&D	Technology Company

Personal Systems

Imaging & Printing

Enterprise
Servers & Storage

Services

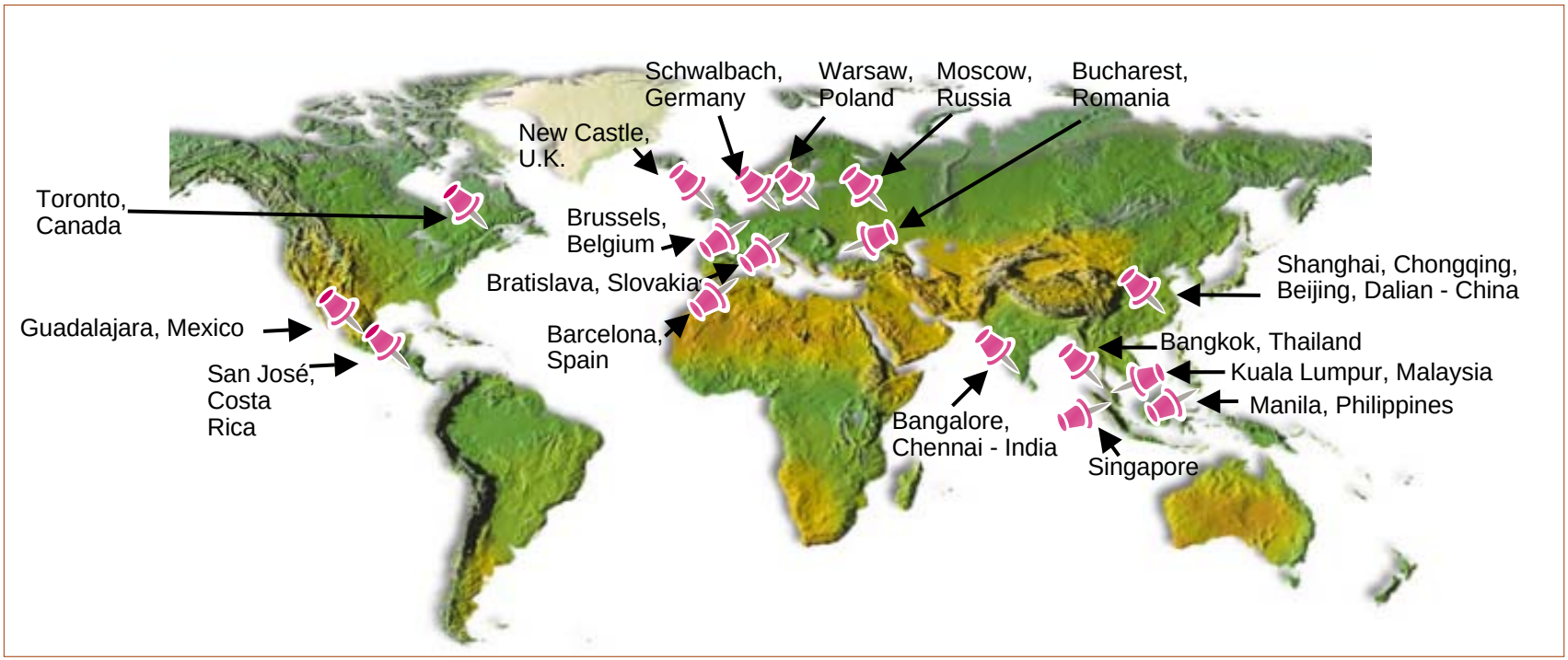
Software

- Managing the IT infrastructure for over 700 manufacturing, financial services, consumer product, telecommunications, and public sector clients around the world
- Powering 106 of the world's 120 stock exchanges
- Enabling 100 million cell phone users
- Processing 95% of the world's securities transactions
- Handling two out of three credit-card transactions
- Delivering solutions to 100% of the Fortune 100
- Innovation resulting in 11 patents per day

hp invent

HP Global Outsourcing Presence

Key facilities



Considerations:

- Geographic location
- Workforce
- Local Laws
- Political stability
- Labor laws
- Infrastructure

Outsourcing Trends

- Data Controllers increasingly raising privacy in outsourcing deals and desire to transfer responsibility to the Processor
- Increasing PII complexities and more highly regulated industries outsourcing
- Lack of understanding of the global/local landscape
- Data Controllers looking to Processors for guidance and

Outsourcing Responsibilities

Data Controller

- Determines compliance requirements based on applicable laws and internal policies
- Informs the Data Processor (i.e. service provider) of the requirements that come with the information and documents these obligations in the contract
- Selects the service provider based on trustworthiness and competency to manage to the requirements that come with the data
- Retains accountability

Outsourcing Responsibilities

Data Processor

- Follows the contract and instructions, but does not determine compliance requirements
  - No legal advice – may raise issues but Controller makes decision
  - Can cite legal principles with source – but avoids interpretation
  - Does not guarantee use of their solution will produce compliance
- Effective management and oversight of the appropriate safeguards and obligations that came with the data
- Compliance with law should be limited to performing against the contract

Managing Compliance & Assurance

- Data Controller responsible for setting compliance requirements with limited diligence by the Processor
- Data Processor ensures that the compliance requirements in its service scope are met along with assurance processes for other deliverables
- In cases where the Data Controller's requirements are questionable or illegal, the Data Processor should notify the Controller and/or be willing to walk away from the business (accountability)
- The Data Processor should have robust internal auditing of contracts and operations

How APEC Will Help?

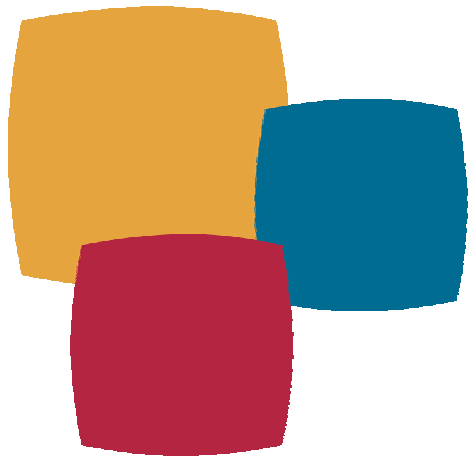
- Provides a more common framework between the Controller and Processor
- Allows companies to leverage global models due to common standards
- A practical solution for cross-boarder data flows
- Legal compliance will be easier to understand and achieve
- Enables improved accountability on the part of all parties

Asia-Pacific
Economic Cooperation

hp invent

Industry Canada Industrie Canada

Data Privacy & E-commerce: Fostering Economic Growth



Session V:
APEC Principles and Fostering Economic Growth

Richard Bourassa

Canada

Objective

- Demonstrate how APEC Principles foster business opportunity by fostering a trusted environment for outsourcing information-intensive business processes (BPO) in growing economies.

  ie: privacy protection and economic growth can go together

History

- **Policy framework:**
  - APEC Privacy Principles adopted in 2004
  - Informal coordination APEC-OECD
  - Multistakeholder process: governments, industry, civil society
  - Different perspectives integrated: legal, policy, economic, trade

- **Implementation**
  1. Domestic: legislation; regulations; private sector codes of conduct; etc.
  2. International: cooperation (information sharing, investigation, enforcement); cross-border privacy rules

APEC Principles

1. Preventing harm (misuse)
2. Notice (re. Collection of information)
3. Collection limitation (collect only relevant info)
4. Uses of personal info (purpose of collection)
5. Choice (by individuals)
6. Integrity of personal information
7. Security safeguards (protect from misuse, loss…)
8. Access and correction
9. Accountability

APEC Principles

Where we stand:

- Current focus on implementation – international dimension
  - Goal: facilitate responsible and accountable cross-border data transfers and effective privacy protection
  - Tools:
    - Pathfinder Statement
    - Work Program on CBPR
    - 9 projects
  - Cross-border cooperation:
    - Government-government
    - Regulator-regulator
    - Trustmark-trustmark
- Need to comply with domestic regimes (legislation, regulations)
- Need to avoid creating unnecessary administrative and bureaucratic burdens for businesses and consumers

APEC Priorities

- The APEC context:
  - Trade and Investment
    - WTO; RTA/FTA
    - Trade Facilitation
    - Transparency
    - Digital economy

Data Privacy is about trade facilitation, transparency, digital economy

Benefits

- **Benefits for industry**
  - Recognition: domestic; cross-border
    - they are taking privacy seriously
    - Treat a foreign customer like a domestic customer
  - Harmonized approach
  - Transparent marketplace rules
  - Less red tape
  - Facilitates selection of cross-border business partners

- **Benefits for consumers:**
  - Trust and confidence
  - Greater choice

- **Benefits for an economy:**
  - Facilitates trade
  - Facilitates investment
  - Protect consumers

The case of BPO

- Outsourcing & Offshoring of Business Processes is stimulated by globalisation
  - Cross-border trade in services is raising dramatically;
  - Notably in information-intensive services: banking, insurance, health, IT
  - Global supply chains (trade in goods) rely on electronic transfer of information: some is private, some is sensitive
- It makes business sense : cost reduction
- …But it needs to make sense for consumers and governments

The case of BPO (cont'd)

- **A government perspective:**
  - In a globalized world, governments need to ensure that their citizens will continue to receive the same level of protection as they do domestically
    - Privacy protection
    - Consumer protection
  - Need to trust the business environment of the third country where offshoring is taking place
  - Build trust and confidence
    - information sharing
    - Cooperation at all levels
    - Investigation and enforcement

Next Steps

- Implement a privacy policy in accordance with APEC Framework (and/or higher standard)

- Willingness to participate in Pathfinder projects

Thank you

bourassa.richard@ic.gc.ca


Canada

APEC Information Privacy Principles in the development of Outsourcing Business:
CONTACT CENTER IN PERU

Harry Chang

Chief Investment Promotion

ProInversión

APEC Feb 2008

Agenda

1. Foreign Investment in Peru – Legal Framework

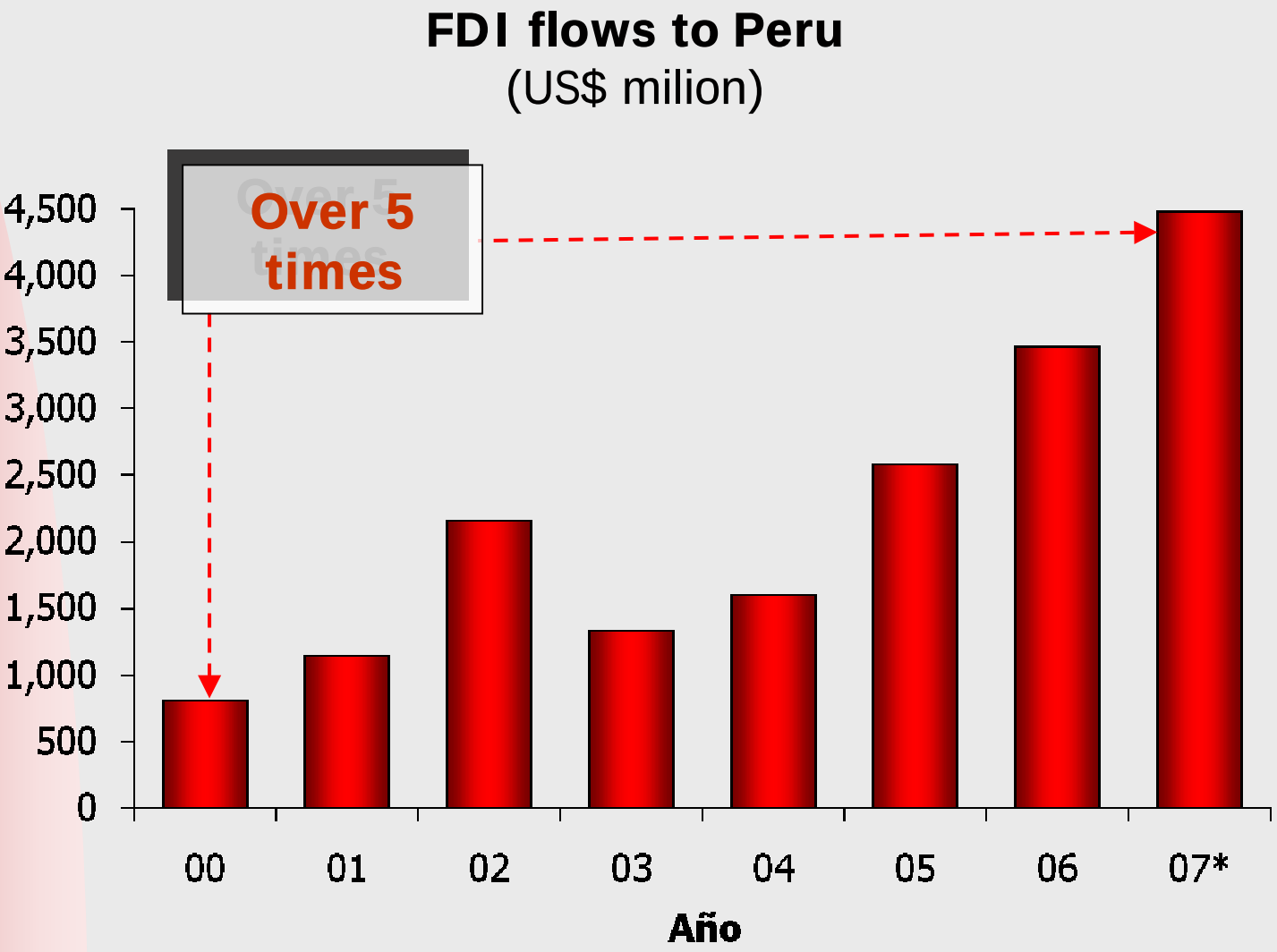
2. Development of the Outsourcing Business. Contact Center in Peru.

3. Peru: Business Hub in Contact Centers: Private and Public Institutions Commitment.

4. Data Protection Law and APEC Information Privacy Principles

Foreign Investment in Peru

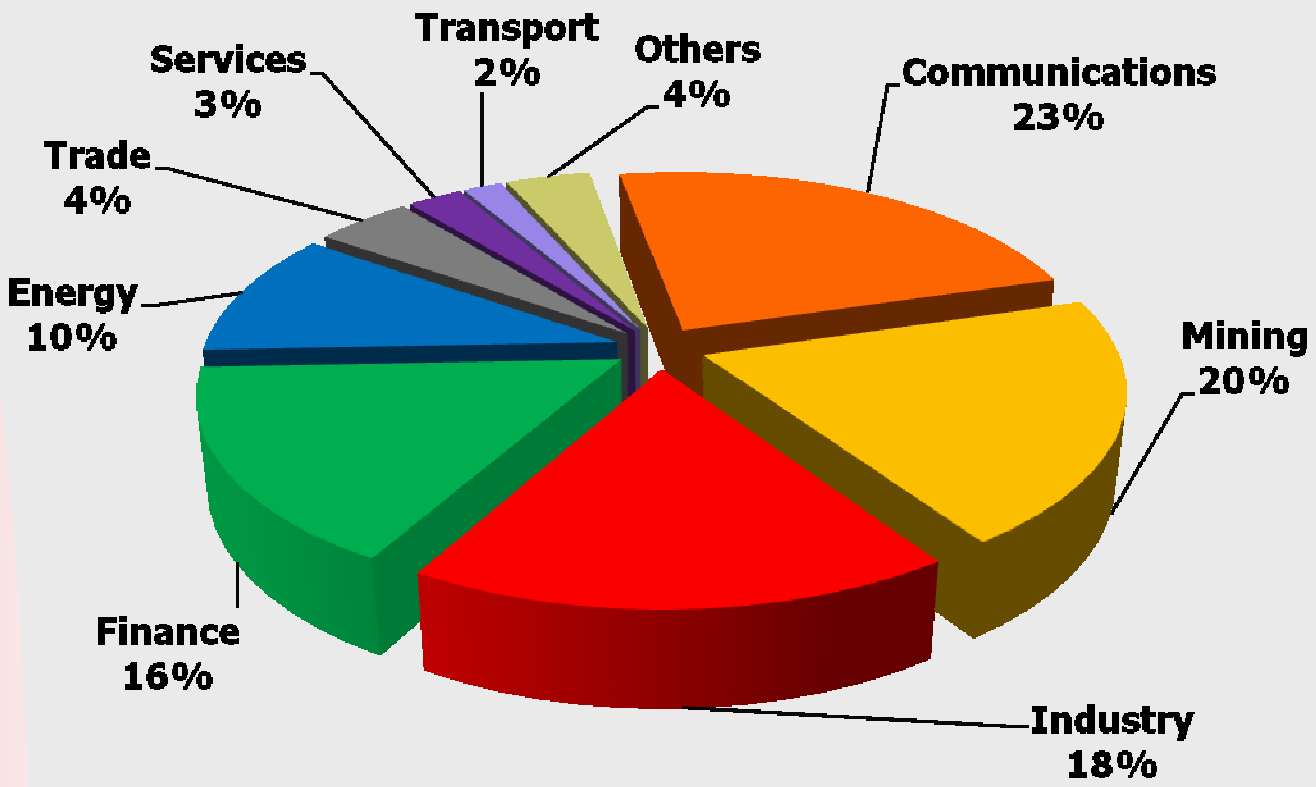
Growing FDI



*Cumulative from January to September, 2007

Source: Central Bank, Proinversión

FDI Stock by destination sector, 2007 (%)



Source: Central Bank, Proinversión

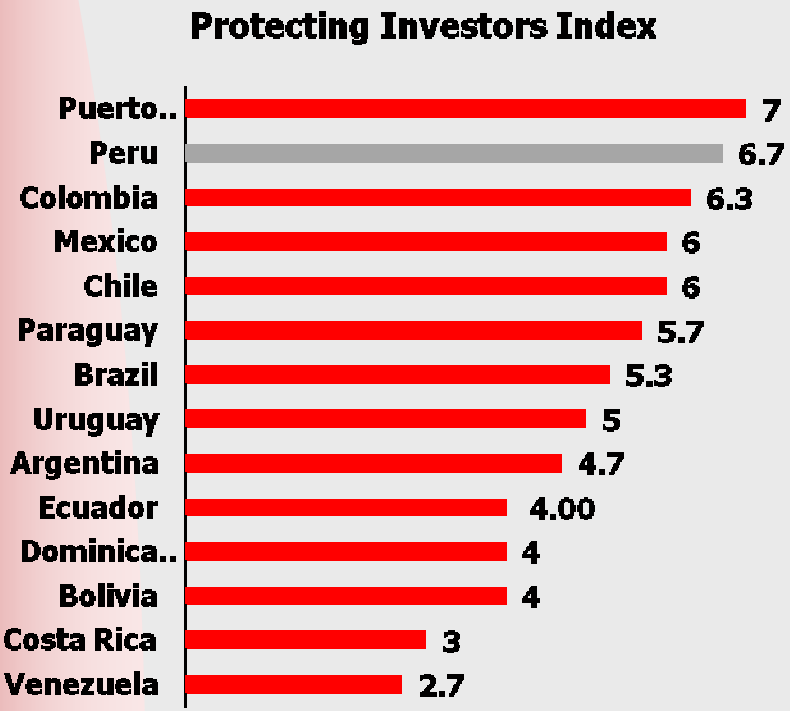
Peru offers a favorable legal framework for foreign investment ...

- Non discriminatory treatment.
- Unrestrictive access to most economic sectors.
- No performance requirements.
- Free transfer of capital.
- Free competition.
- Guarantee for Private Property
- Freedom to purchase stocks from locals.
- Freedom to access internal and external credit.
- Freedom to pay royalties.
- Network of investments agreements and member of ICSID and MIGA

Legal Framework: Constitutional provisions, "Law for the Promotion of Foreign Investment", Legislative Decree N° 662, "Framework Law for Private Investment Growth", Legislative Decree N° 757, "Law for the Promotion of Private Investment in Infrastructure and Public Service Works", Approved by Supreme Decree N° 059-96-PCM

According to a World's Bank survey and World Economic Forum:

Peru stands second in the Latin America region in protecting investors, and 15th in the World



Source: Doing Business 2008.

Peru is first in the region for government readiness for private investment

Position	Country	Points
1	Peru	5.8
2	Colombia	5.6
3	Chile	5.5
4	Uruguay	4.8
5	El Salvador	4.6
6	Bolivia	4.5
7	Brazil	4.2
8	Dominic. Rep.	4.2
9	Mexico	4.1
10	Guatemala	4.0
11	Venezuela	3.2
12	Argentina	3.1

Source: World Economic Forum, Benchmarking National Attractiveness for Private Investment in LA Infrastructure. 2007

Development of Outsourcing Business: Contact Centers

BACKGROUNDS

- **18% of young people in Lima does not study and have an informal job, reported the WLO.** This report informs that almost 300 thousand young people in Peru is jobless. This means that 10% of Peruvian labor force from 15 to 24 years old is unemployed.

- The service sector is a dynamic and fast growing sector that generates many jobs, especially TI-related jobs.

- The highest impact of investments is shown in the generation of jobs.

Contact Center: Opportunity to generate thousands of jobs……

- There are approximately **15,000** installed and available sites in Peru (30% in house), growing at an average **30% per year**. However, there is still idle capacity during the night shift. The purpose is to provide this service to Europe and Asia.

- A report by a US consultant "Datamonitor" reveals that the number of teleoperator positions at Latin American and the Caribbean contact centers will grow from **336,000 in 2003 to 730,000 in 2008.** The highest growth rate worldwide.

Country	Direct jobs
Colombia	40,000
Argentina	50,000
Chile	30,000
Mexico	250,000
Spain	200,000
Peru	30,000

Public - Private Commitment

- Government priority on creating jobs. (Well paid, legal benefits package, good working environment, job tenure).

- 19% Value Added Tax (IGV) for call center export service eliminated in 2006 thanks to joint effort of local Contact Centers and public sector (MINCETUR, PROMPERU, PROINVERSION).

Perú: "Business HUB for Contact Centers"

Investment Promotion Program seeks to change current Peru's comparative advantages into sustainable competitive advantages, in order to place Peru as a sound platform for the exportation of contact centers services, generating thousands of jobs.

ProInversión

Benefits of Contact Centers sector for Peru

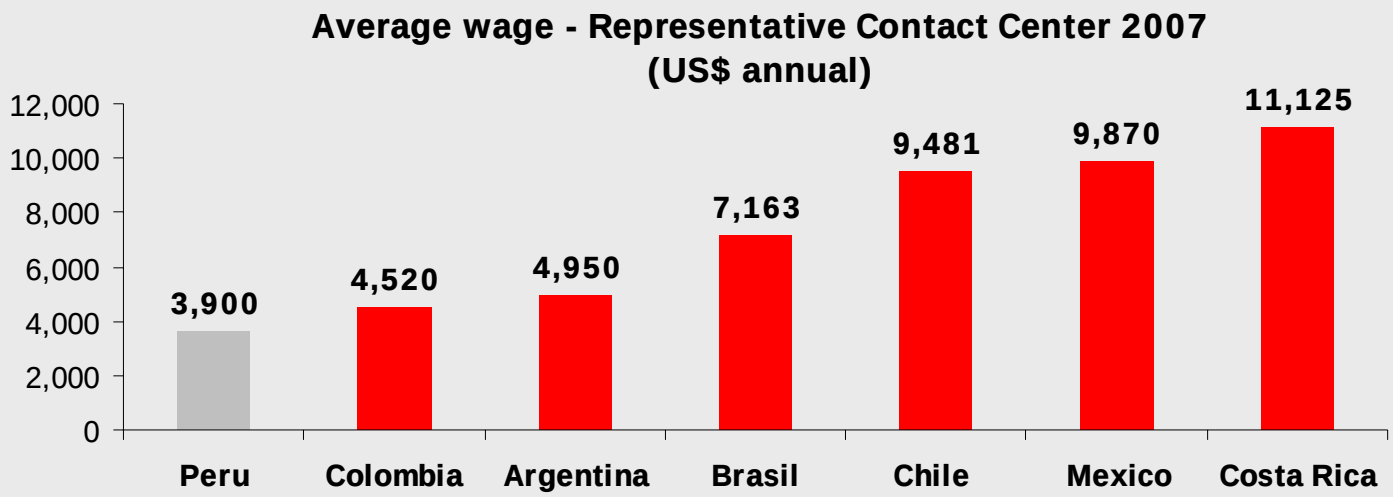
1. Increase of investments
2. Generation of jobs
3. Main labor force: college students
4. Ongoing Professional Training
5. Labor Opportunity
6. Improve work conditions
7. Services Exportation
8. Descentralization of investments

Peru: Business Hub for Contact Centers

Why invest in Peru?

5 important reasons for the growth of Peru's Contact Centers:

a. Lower labor costs and labor flexibility (60% operating cost)
b. Quality and experience of Peruvian labor
c. Neutral voice tone (Spanish)
d. Technological requirements
e. Real Estate: Lower costs



Source: Economist Intelligence Unit, pay scale 2007. Telemarketing Argentina

ProInversion: Strategic Plan

The Investment Promotion Program for Contact Centers is based on <u>5 parallel work schemes:</u>

1. Removal of Barriers for the development of this sector:
   - Removal of VAT for the exportation of Contact centers service (March 2006)
   - **Personal Data Protection Law.**
2. Foreign Investment attraction campaign for contact centers.
3. Creation of a Peruvian Association of Contact Centers – APECCO
4. Decentralization of contact centers.
5. Generation of business clusters in contact centers and training programs

ProInversión

Contact Centers that invested in 2007

Company	Country	WEB	Invest. US$*	Direct Job*
1. GSS	Spain	www.grupogss.com	3,000,000	1,000
2. Lexiconmarketing	USA	www.lexiconmarketing.com	4,000,000	1,000
3. Vidisa	Spain	www.vidisa.com	300,000	270
4. Digitex	Spain	www.digitex.es	1,000,000	1,000
5. Avante	Spain		400,000	400
6. Multivoice	Argentina	www.grupomultivoice.com	600,000	600
7. Telemark Spain	Spain	www.telemark-spain.com	3,000,000	1,000
TOTAL			**12,300,000**	**5,270**

* Estimated

Personal Data Protection Law

Draft of the Personal Data Protection Law which purpose it to elaborate a whole legal framework that guarantee the right to protect personal data.

Purposes:

- To guarantee the protection and appropriate use of personal data.
- To create a reliable environment to foster a fluid exchange of data (commercial services) with developed countries.
- To increase Peruvian competitiveness for the attraction of investments in Outsourcing Business.

Criteria: APEC Information Privacy Principles

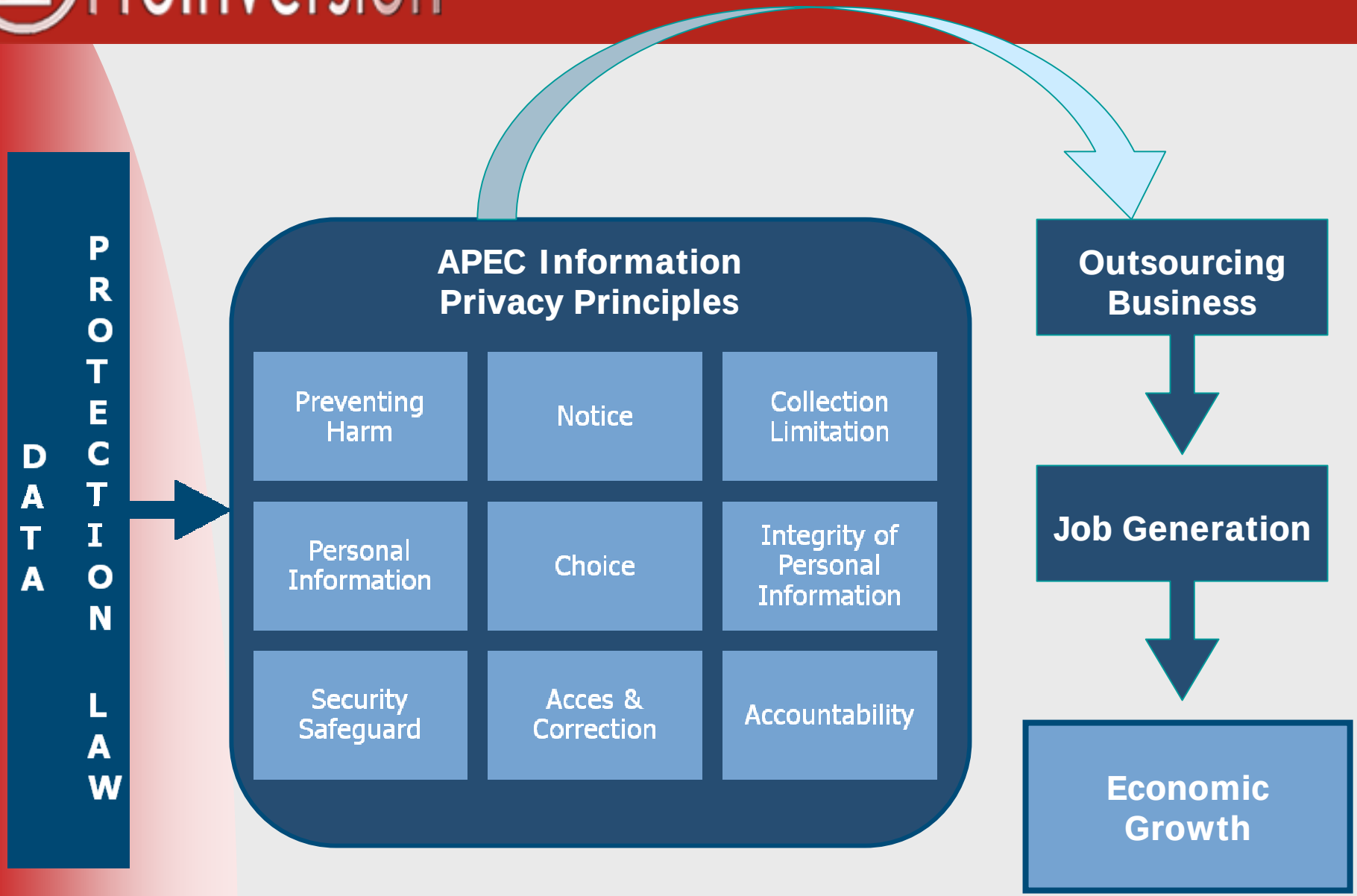
a. To develop appropriate privacy protections for personal information.
b. Implementation of security measures for effective data protection.
c. Organization in charge of the enforcement of the pertaining legislation.

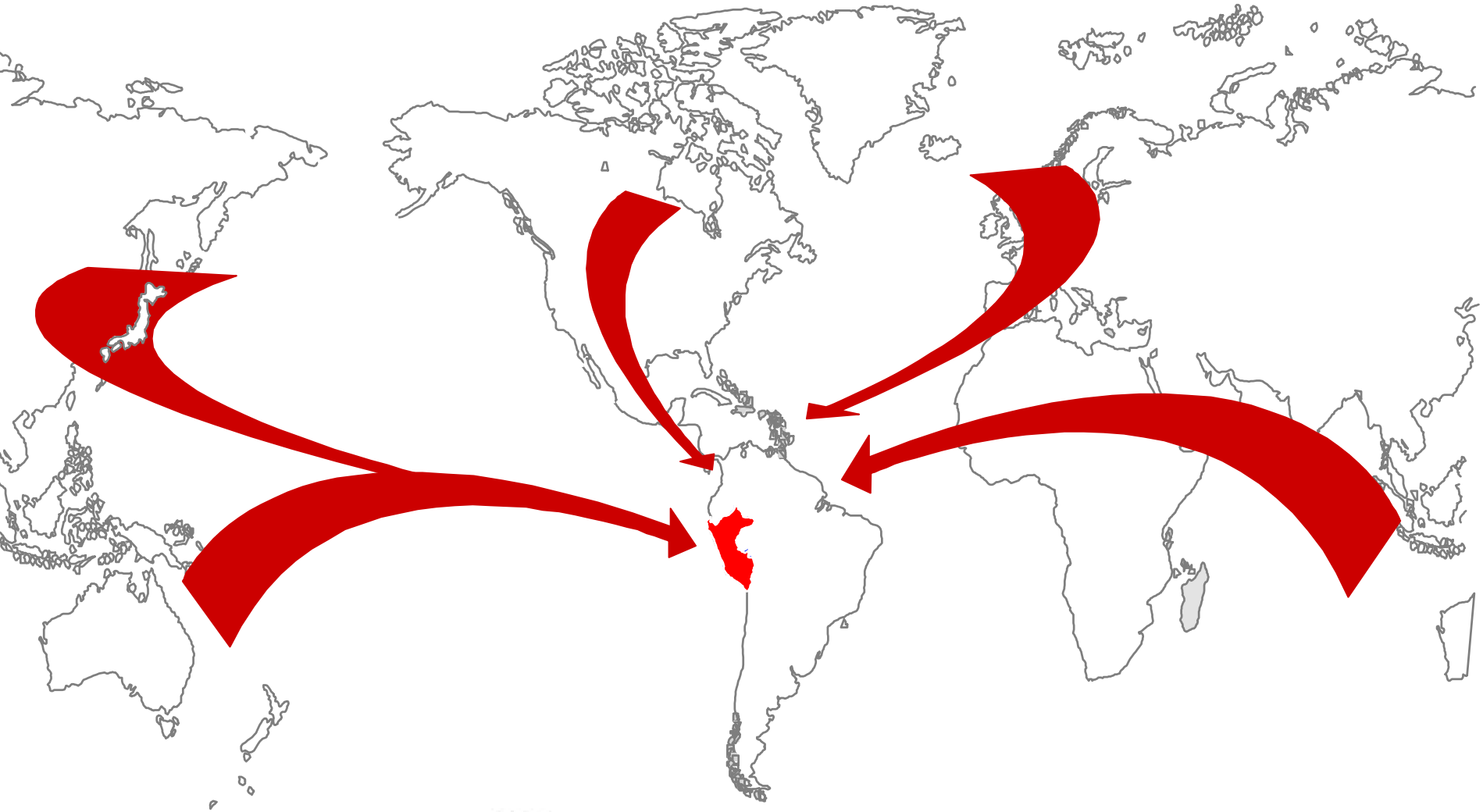
Data Protection

- Percentage of companies that carry out formal risk studies
  - Brazil : 70%
  - Venezuela : 71%
  - Peru : 66%
- Percentage of companies with information security systems:
  - Peru : 93%
  - Argentina : 88%
  - Brazil : 85%
- Barriers found in Peruvian companies that hinder the implementation of information security projects:
  - Not enough funds (52% of the cases)
  - Not enough specialists (30% of the cases)

Source: Ernst & Young. Global Survey on Information Security

ProInversión





ProInversión

www.proinversion.gob.pe

INFORMATION INTEGRITY SOLUTIONS

Malcolm Crompton

APEC & Privacy: The 9 Pathfinder projects

First Technical Assistance Seminar on International Implementation of the APEC Privacy Framwork, 2008

Lima, Peru
20 February 2008

INFORMATION INTEGRITY SOLUTIONS

2008 Pathfinder pilots: Current ideas

- CBPR self-assessment guidance for organisations
- Guidelines for trustmarks participating in a CBPR system
- Compliance review of an organisation's CBPRs
- Directory of compliant organisations
- Data Protection Authority & Privacy Contact Officer Directory
- Template Enforcement Cooperation Arrangements
- Template cross-border complaint handling form
- Guidelines & procedures for responsive regulation in a CBPR system
- Cross-Border Privacy Rules International Implementation Pilot Project

INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton
Managing Director

53 Balfour Street
Chippendale NSW 2008
Australia

+61 407 014 450

MCrompton@iispartners.com
www.iispartners.com

DAVARA
ABOGADOS, S.C.

DATA PRIVACY & E-COMMERCE: FOSTERING ECONOMIC GROWTH

Technical Assistance Seminar on International Implementation of the APEC Privacy Framework, 2008

USING PATHFINDER TO BUILD CAPACITY IN EMERGING ECONOMIES

Dra. Isabel Davara F. de Marcos
Partner, Davara Abogados, S.C.
Chair Latin America Electronic Commerce Committee, ABA
Lima, Peru
February 2008
idavara@davara.com.mx

OUTSOURCING

- Outsourcing as a great opportunity in emerging economies to foster economic growth, provided quality and efficiency of the SLA.

- Key actors:
  - Governments
  - Regulators
  - Businesses
  - Consumers
  - “Trustmarks”

ACTORS INVOLVED IN DATA PROCESSING

- Personal information controller
- Processor
- Consumer/ data´s subject

WORLDWIDE MAIN PRIVACY SCHEMES

- European Union → privacy laws
- USA → some federal and state laws (moreover sectorial) + self-regulation
- Australia and New Zealand → privacy codes (hybrid approach)
- So: there is a wide range of approaches to privacy frameworks applying to personal information across APEC economies.

APEC PRIVACY PRINCIPLES

- Preventing harm
- Integrity of Personal Information
- Notice
- Security Safeguards
- Collection Limitations
- Access and Correction
- Accountability
- Choice

Four main goals:

a) to develop **appropriate privacy protections** for personal information
b) to prevent the creation of **unnecessary barriers to information flows**
c) to enable multinational businesses to implement **uniform approaches** to the collection, use and processing of data, and
d) to facilitate both domestic and international efforts to promote and **enforce information privacy protections**.

KEY PRINCIPLES FOR E-COMMERCE AND OUTSOURCING

- Responsibility
- Accountability
- Effectiveness (of privacy protections)
- Free movement (without creating barriers to cross border data flows)

OUTSOURCING EXAMPLES

- Call Centers in LatAm and Asian countries (i.e. Colombia and Spanish DPA last case)
- Hosting and other services related to ITC
- Marketing activities
- Banking and financial services
- Other online activities

CONCERNS ABOUT PRIVACY & OUTSOURCING

- Cross border data flows: different countries and different legal and/or privacy protection schemes
- CBPR governing relations controller-processor
- Accountability
- Enforcement

THE MOST USUAL PROBLEMS

- Lack of legal/self-regulation protection in processor's country
- Breach of contract (privacy principles, security measures, …)
- Difficulties for audit compliance
- Lack of consumer and business trust

CURRENT SCHEMES FOR OUTSOURCING

- Binding Corporate Rules (EU)
- Contractual solution (EU + ICC)
- Cross-Border Privacy Rules (APEC)

ELEMENTS OF A CBPR SYSTEM

- Self-assessment
- Compliance review
- Recognition/Acceptance
- Dispute Resolution/Enforcement

BENEFITS OF A CBPR SYSTEM

- Flexibility
- Consistency with legal framework that supports the cross-border handling of personal information

SOME IMPORTANT POINTS

- Audit of security measures
- Audit of privacy principles
- Legal cooperation between governments and business
- Investigation and enforcement powers

SOME FINAL THOUGHTS

- Privacy is an essential factor for promoting consumer confidence and therefore an opportunity for APEC economies to enjoin a digital economy

- If privacy law is unpredictable = Limits outsourcing choices + Increases business risk = Problematic decision-making + impact on consumer and business trust

Thank you!

Towards Personal Data Protection in Thailand

Dr.Nakorn Serirak

Official Information Act 1997

- Guarantee Right to Know
- Protect Personal Data

The legal basis of Freedom of Information is the guarantee of the people's rights to have full access to information, the so-called Right to Know. The main process towards establishing accountable and transparent government, key elements of Good Governance.

Data Protection under Official Information Act

the act allows state agencies to collect, process, and use personal data of the people only when it deems necessary for its authoritative operation. Meanwhile they are obliged to provide appropriate security system for such personal data.

Termination of the system will be finalized when its operation has been accomplished or when the system is no more necessary

State agencies are not normally allowed to trace and store personal data of citizens, but are obliged to, in advance, inform the data subject about the collection of such personal data.

A personal information system to be established has to be publicly informed by announcement in the government gazette.

personal data has to be kept safely and state agencies has to take good care of preventing any dissemination or disclosure of personal data to other state agencies or any private individuals without consent of the data owner.

state agencies have to make the personal information system open. It must be possible for individuals to access their own data file and to review its content

Problems in Implementation

Information Act is a newly established law, the perceptions and the understanding of freedom of information and personal data protection has been very limited.

Information Law covers only personal data occupied by state agency, no legal mechanism to protect data in business sector.

As government and business occupy a great deal of personal data of which is indeed people’s property, and more importantly, human dignity. They might cause the violation of privacy.

Personal Data Protection Act (draft)

approved by the cabinet
August 1st, 2006

Section 4

Enforce data processing of processor whether it be individual, organization, or state agencies with business or commercial objectives

Operation Plan for Public Relation and Knowledge Dissemination

- Distribute APEC Framework to state agencies as well as private organization through Chamber of Commerce, Industrial Association, Bank Association, Insurance Association, Direct Marketing Association, Webmaster Association, consumer's organization, and non-government organization

Operation Plan for Public Relation and Knowledge Dissemination

- Organize conference and meeting of all parties concerned both for knowledge sharing and seeking coordination in knowledge transfer to members and general public

Operation Plan for Public Relation and Knowledge Dissemination

- Implement survey of Data Protection measure both in government and business organization to assess how they compile APEC to their practices

Operation Plan for Public Relation and Knowledge Dissemination

- Publish APEC framework and related articles in various media, newspaper, journals, and website
- Organize meeting and conference to disseminate knowledge concerning privacy protection and APEC rules.

new constitution of 2007, personal data has been more emphasized as written in article 35 as follows: “A person’s family rights, dignity, reputation and the **right of privacy** shall be protected. The assertion of circulation of a statement or picture in any manner whatsoever to the public, which violates a person’s family right, dignity, reputation or the **right of privacy**, shall not be made except for the case which is beneficial to the public. A person shall have the right to be accorded protection against undue exploitation of **personal data** related to his or her individuality, as provided by law.”

Concluding remarks

Considering personal data as a part of human rights, namely informational privacy right, legal mechanism, either the enactment of new law or the amendment of the present one, is therefore inevitable. Thai people, as the same as humans of all nations, should also have mechanisms to protect human dignity and prevent any privacy violations.

Information Law and the concepts of Freedom of Information as well as Privacy Protection or Personal Data Protection are totally new, thus requiring some time to become more efficiently effective.

Thai society needs some time to learn and recognize the “Right to Know” as an essential part of establishing transparent government and “Personal Data Protection” as an element of securing human dignity.

Nakorn Serirak, PhD

Information Commissioner's Office

Thailand

nakorn@oic.go.th, nakornseri@gmail.com

Asia-Pacific
Economic Cooperation

Second Report of the Technical Assistance Workshops on International Implementation of the APEC Privacy Framework, 2008

Electronic Commerce Steering Group

August, 2008

Prepared by:

Paula Bruening - Hunton & Williams LLP
1900 K Street NW
Washington, DC 20006
(202) 955-1500 Phone
(202) 778-2201 Fax
pbruening@hunton.com
http://www.hunton.com

Jorge Bossio – Organismo Supervisor de la Inversión Privada en Telecomunicaciones
ECSG04/2008T Project Overseer
Calle de la Prosa 136 – San Borja – Lima 41
(511) 225-1313 Phone
(511) 475-1816 Fax
rrii@osiptel.gob.pe
http://www.osiptel.gob.pe

Prepared for:

Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel +65-68919-600 Fax: +65-68919-600
Email: info@apec.org
www.apec.org

Content

Report of the Second Technical Assistance Workshop on International Implementation of the APEC Privacy Framework, 2008

"Data Privacy & E-Commerce: Enhancing Privacy in Global Transactions"

August 12 and13, 2008

Introduction

The second technical workshop was held in Lima, Peru on August 12-13, 2008.

The themes and goals of the meeting built upon the findings of the Data Privacy Subgroup at its meeting in Lima in February 2008. At that meeting, the Subgroup established working groups and work plans to facilitate the work of nine Pathfinder projects that would provide tools and mechanisms to further the adoption of the APEC privacy principles and to test its practical implementation.

Purpose of the Workshop

The workshop was designed to provide updated information about the development of legal frameworks for privacy protection and work on specific tools and mechanisms that support privacy governance. It opened discussion about corporate social responsibility issues and its relationship to privacy and e-commerce. Finally, the workshop goals included information exchange about outreach to consumers and other stakeholders about the APEC framework and in depth discussions about the work of the Pathfinder projects.

Structure of the Workshop

The Workshop was structured to provide ample opportunity for information exchange related to developments in law, regulation, self-governance and accountability agents in member economies through panel discussion. It was further designed to encourage robust interaction among participants in breakout sessions that focused on issues related to building stakeholder awareness and understanding of the APEC approach, and to elicit reaction to developments in the work of the Pathfinder project and recommendations about the work going forward.

Summary of Proceedings

Welcome and Introduction

Guillermo Thornberry, Chairman of the Board, Osiptel, welcomed participants to the second meeting on data privacy. He spoke of the importance of cross border data flow protection to trade and employment and the need for sound frameworks for the security, reliability, and integrity of data and data exchanges. He noted the importance in particular of information flows in increasing Peru's trade with countries around the globe.

Peru looks forward, he said, to strengthening ties with APEC countries and wants to continue to be an active participant in APEC work.

Richard Bourassa, Chair of the Electronic Commerce Steering Group and Director, International Policy, E-Commerce Branch, Industry Canada, characterized the workshop as part of continued sharing of the experience of stakeholders to gain a better appreciation of regulatory, self-regulatory and legal environments within the region, and an understanding of how we might design a system across borders.

Mr Bourassa's remarks highlighted the work of the Pathfinder, which he described as a way of highlighting for leaders the areas that should be further developed and the linkages with trade, capacity building. The Pathfinders promote a multi-stakeholder approach to the work of building a cross-border mechanism and an open, frank, sharing of ideas and domestic and international experiences. As work on privacy is a clear priority for APEC; ministers have asked for annual reports on the progress of the Pathfinder

Rosario Fernandez, Minister of Justice, Peru, provided an overview of privacy protection in Peru. She talked about its roots as a human right and that that the importance of the right has been magnified because of the growing ability to store, reproduce, share and compile data. She referenced many international instruments for protecting data and the constitutional foundations for the Peruvian legal framework for data protection.

She then talked about the constitutional foundations for the Peruvian legal framework for data protection. She discussed in some depth the goals of the Peruvian approach - transparency about data collection (what, why and for what reasons is data being collected) and about the importance of ensuring data accuracy, completeness. She also noted the criminal sanctions available for violations of privacy.

Session I: International approaches to cross-border data flows

The moderator described the panel as a sharing of perspectives related to different way of making progress in development of cross border privacy rules to provide a context for cross-border flows of information.

Alfredo Reyes Krafft, Executive Vice President, Mexican Internet Association, described data as the new currency of international economy. Economic development, he said, will depend upon the way public policy is developed so that it does not limit the flow of information, while recognizing and addressing through security measures the risk that comes from the use of this information. He discussed the complications that compliance with the EU adequacy approach can present, and how it can seriously challenge the operations of companies.

Mr Reyes highlighted the need to find an adequate balance of public policy at the national level and codes of conduct that can be implemented through seal programs, He cited the Mexican experience, where two initiatives for national reform are under consideration beginning at the constitutional level. Mexico has also located data protection in the Ministry of Economy, which has a deep knowledge of the issue and of the critical value of data to commercial activity.

Kamlesh Bajaj, CEO, Data Security Council of India, NASSCOM, introduced meeting participants to NASSCOM - the National Association of Software and Service Companies, and described their "4E Framework for Trusted Outsourcing" that involves engagement with customers, governments, regulators, industry bodies and think tanks; education for members, law enforcement and media; enactment of IT Act and new sections to cover emerging crimes; and enforcement through certification, and dispute resolution.

He talked about NASSCOM's work to develop the Data Security Council of India - an independent, non-profit self regulatory organization that seeks to create a culture of security and privacy in the Indian IT industry. The DSCI will propose a basic set of security and privacy standards to which companies can choose to adhere. The key objective is to strengthen India as a secure outsourcing destination by promoting practical measures that foster confidence in market rules and institutions.

Michikazu Chihara - Consumer Confidence Issue Group, Global Business Dialog discussed the evolution of complaint handling systems beginning with the bilateral approach of the European Consumer Center Network established in 2005. At the GBDe Tokyo Summit in 2007 ICA Net International Consumer Advocacy Network was proposed, an approach that provides for complaint intake, case management through liaison between consumer advocacy liaison offices (CALOs), and involvement of law enforcement and alternative dispute resolution.

Michael Donohue, Organization for Economic Cooperation and Development, discussed the OECD's perspective on free flows of data and their work to foster a protection for data both at a high level (OECD Guidelines) and at a more granular level. It has worked to develop a contact list of single national points of contact for bringing privacy complaints; and a request for assistance form that identifies key categories of information to be provided an ensures careful pre-request preparation.

Mr Donohue highlighted the OECD's work to promote meetings between privacy enforcement authorities and privacy officers about how to resolve privacy related complaints to encourage maximum ease and effectiveness; the OECD convened a joint meeting between privacy authorities and privacy professionals in May 2008. In the Seoul Declaration the OECD endorsed cooperation between governments and enforcement authorities in the areas of protecting privacy and reinforce co-operative relationships and mutually beneficial collaboration with the Asia Pacific Economic Cooperation.

Lourdes Zamudio, Iberic American Expert stated that an overarching objective in Latin America is that the current regulation should ensure that information transfer not be limited but guarantee that world trade development can be compatible with rights of people regarding information.

She indicated that the goal of law in Latin America is to recognize data as an asset of the organization that must be balanced with the right of individual to privacy. She also talked about the characteristics of regulatory protection in Latin America, emphasizing the asymmetry in the way that Latin American economies regard data protection rights; the political considerations at the regional level; and the influence of the European model for data protection. She emphasized the need for a homogeneous coordinate legal framework for protection of data to smooth data flows as essential to development of global markets.

Colin Minihan, Chair of the Data Privacy Subgroup provided context for the work of the Pathfinder. He explained that the Pathfinder work grows out of the high level principles of the APEC Privacy Framework. While the Framework offers principles and commentary, the Pathfinders focus on implementation and on ensuring that the APEC principles are effective. By providing these practical tools, the Pathfinder fosters an environment conducive to achieving the goals of trade and investment in the region.

The Pathfinder divides a large endeavor into nine pieces that attempt to accomplish implementation of four aspects of the Framework: self assessment, compliance review, recognition/acceptance, and dispute resolution and enforcement. Project nine will test the practical tools that will be developed in project one through eight. The final documents generated by the Pathfinders will form the basis for the system.

Session II: How Stakeholders Understand Data Privacy

Nigel Waters, Australian Privacy Foundation, provided the perspective of the consumer advocacy community on the APEC approach. He noted the varied views within the privacy community on the effort, as well as the overlapping objectives of the advocacy community and the APEC framework, although he indicated that civil society will push for higher standards. Civil society is looking for reassurance that the APEC approach will not replace domestic law. Growing recognition of the need for and value of, civil society input on the work. He expressed concern that there is still no independent civil society voice on the Privacy Subgroup to balance business interests. He expressed interest within civil society in the pathfinder process which they will monitor, particularly project 9, and encourages consultation with civil society within economies.

Claro Parlade discussed data privacy in the Philippines, reviewing the law and administrative orders relevant to privacy in the economy. He talked about how data privacy protection approaches in the Philippines adhere to the 9 principles of the APEC Privacy Framework through administrative order number eight (2006) and in pending bills related to privacy. The Philippines has also developed a multi-stakeholder technical working group on data privacy convened by the

Commission on ICT and Business Processing Association of the Philippines and composed of other stakeholders. It seeks to develop a common position on the issues of data privacy to be recommended to the Senate and the House of Representatives.

Alexander Forsyth, discussed the importance of the strong role of civil society with respect to data privacy, and of the critical role of raising consumer awareness. He discussed the high level of informality that can exist in addressing privacy, particularly in developing countries, that does not allow for adequate follow-up and monitoring and that must be remedied to assure appropriate protection.

Lai Viet Anh discussed Vntrust and data privacy in Viet Nam. She talked about the evolving culture of privacy in Viet Nam, the perspective of stakeholders on data privacy and the legal framework in the economy for privacy protection as embodied in the civil code, the law of e-transactions and the law on information technology.. She spoke in some detail about TrustVn - the trust mark program for websites as the first self-regulatory mechanism for businesses in the e-commerce arena in Viet Nam, promoting good practices rather than imposing legal sanctions.

Leigh Williams, BITS Financial Services Roundtable, discussed the importance of collaboration between in industry and government in addressing privacy and protecting data flows from loss or misuses. APEC represents that kind of collaboration. Its power will come of it being an internationally standard tool. He spoke of the shared self assessment tool developed and used by the financial services industry as the kind of tool that, when accepted by regulators, can further that collaborative approach. He also talked about the need to align individuals' expectations about the use of information with the actual use of information. When there is a trusted relationship with an organization, the consumer will also trust their use of the information.

Session III: Corporate Social Responsibility Issues related to data privacy and e-commerce

Luis Quesada, Peruvian SOM, set the stage for the session, talking about corporate social responsibility as the commitment of business to contribute to sustainable economic development by working with communities to promote quality of life. He characterized this effort as one with benefits for both business and development. He discussed the business case for corporate social responsibility, and discussed APEC's potential role in facilitating its growth in the region.

Scott Taylor, Hewlett-Packard, discussed privacy is one aspect of the company's broader approach to corporate responsibility. The company structures its obligations as liability based and accountability based. In the company decision-makers are made accountable, and in addition to legal liability, the company considers ethics and risks. Is it legal, is it secure, does it meet our privacy promises. This decision making is formally integrated into the decision making of the company. Self Certified companies meet certain proof points and trust. For cross-border privacy rules to work companies will have to do a better job of demonstrating how companies actually do what they say. Some outside party will have to provide oversight.

Peter Cullen, Microsoft discussed the special responsibility that Microsoft carries that comes with market success. He discussed Microsoft's trustworthy computing initiative, which was an outgrowth of questions raised about product and system security shortly after September 11. The attack exposed vulnerability in Microsoft products; Bill Gates said that in order to have trust, systems and software must be secure, private, reliable and that business needed to operate with a great deal of integrity.

Mr Cullen noted that Microsoft recognized its responsibility not only to address these concerns within its own products and systems, but to encourage and participate with companies to help the business ecosystem of which it is a part change its ways, incorporating privacy, security, but the new business models created new value for consumers and new opportunities for bad actors.

Mr Cullen discussed the need not only for his company to address these questions, but also to collaborate with other companies, some of whom are competitors, to promote transparency and to help create a better ecosystem. He encouraged companies to think more holistically about their role to create trusted information flows.

Maite Vizcarra, Ericsson, discussed privacy as one aspect of her company's commitment to corporate social responsibility. For Ericsson, corporate social responsibility provides competitive advantages by encouraging new business opportunities and supporting sustainable business solutions.

Session IV: Building consumer/stakeholder awareness

Participants gathered into three groups to consider and discuss questions related to building consumer and stakeholder awareness of the APEC approach to protecting cross border data flows across the region.

Session V: Approaches to Cross-border Data Privacy

Pamela Harbour, Commissioner, U.S. Federal Trade Commission talked about the work being done toward practical implementation of the APEC Framework and about the challenges to develop an enforcement cooperation arrangement that makes the system work. She emphasized that while enforcement is never as seamless as the rate of global information flows, seamlessness is the goal. She talked about three requirements for enforcement cooperation agreements: the need to be able to share information, to provide investigative assistance; to set priorities about what cases will be considered, and to maintain appropriate levels of confidentiality for information relevant to an investigation. She illustrated the practical aspects of furthering these goals through FTC experience and the laws enacted to grant FTC the ability to exercise its investigative authority in cross border cases. She also talked about the international agreements to which the FTC is a party and their importance to cross-border cooperation.

Brenda Kwok, Office of the Data Privacy Commissioner, Hong Kong, *China* discussed the provisions of the Hong Kong law and the prevalence of outsourcing by Hong Kong businesses. She talked about the obstacles in the legal regime to cross-border enforcement and the need to tackle those challenges. Work to review Hong Kong law in the context of APEC and to consider provisions in international privacy laws and standards now take priority as Hong Kong considers how it will implement the APEC initiative. She emphasized the need for cooperation within economies to ensure a single point of contact and comprehensive coverage across industries.

Session VI: The Data Privacy Pathfinder projects and stakeholder roles

Heather Shaw, International Chamber of Commerce, discussed the work led by her organization on Projects one and three. She reviewed the work on development of accountability agent program requirements and participant self assessment. She discussed the combination of projects one and three, the need for program requirements to be applicable to participants in all economies no matter what kind of accountability agent is under consideration and the need to keep the forms simple and complete. She also emphasized the need for clear definitions for many of the terms used in the documents. She indicated that work toward a glossary of terms could cut across all of the Pathfinder projects. She noted that the overall goal was development of specific, objective criteria for both accountability agents and self assessment that also allowed for the flexibility necessary to be applicable across privacy regimes. The documents are works in progress and subject to change..

Robin Layton, U.S. Department of Commerce (Project Two) - Project Two involves creation of a document to set out the criteria necessary for a private sector Accountability Agent to participate in the APEC Cross-border Privacy Rules program. The form under development would be

submitted to the appropriate government agency within an economy for review of compliance with the criteria. The work of the group was limited to private sector and the work of the group will turn attention to public sector, where an accountability agent might be a trust mark or other private sector body. That effort may involve an amalgamation of approaches.

Blair Stewart, Office of the Privacy Commissioner, New Zealand, discussed work on projects five, six and seven.

The goal of Project five is to establish a directory of Data Protection Agencies, supervisory authorities and/or privacy contact officers. Such a directory would assist privacy enforcement authorities to locate counterparts in the event of cross-border complaints. The approach taken by the project is to provide a single contact point approach and is compatible with the strategy taken by the OECD, so that a shared or common directory may be possible in the future. Project six entails development of template documentation for cooperation arrangements between enforcement authorities to facilitate exchange of information for enforcement and increase and promote cross-border investigation and enforcement cooperation. The approach of the project is a multilateral memorandum of understanding, with the core focus on requesting and providing assistance in investigation and enforcement but framework able to expand to wider areas of enforcement cooperation. Project seven will develop a template enforcement 'request for assistance' form. The project will facilitate the seeking and providing of assistance in efficient and appropriate form, allowing for low level resolution and responsive regulation. The form is closely modelled on OECD form, tailored for APEC Privacy Framework

This arrangement facilitated by these projects will be a significant step forward for general enforcement cooperation (desirable in the global digital economy) regardless of the pace of development of CBPRs or the particular direction that CBPRs might take in an individual economy or across APEC. The arrangement has been prepared while conceptual and developmental work is ongoing on CBPRs – while the arrangement anticipates and address CBPRs there may be room for improvement as other parts of the CBPR framework becomes clearer. Some matters of detail yet to be worked through and agreed before the arrangement is piloted

Reporting outcomes from breakout sessions

The session began with reports of the three breakout sessions on the Pathfinder projects organized into discussions of business, consumer and regulator considerations.

The business breakout session, led by *Markus Heyder and Kenjiro Suzuki,* focused on why businesses would be interested in participating in the APEC approach. The discussion focused on business's desire for more consistent, efficient complaint handling. They look to cross border privacy rules to create regulatory certainty and standardization and uniformity in procedures, forms and rules. They also see benefit in creating uniformity and a more common language in the way in which we talk about privacy. It will simplify risk management, compliance, contract enforcement and provide a competitive advantage for participating companies. They noted the possibility of enhanced privacy protection because of the ability of government to outsource some of the enforcement functions for which they do not have sufficient resources. Cross border privacy rules might also provide a way to address risks in economies where there is no privacy law.

The consumer breakout discussion, moderated by *Nigel Waters and Ivan Ferrando,* focused on the possibility of protection for consumers. They commented on needing reassurance that APEC approach will not supplant domestic regulation or the ability of individuals from pursuing alternative remedies. They saw the system as possibly overcoming jurisdictional limitation and encouraging a higher level of business engagement in addressing privacy. The group made three recommendations: first, there should be a continuous improvement loop for the implementation to assure monitoring about how it is developing and working in practice; the need

for effective regulatory mechanisms to support cross-border privacy rules; and third, the importance of education and awareness throughout APEC and within member economies.

Carman Bagley reported the discussion of the regulator group discussion led by *Blair Stewart, Julio Cesar Vega and Edgardo Martinez*, which considered what kind of infrastructure was necessary to promote awareness and understanding of the cross-border privacy rule process. They emphasized a multi-stakeholder approach to furthering that awareness. They noted the particular need to reach small and medium size enterprises. They also emphasized the need for regulators to have the authority necessary to cooperate with one another and for economies in the initial stages of setting up a privacy regime to be sure to establish the authority to share information and cooperate within the region. Regulators will also need to figure out what the relationship will be with accountability agents and how their effectiveness will be evaluated. They cautioned about the need for some uniformity among accountability agents and the standards for accreditation to avoid possible issues of accreditation shopping.

The final presentation was of the results of the Day I breakout discussion on building stakeholder awareness.

Group One, led by Claro Parlade and Jorge Bossio commented on his group's discussion of the culture of privacy developing now in economies and that exposure to new risks raised by data, particularly through e-commerce, drives the development of a privacy culture. He noted ways to build awareness as including government policy, adoption by business of best practices based on APEC principles as part of their corporate strategy and a solid communication plan.

Group Two led by Michael Donohue and Katitza Rodriguez considered the status of government understanding of privacy concerns and realities and looked to strategic approaches in instruments such as free trade agreements as a way to raise government awareness. They encouraged multi-channel outreach but cautioned that pathfinder projects must launch before communication can happen.

Group Three led by Nigel Waters and Rosario Chuecas reported that while levels of awareness of the work of APEC are not high, they are increasing rapidly. Broad educational efforts may be premature, but business awareness is needed urgently and a wider range of businesses need to be included in the process. The breakout group also noted that engagement of international bodies could also foster progress.

Proceedings of Second Technical Workshop on International Implementation of the APEC Privacy Framework

Peru, 12-13 August 2008

Global Business Dialogue on Electronic Commerce

International Consumers Advisory Network (ICA-Net)

- A Key for Consumers Protection in Cross-Border e-Commerce -

Mitch Chihara
Consumer Confidence Issue Group
GBDe

APEC Privacy Seminar
Lima, Peru
August 12th , 2008

Outline

- GBDe overview
- Consumer protection in cross-border e-commerce (current status)
- ICA-Net
  - Framework
  - Implementation schedule
  - Platform
- Others

GBDe Introduction

- **The GBDe (Global Business Dialogue on electronic commerce) is a worldwide, CEO-led, business initiative, established in January 1999 to assist the development of a global policy framework for the emerging online economy.**

- **21 members in 2008 (USA, Japan, Taiwan, Malaysia, Hong Kong)**

- **GBDe has the guest status in APEC ECSG and TEL since 2003.**

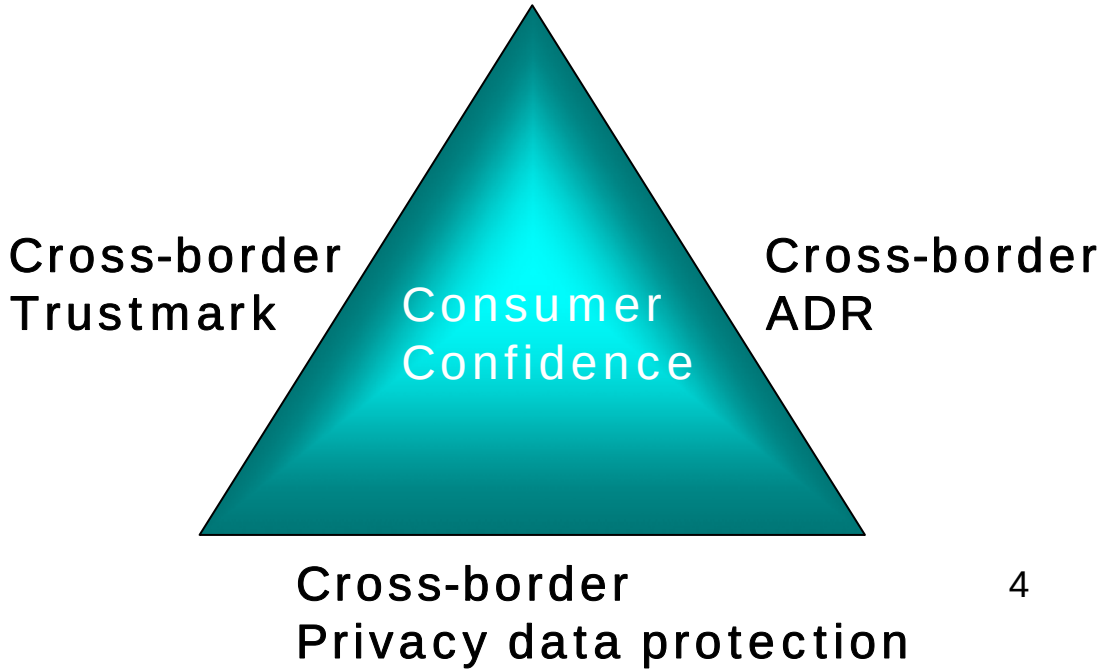
- **6 Issue Groups have been established and having dialogues for recommendations in 2008.**
  - **Digital Home (DH)**
  - **International Micro Payment (IMP)**
  - **Consumer Confidence (CC)**
  - **Ubiquitous Network Society (UNS)**
  - **Cyber Security (CYS)**
  - **Digital Opportunity (DO)**

- **Mr. Heseltine (2007 Executive Director of APEC) attended 2007 GBDe Summit in Tokyo.**

GBDe's Consumer Confidence Issue Group

Building trust between consumers and merchants is the key for sound growth of cross-border on-line shopping.
5 elements for producing confidence among consumers:

- ✓**Trustmark**
- ✓**Alternative Dispute resolution (ADR)**
- ✓**Privacy data protection**
- ✓**Safe payment**
- ✓**Reliable network**



Consumer Protection in Cross-Border e-Commerce

- **OECD Guidelines** for Consumer Protection in the Context of Electronic Commerce (1999)
- **APEC** Voluntary Consumer Protection Guidelines for the On-line Environment (2002)
- **OECD Guidelines** for Protecting Consumers from Fraudulent and Deceptive Commercial Practices Across Borders (2003)
- **OECD Recommendation** on Consumer Dispute Resolution and Redress (2007)
- **ICPEN** (International Consumer Protection and Enforcement Network) : sharing information about cross-border commercial activities that may affect consumer interests, and to encourage international cooperation among law enforcement agencies.
- **econsumer.gov**: a joint effort to gather and share cross-border e-commerce complaints, providing information about consumer protection in all countries that belong to the ICPEN, contact information for consumer protection authorities in those countries

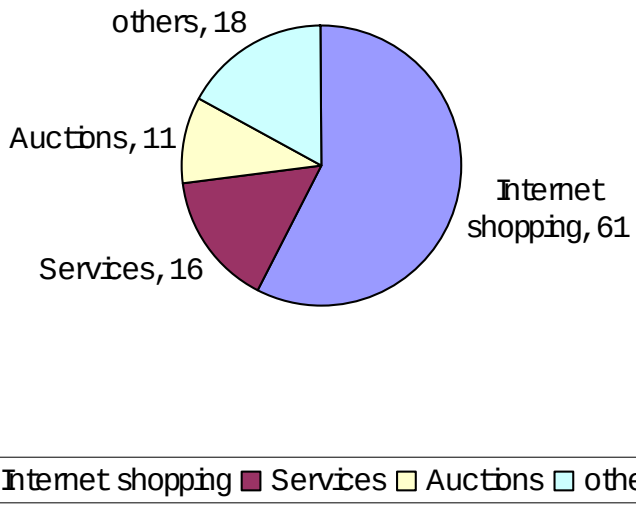
GBDe's Achievement in Consumer Protection in Cross-Border e-Commerce

- Recommended the international collaboration on trustmark of web site since its inception. GBDe issued TM Guideline and proposed this in 2001. ATA (Asia Trustmark Alliance) was established in 2003. ATA adopted GBDe's trustmark guideline as the code of conduct in investing with trustmark in 2007.
- Issued the joint guideline in 2003 with Consumer International for ADR (Alternative Dispute Resolution) , the first joint-document concluded between private enterprises and consumers. This guideline has been utilized as a standard of ADR in many Asian countries.
- Helped and promoted joint-study on cross-border complaint-handling mechanism in e-commerce with EC Network in Japan since 2003.
- Made a recommendation on consumers complaint handling mechanism for international on-line transaction (ICA-Net) in 2007

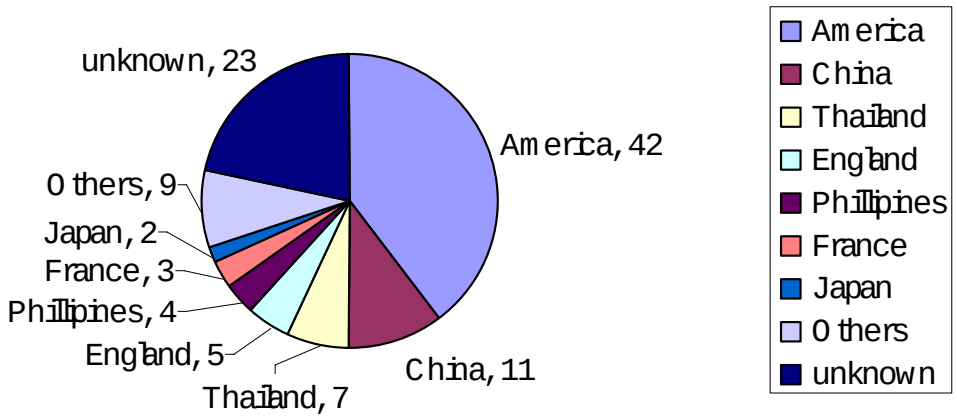
Cross-border complaints

From Japanese ADR service provider's experience

Breakdown by transaction type
(2006.4-2007.3)



Breakdown by trading partners
(20006.4-2007.3)



[Source: EC Network]

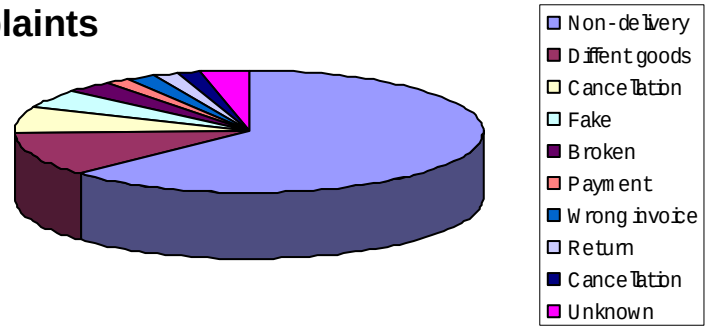
These days, Asian countries portion increase rapidly.

← Complaint-handling collaboration needs to **expand to Asian countries**.

Cross Border Complaints

From Japanese ADR service provider's experience

Breakdown of Complaints



[Source: EC Network]

- 6,200 cases reported in 5 years
- ADR (mediation, conciliation) conducted 500 cases (8%)
- Fraud cases: 25%
- About 750 cross-border cases (12%)

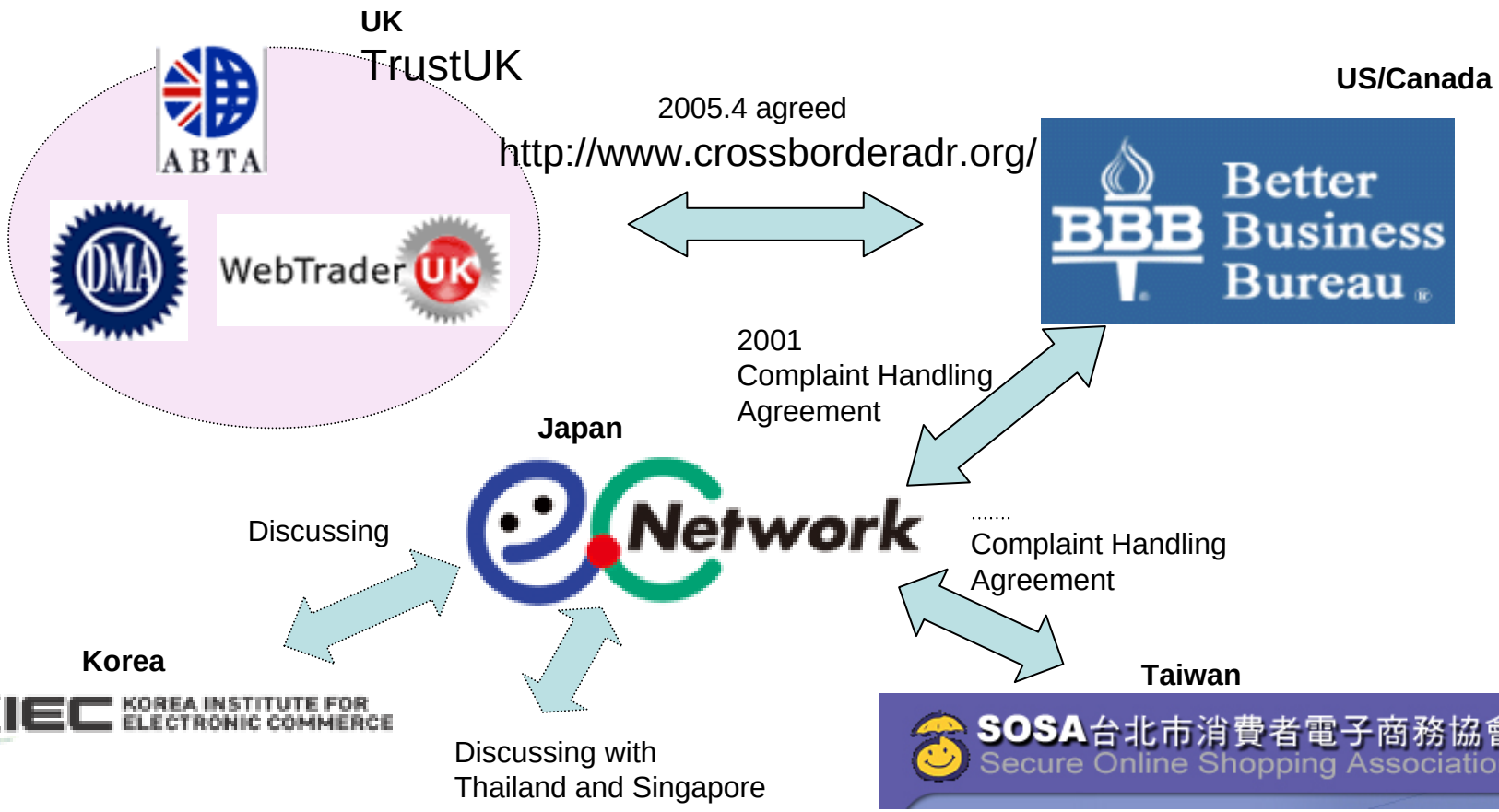
Findings:

✓**More than half of cross-border complaints occurred because of difference in language, commercial customs, etc. and they could be solved when properly handled/communicated.**

✓**In case of fraud, especially in the cross-border environment, it is hard to track. → Solution required to bridge the missing link**

Current Status of Cross-Border e-Commerce Complaint Handling

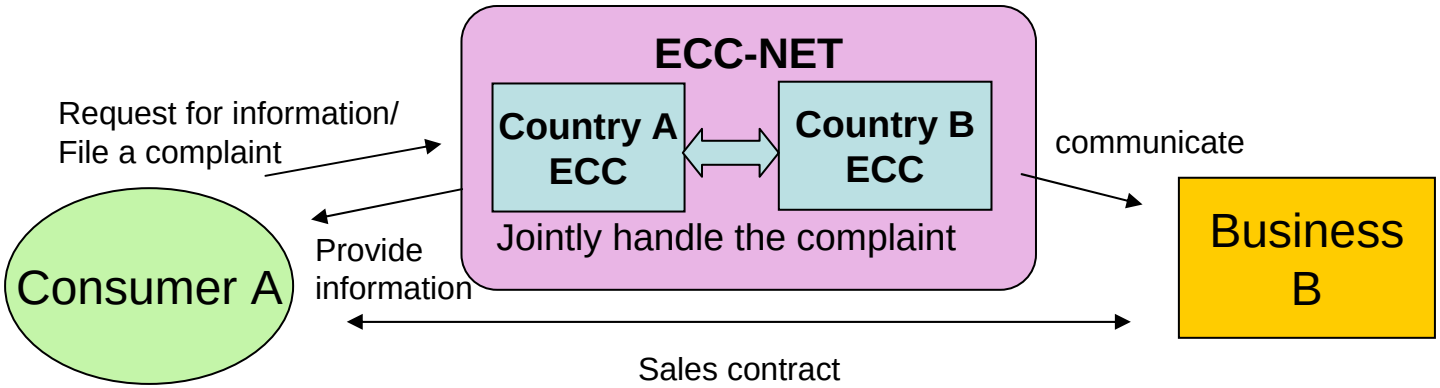
Bilateral Complaint Handling scheme



Current Status of Cross-Border e-Commerce Complaint Handling

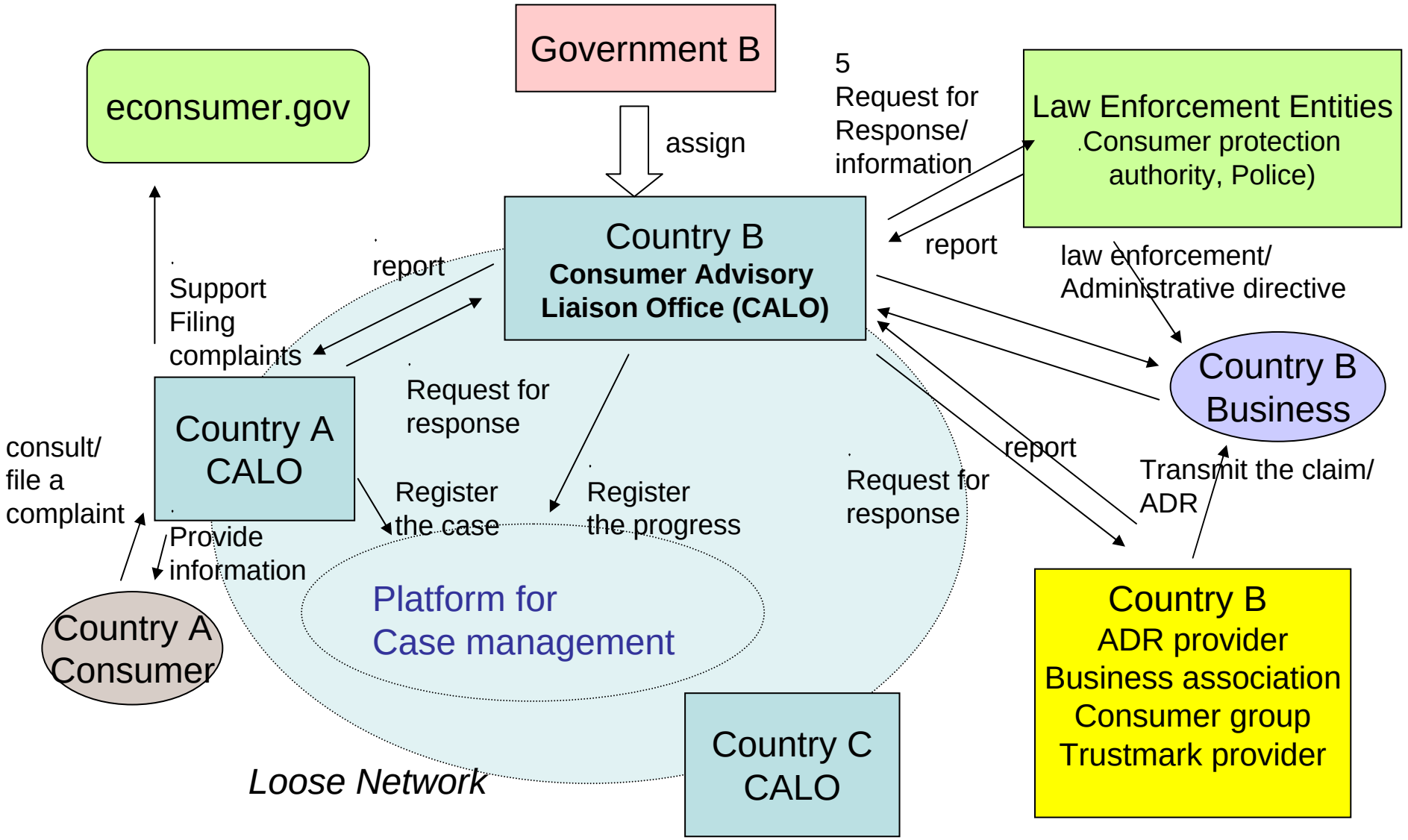
ECC-Net (European Consumer Center Net)

- Established in 2005 and all of EU countries joined
- Funding from European Commissions as well as its member countries
- Providing complaint handling service and related information upon request to consumers by phone and email (as well as in translation)



International Consumer Advisory Network (ICA-Net)

The concept was proposed at GBDe Tokyo Summit (Nov. 2007)



ICA-Net Schedule

(Tentative)

- **Phase 1 (2009-2010)**
  - **Trial**
  - **Existing ADR service providers or consumer organizations as CALOs**
  - **Utilization of existing resources at each participating organization**
  - **Small and voluntary start:**

    Possible participants: Japan (EC Network), USA(BBB), Singapore, Malaysia

- **Phase 2 .2011-2013.**
  - **Expansion to APEC regions**

- **Phase 3 .2014-2015.**
  - **Connected with ECC-Net in Europe**

Promoting implementation of ICA-Net

- Discussions with stakeholders (March – May)
  - ◆ Government organization (Japan, USA, Taiwan, Singapore)
  - ◆ Consumers Organization (CI, NCCC)
    - "Meaningful Initiatives" (All governments)
    - "Will cooperate with associates members" (CI)
    - "Collaboration with APEC Pathfinder Project recommended" (USA, Taiwan)
- Discussions with ADR providers as CALO candidates
  - ◆EC Network (Japan)
  - ◆BBB (USA)
  - ◆SOSA (Taiwan)
  - ◆CASE (Singapore)
  - ◆NCCC (Malaysia)
  - ◆KIEC (Korea)

Meeting with KIEC (Korea)

Meeting with DOC (USA)

- "Willing to collaborate as CALO" (Japan, Singapore, Malaysia, Korea)

ICA-Net Community-style Platform

CALO
Country A

Case registration

Community Style platform
for CALO

CALO
Country B

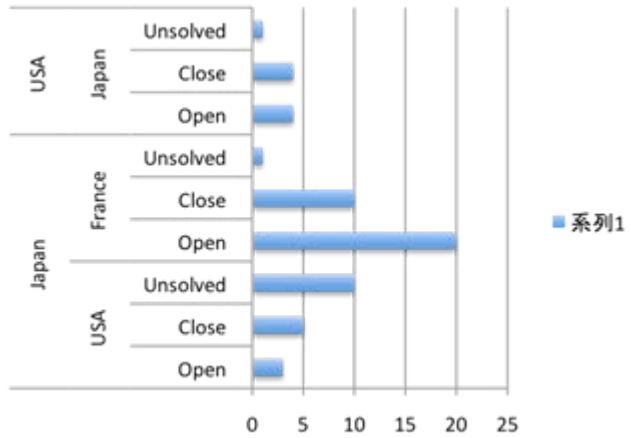
Update registration

ICA-Net Community-style Platform (Summary sample)

No.	CALO-A	Registered Date	Abstract	CALO-B	Updated Date	Status	Closing Date	category
1	Japan	2008.7.26	abcdefghijklmn	USA	7.29	Open	-	
2	Hong Kong	7.26		Japan	8.1	Close	8.2	
3	Automatic extract from community data base					Update by CALO-B		
4								

Fraud
Unpaid
Not delivery

CALO-A	CALO-B	Status	count
Japan	USA	Open	3
		Close	5
		Unsolved	10
	France	Open	20
		Close	10
		Unsolved	1
USA	Japan	Open	4
		Close	4
		Unsolved	1



Significance of ICA-Net

• CALO to be the 1st contact point for cross-border consumer complaints (including privacy issues) in B2C e-commerce

• CALO to identify the nature of the complaints and to connect with (and to request for cooperation to) proper organizations including law enforcement entities

• CALO to enhance each country's capability for complaint-handling through the voices from foreign consumers and by analyzing and making them public , leading to more attractive cross-border e-commerce marketplace in each country.

2008 GBDe SF Summit

- Theme. " Sustainable e-commerce Business Society"
- Date/Time. October 31st (Fri) 9:00 – 18:00
- Venue. Hilton Hotel, downtown San Francisco
- Guest speakers:
  - APEC Executive Director
  - Consumers International, Head
  - US Government, DOC, FTC
  - OECD
  - Japanese Government, METI / MIC
  - Chairman, International Telecommunications User Group
  - Technical University Berlin
  - Salesforce.com
  - HP
  - NTT docomo
  - etc.

The 2008 Summit in San Francisco will provide you with a unique opportunity to interact with executives and policymakers from corporations, governments and non-governmental organizations.

GBDe Consumer Confidence Issue Group Meeting

- Date/Time. October 30th (Thu) 9:00 – 12:00
- Venue. Hilton Hotel, downtown San Francisco
- Agenda:
  - Cross-border ADR
    - ICA-Net update
  - Cross-border Trustmark
    - Asia-pacific Trustmark Alliance activity update
  - Cross-border Privacy Data Protection
    - Review of international survey on Privacy Data Handling

- Guest speakers:
  - Consumers International
  - ATA
  - CPO Conference

Data Privacy Survey
Preliminary Analysis

August 2008

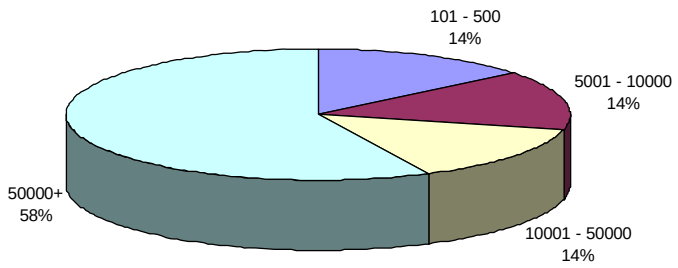
Survey Background / Overview

- Background
  - Conducted in Q2 2008 by GBDe and TPI
  - Sent to about 400 global organizations
    - Strong focus on APEC based companies
  - Response rate of approximately 5%
- The four main issues (cited by 20-40% of respondents) raised with respect to privacy regimes are:
  - Insufficient guidance
  - Conflicting requirements
  - Too prescriptive (rigid and detailed)
  - Confusing
- In-depth analysis will be available at the GBDe Summit Oct 30/31 in San Francisco

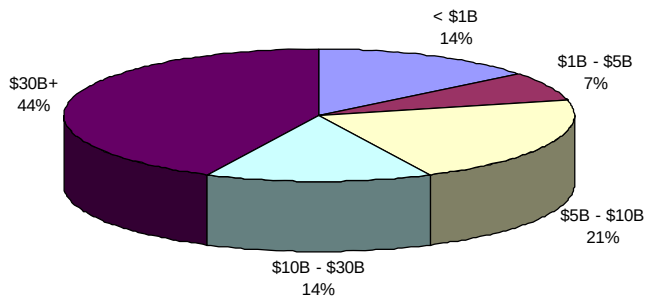
Respondent Profile

Most respondents are Chief Privacy Officers from larger companies.

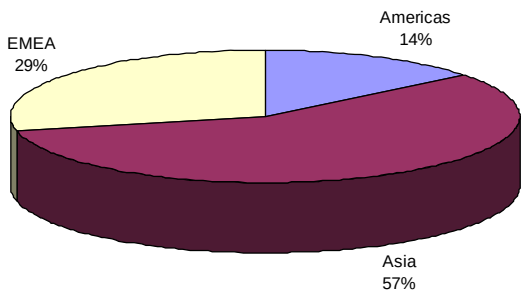
Number of Employees



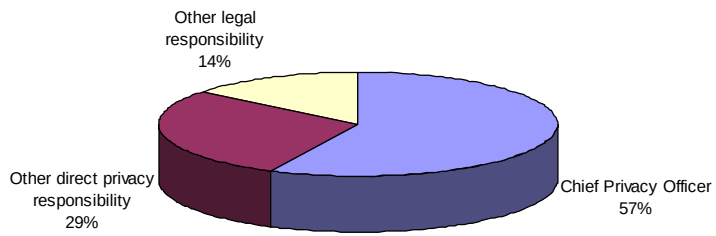
Annual Revenue



Head Office Location

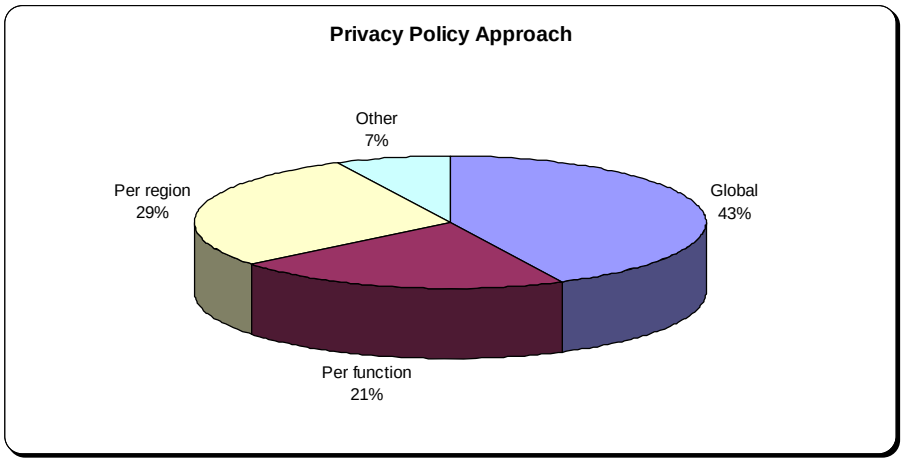


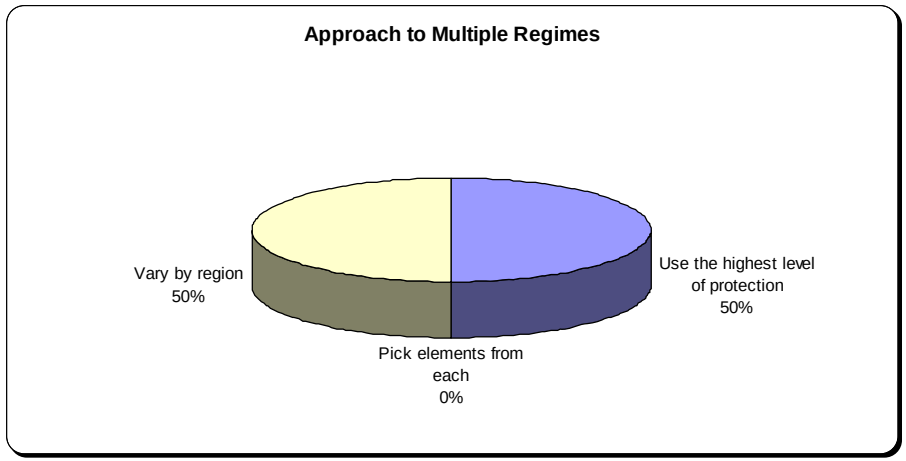
Respondent's Role

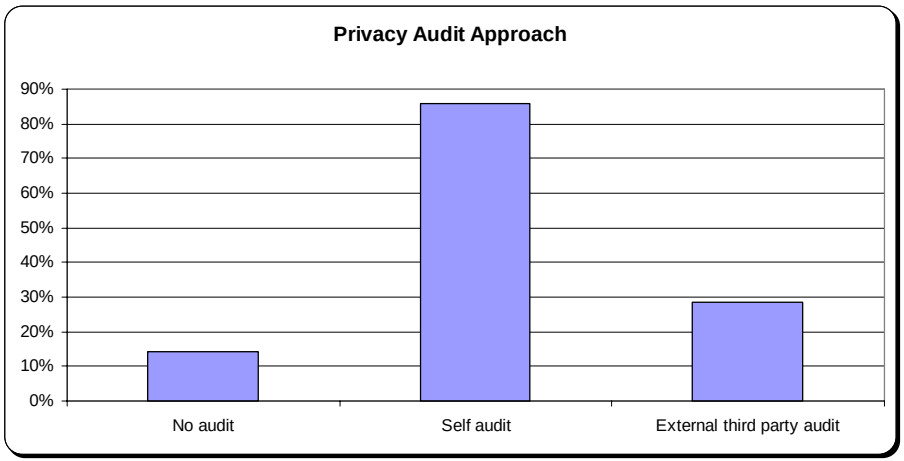


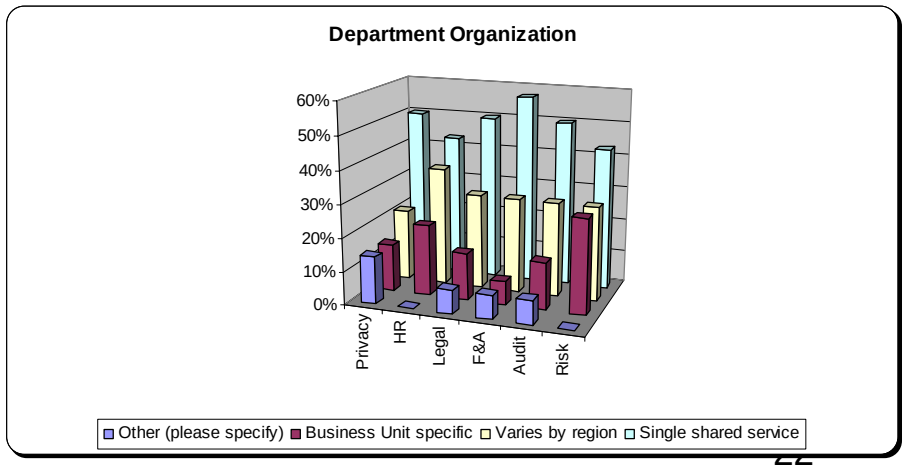
Privacy Approach

Structurally privacy groups are similar to other support groups but there is inconsistency between privacy policies that vary by region when multiple regimes are involved.



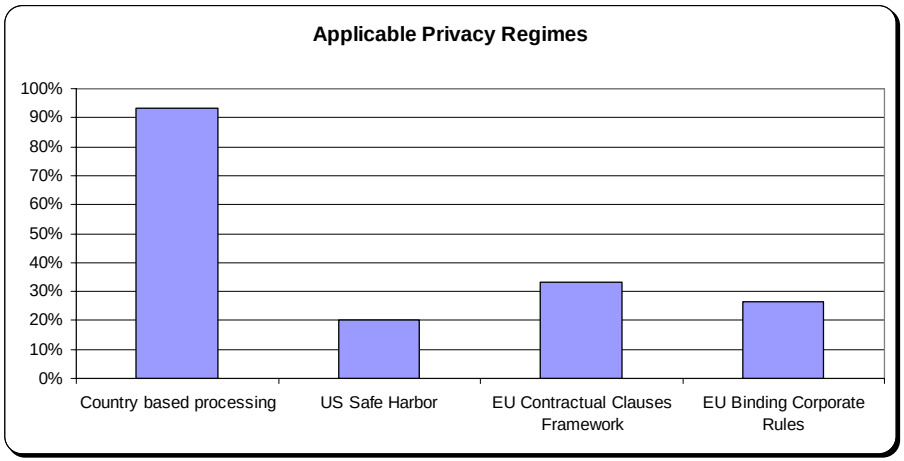


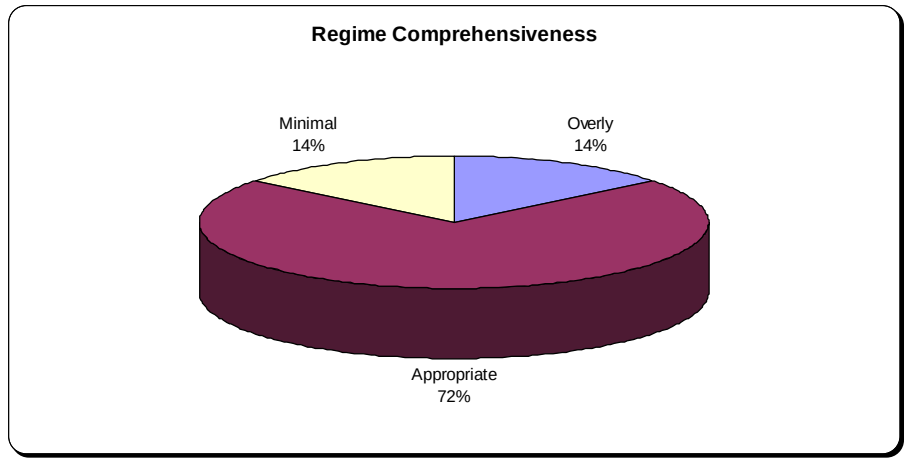


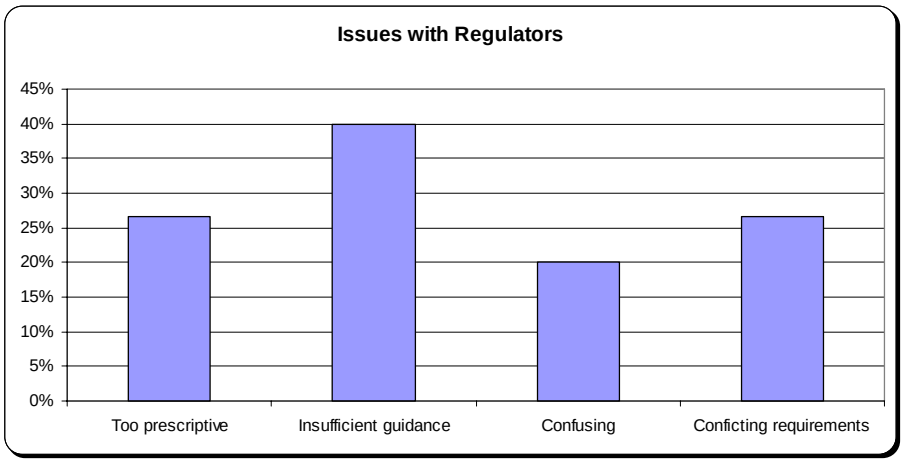


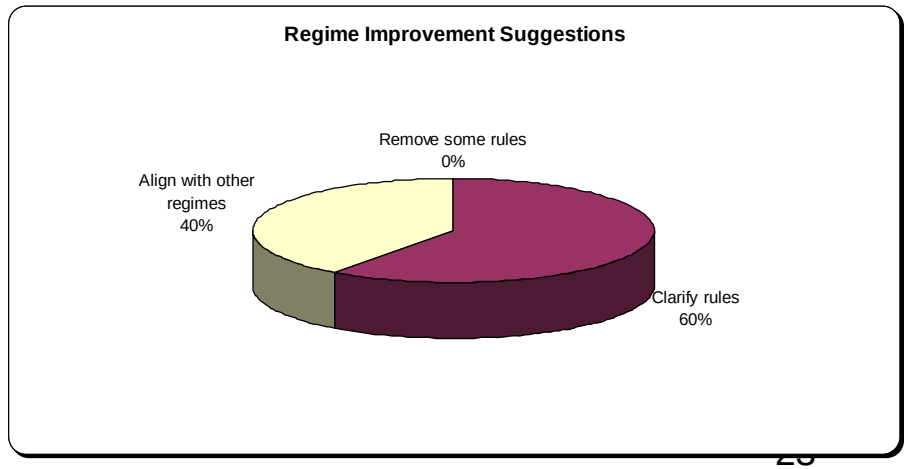
Privacy Regime Views

Regimes are generally perceived to be appropriately comprehensive but clarification and alignment are the dominant improvement suggestions with a variety of regulator issues.









Thank you

Mitch Chihara
NEC Corporation
A member of GBDe

m-chihara@ah.jp.nec.com
+81-3-3798-6525

GBDe
Global Business Dialogue on Electronic Commerce

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

OECD Approach to Cross-border Data Flows

APEC Data Privacy Seminar

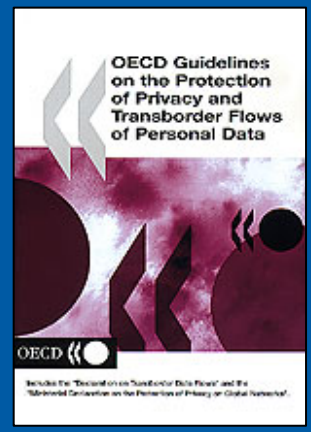
Lima, Peru

12-13 August 2008

OECD privacy building blocks

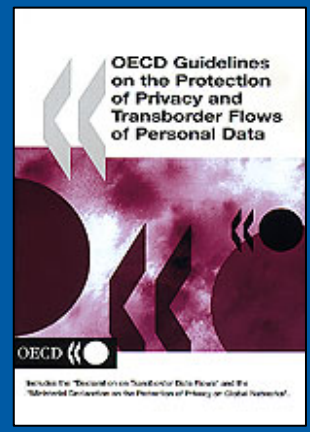
- Privacy Guidelines (1980)
- Ministerial Declaration on Trans-border Data Flows (TBDF) (1985)
- Ottawa Ministerial Declaration (1998)
- Recommendation on Cross-border Privacy Enforcement Co-operation (2007)
- Seoul Ministerial Declaration (2008)

Privacy Guidelines



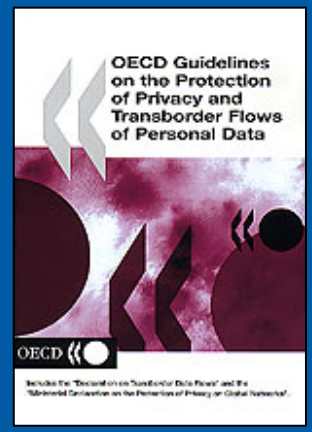
- don't restrict TBDF except where the other member does not substantially observe the Guidelines
- restraints may be imposed where there is no equivalent protection for sensitive information
- procedures for TBDF and privacy should be simple and compatible with those of other members that are compliant

Declaration on TBDF



- Recognised
  - the progress in privacy protection
  - the growing importance and benefits of TBDF
- Declared intention to
  - seek transparency in the regulation of TBDF
  - avoid unjustified restrictions on the free flow of information
  - work to develop common approaches to TBDF

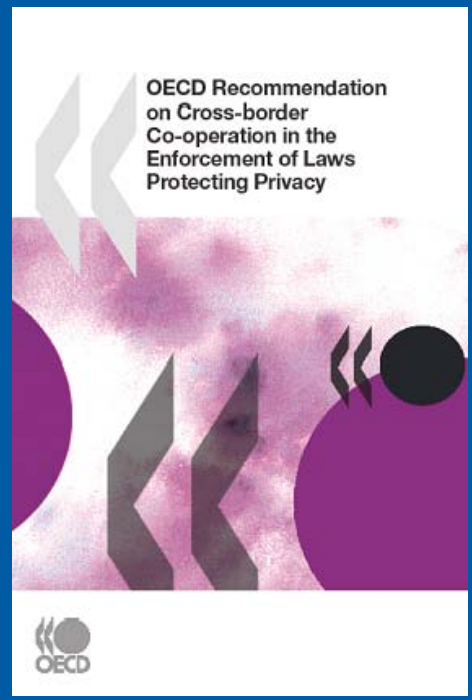
Ottawa Declaration on Privacy and Global Networks



- Recognised
  - that different effective approaches to privacy protection can work together to achieve effective protection on global networks
- Reaffirmed commitment to
  - the protection of privacy on global networks
  - prevent unnecessary restrictions on TBDF
- Work together to
  - build bridges between different approaches

Recommendation on Privacy Law Enforcement Co-operation (2007)

- recognises the benefits of increased TBDF and new challenges to privacy protection
- calls for co-operation despite variations in domestic approaches
- identifies key elements for successful law enforcement co-operation



implementation

- Developing a contact list
  - Single national point of contact
  - Internal list and public list
  - Co-ordinating with other contact lists (e.g. APEC)

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
  - Identifies key categories of information to be provided
  - Ensures careful pre-request preparation
  - Flexible: can be adopted to fit the situation (referral, audit, etc.)

Privacy Law Enforcement Co-operation

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

consulting with privacy officers

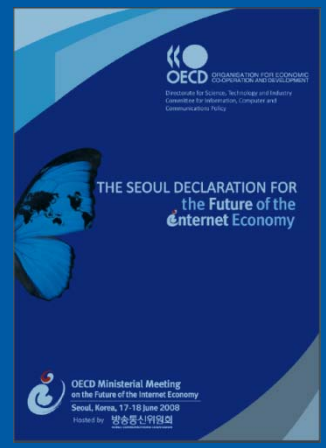
- Privacy Enforcement Authorities should consult with privacy officers in organisations
  - on how to resolve privacy-related complaints
  - at an early stage, with maximum ease and effectiveness
- Joint meeting between privacy authorities and privacy professionals
  - 27 May 2008, OECD Conference Centre
  - Chaired by Canadian Commissioner Jennifer Stoddart

OECD Ministerial Meeting
on the Future of the Internet Economy

Seoul, Korea, 17-18 June 2008

www.oecd.org/FutureInternet

Seoul Declaration

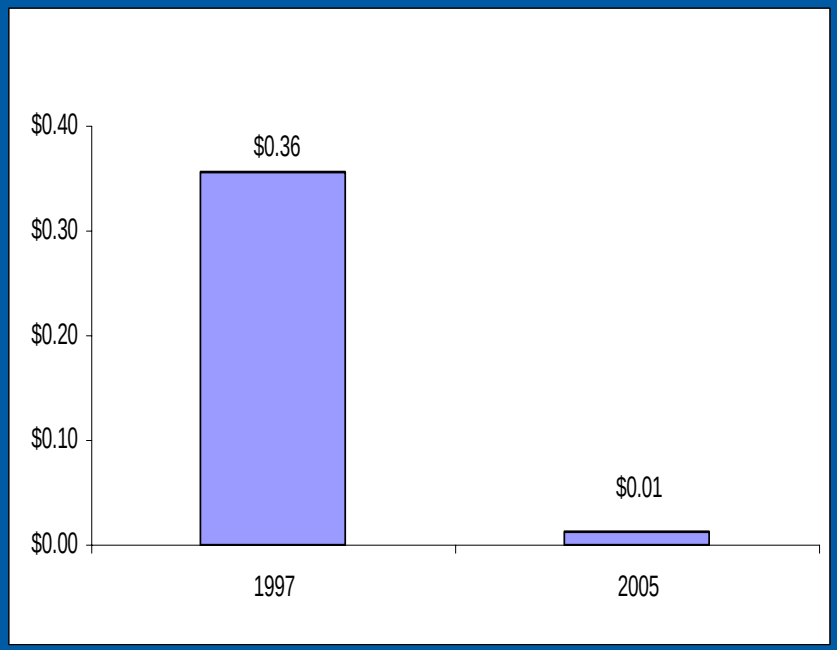


- Increase cross-border co-operation of governments and enforcement authorities in the areas of . . . protecting privacy

- Reinforce co-operative relationships and mutually beneficial collaboration with the Asia-Pacific Economic Co-operation

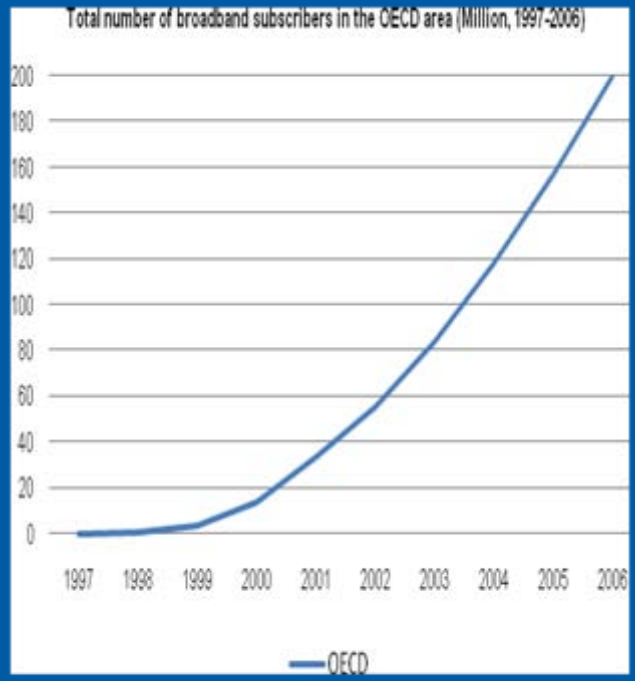
fast internet connections

cheap



Price of “always on” Internet access (per kilobit / second, USD, US incumbent operator)

widespread



Source: OECD Broadband Portal, www.oecd.org/sti/ict/broadband

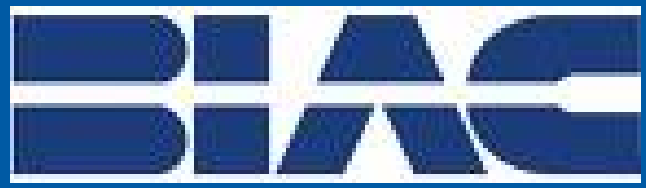
“Technology will outpace in its capacity the imagination of even the most clever law makers”

Hon. Justice Michael Kirby

- Australian High Court Judge
- Chair of the privacy expert group that developed the 1980 OECD Guidelines

- At the Internet Industry Association, Sydney, 21 February 2008

global dialogue



michael.donohue@oecd.org

+33 1 4524 1479

www.oecd.org/sti/privacycooperation

www.oecd.org/sti/security-privacy

DSCI Framework

Kamlesh Bajaj
CEO, DSCI

APEC Privacy Seminar

Lima, Peru, 12th August, 2008

Agenda

- NASSCOM
- 4E Framework for Trusted Sourcing
- DSCI – SRO Approach
- DSCI Mission and Activities
- India's Legal Framework for Data Protection
- DSCI Framework

About NASSCOM

- National Association of Software and Service Companies
- Apex trade development body of the Indian IT-BPO industry
- Established in 1988 with 38 companies, now has 1200 members
  - Of these, 250 are global companies with presence in India
  - NASSCOM membership accounts for 95% of India's IT revenues
- NASSCOM and its members have client relationships with over 60% of the Global Fortune 2000 corporations
- Direct employment: 2 million
- Indirect employment over 8 million additional jobs
- IT and ITES saw a total revenue of USD 52 billion in fiscal year 2007-08.
  - Exports comprised USD 40.3 billion
  - Export Growth over the previous year was 28.7%

4E Framework for Trusted Outsourcing

Engagement

- ❑ Customers / Governments / Regulators in Different Countries
- ❑ Industry bodies / Think Tanks / Law firms
- ❑ Steering Committee
  – Leading Academics, Consulting Firms, Security Experts and Industry

Education

- ❑ Focus on members:
  – Secure Sourcing
  – Research Reports
  – Guidelines for Contracts
  – SLAs, Best Practices
- ❑ Educational collateral for judiciary and police in India
- ❑ Continuous media briefing around security and privacy
- ❑ Cyber Safety Weeks

Enactment

- ❑ Working with Ministry of IT and Ministry of Law.

– IT Act 2000 being strengthened to bridge the gap – New sections brought in to cover emerging crimes, procedural improvements introduced, responsibility cast on companies to protect information

Enforcement

- ❑ Promote and Prescribe Security Standards, Best Practices, Self Checks
- ❑ DSCI Certification against prescribed standards after independent audits
- ❑ Membership of DSCI to signify trustworthiness to customers abroad
- ❑ Removal of DSCI Certification and/or Membership to act as market-driven enforcement
- ❑ Complaints and Dispute Resolution

Data Security Council of India
Self Regulatory Organization

- An independent body that seeks to create the culture of security and privacy in the Indian IT industry; will propose a basic set of security and privacy standards, to which companies can choose to adhere.
    - Board of Directors - industry leaders as well as representatives from the academic, government, and/or consumer communities.
    - Chairman of DSCI – from outside the industry and independent
    - Steering Committee comprising eminent experts from industry, academia, law enforcement and government
  - Develop, establish, monitor and enforce necessary minimum standards for privacy and security including best practices
  - Advocacy with government on data protection framework
- Key objective: Raise the floor when it comes to strengthening India as a secure outsourcing destination, across the IT Industry
- Not-for-Profit, Self Regulatory Organization in Data Security and Privacy Protection
- Diversified Membership including companies in IT, and BPO Sector
- DSCI Certification to Members

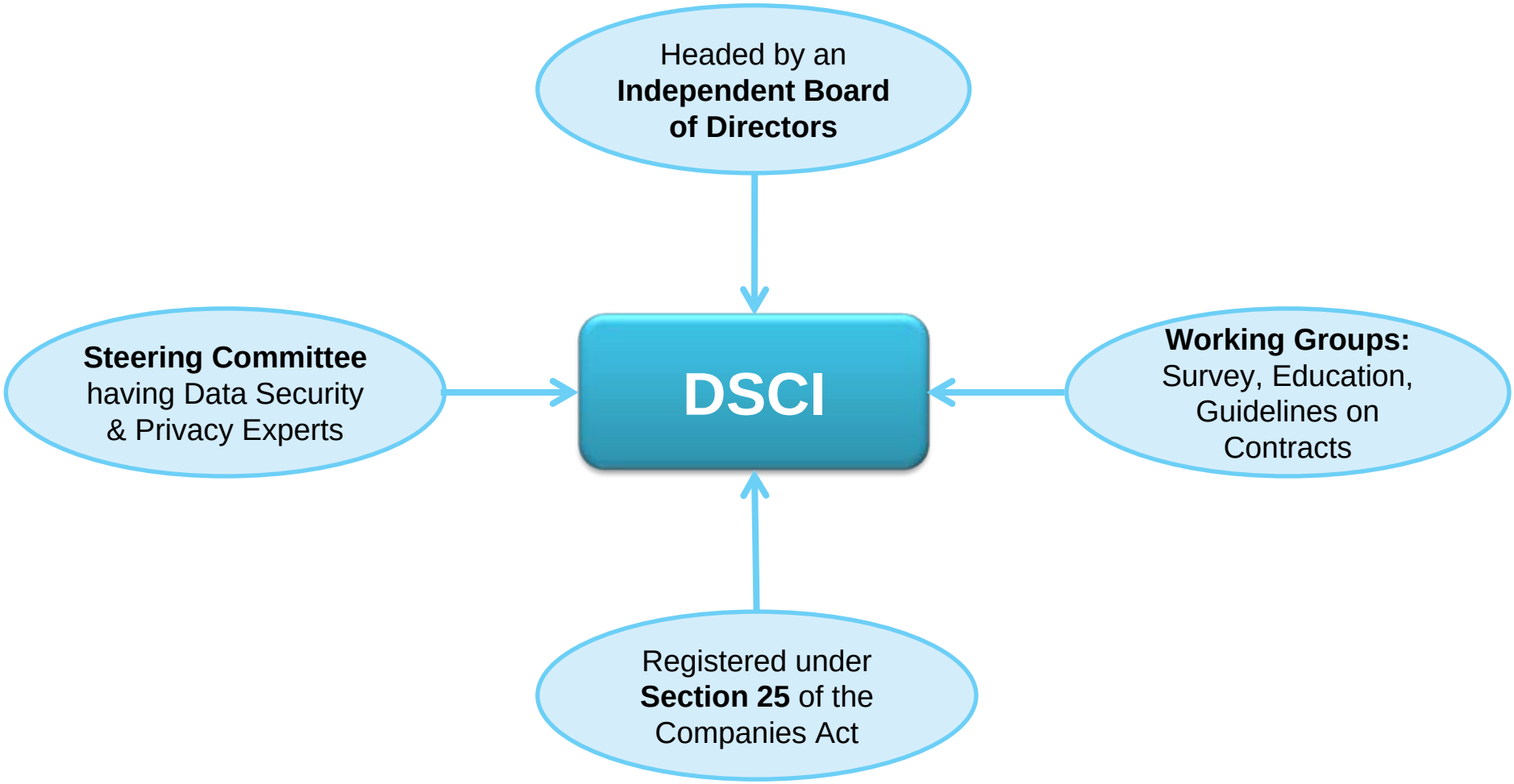
Pros and Cons of Self Regulation

- **For**
  - Promote best practices, independent audits, and certification based on audits
  - Specific guidance tailored to a particular market; best practices target clients' privacy requirements
  - Promote confidence in market rules and institutions
  - Provide access to quick dispute resolution mechanisms
  - Sanctions may be more appropriate than those proposed by government
  - Less costly than government regulation due to industry's focus on minimising costs benefiting firms and customers
- **Against**
  - May lack teeth; may not align with customers' and government priorities

DSCI Mission

- **What:**
  - Message to clients worldwide that India is a secure destination for outsourcing where privacy and protection of customer data are enshrined in the best practices followed by the industry
  - Create an accountability framework
  - Monitor and enforce compliance through promotion of self regulation of industry, and to act as a self regulatory organization (SRO)
- **How:**
  - Create awareness - Organizations and individuals
  - Build capacity
  - Provide certification services
  - Create a common platform for sharing knowledge
  - Inform external stakeholders

DSCI Structure



DSCI Working Groups

- **Surveys**
  - To understand the current status of data security
- **Education**
  - To organize events, hold training programs, promote certifications
- **Guidelines for contracts**
  - To create a repository of different types of contractual agreements

Surveys

Goals

- To understand the current state of data security controls in place in India
- To benchmark the industry
- To understand the industry expectation for DSCI
- To understand the critical aspects of data security, which organizations find challenging to implement and monitor

Methodology

- **Three level questionnaire**
  - CEO level
    - Personal interview about business logic of security
  - HR Head
    - About training and administrative issues
  - IT Security Head
    - Security controls
    - Operational issues
- **NASSCOM Member organizations**
  - Email / web based questionnaire
  - 50 - 60 in number

Questionnaire

- **Enterprise security**
  - Security and privacy in policy implementation
  - Security and privacy in HR function
  - Security and privacy in compliance
- **Operational security**
  - Information asset management
  - Physical security
  - Operations management
  - System development and maintenance
  - Access controls
  - Business continuity

Education

Goals

- DSCI Annual Security and Privacy Conference
- Plan and conduct awareness programs for conformance to best practices and security standards, accreditation and certification
- Organize chapters for enhanced security awareness in different regions
- Publish a newsletter

Training

- Conduct training for members to attain DSCI Certification
- End-user awareness on security and privacy
- Security and Privacy Managers
- Programmers in secure application development

Certification

- DSCI Certification for service providers
- Data security and privacy for managers
- Programmers in secure coding practices
- End-user security and privacy

Guidelines for Contracts

Objective

- To support its diverse membership by providing them with practical resources that will help in areas of contracting
- To provide NASSCOM members with model contracts , standard clauses and covenants, which they can further customize based on their business needs and client requirements

Approach

- Member organizations willing to participate in the initiative will be identified for a survey
- A survey questionnaire will be distributed to the participating members
- A follow-up telephonic or in-person interview will be conducted to validate and ask further questions
- The data collected will be compiled and then used for making further recommendations regarding this initiative

India's Legal Framework for Data Protection and Data Privacy

Indian Constitution	Supreme Court of India Judgements, articulating 'protection of privacy' as one of the features of the Fundamental Rights [Article 21 – Life and Liberty] to "protection of life and personal liberty"
Indian IT Act, 2000	❑ Section 65 - Tampering with computer source code ❑ Section 66 - Hacking & computer offences ❑ Section 43 – Tampering of electronic records ❑ Section 72 – BPO Data Protection
Indian Copyright Act	❑ Any person who knowingly makes use of an illegal copy of computer program shall be punishable. ❑ Computer programs have copyright protection, but no patent protection.
Indian Penal Code	❑ Section 406 - Punishment for criminal breach of trust ❑ Section 420 - Cheating and dishonestly inducing delivery of property
Indian Contract Act, 1872	Offers following remedies in case of breach of contract: ❑ Damages ❑ Specific performance of the contract

Data Protection Framework

Indian Approach

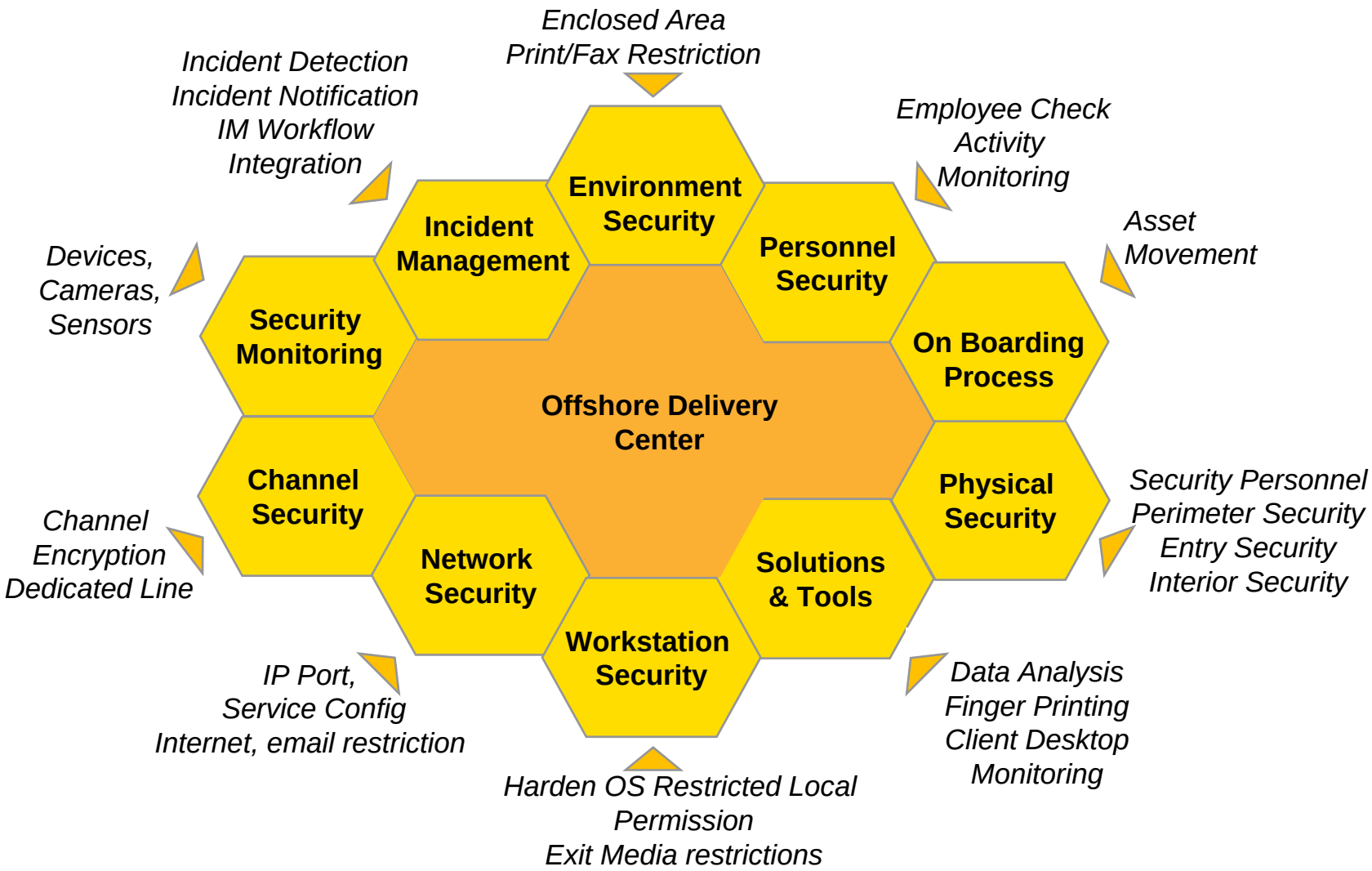
- Different privacy cultures
- Commercial transactions require - information privacy and security obligations be determined by point of origination of data,
- Particular expectations for privacy truly local, while data flows global.
- Difficult to govern cross-border data flows under any one country's laws or legal frameworks.
- Challenge for IT and ITES companies to meet privacy and information security obligations

- Widespread agreement around international data protection and IS Principles; OECD Privacy Principles, APEC Privacy Principles.
- CPRs, grounded upon the APEC and OECD principles as a foundation, can achieve basic compliance with substantive requirements that might be found in any country.
- An IT or ITES service provider can design its operations in the same way. Assess its adherence to common data management principles

Security Controls for Data Protection

- Risk Assessment and Risk Management
- Security management
- Controlling access to information
- Ensuring business continuity
- Compliance
- Staff selection and training
- Information security incident management

Security Requirements at a BPO Center



Global Compliance Model for all BPO/ODCs:

- ISO 27001 audits periodically
- Customer audits on demand

National Skills Registry (NSR)

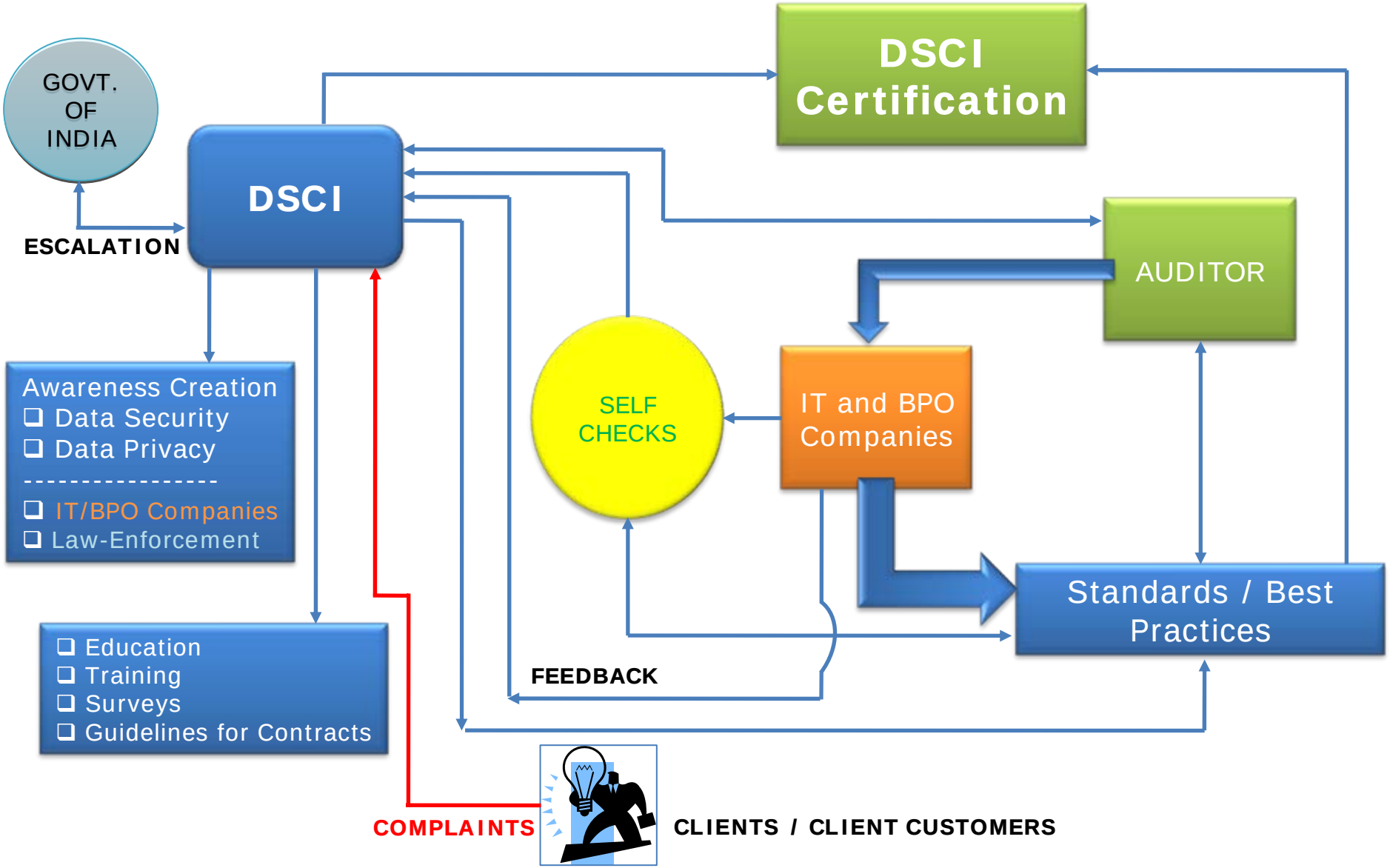
Background Checks of Employees

- Database of pre-verified resumes.
  - Data ownership with IT Professional.
  - Fingerprint for unique identification.
- Web based secure interface
- Subscriber
  - Image Enhancement
  - Pool of country's IT Skills
  - Safer & Efficient Recruitment
  - Standard Verification Process
  - Cost & Time Saving
- IT Professionals
  - Reduced Recruitment Time
  - Transparent Verification Process
- Current Status
  - 70 large employers have pledged to recruit through NSR
  - Enrolments till July, 2008: 350,000
  - Fingerprinting: 100,000
- DSCI: to audit the background checking companies, their processes

Proposed Amendments to the IT Act

- Changes in definitions and introduction of technology neutrality
  - Intermediary
  - Electronic Signature
- Section 43A: Liability of companies
  - For not following ‘reasonable security practices and procedures’
  - Defines ‘sensitive personal data or information’
  - Recognizes the role of ‘professional bodies and associations’
  - Upto Rs 50 million to each person wrongfully affected by the breach
- Section 66: More specific definition of data crimes
- New offences introduced
  - Cyber stalking (section 66A)
  - Privacy invasion
  - Identity theft
- Powers to direct interception or decryption (s. 69)
- Identification and protection of Critical Information Infrastructure (s.70)
- Clarification of the role and liability of the intermediaries (s. 79)
- Strengthening of investigation mechanism
  - Delegation to junior officers (s. 78)
  - Creation of Examiner of Electronic Evidence (s. 79A)

DATA SECURITY COUNCIL OF INDIA - SRO



DSCI - Critical Success Factors

Relevance of Best Practices Framework	Visibility in Outsourcing Market	Research and Development
Large Service Providers: ❑Best Practices Framework relevant for large companies, who already may have certifications such as ISO 27001. ❑Framework to be developed in collaboration with client companies outsourcing to India, to address their unique requirements **Small and Medium SPs:** ❑Framework to meet with their requirements too; help them project as SPs with sound practices, conforming with international standards.	❑ Special focus on understanding the requirements of USA and Europe - the two geographies which dominate the outsourcing industry. ❑ Work with some of the leading companies, associations in USA and Europe, for development of the DSCI Privacy Framework ❑ To be a credible SRO promoting security and privacy in the IT/BPO industry in India, with wide acceptance amongst client firms outsourcing to India.	❑ R&D to develop the best practices framework relevant to the industry ❑ Develop training material for member organizations, to enable them comply with the best practices. ❑Work with Auditors on DSCI Certification as per prescribed practices ❑ Get inputs from leading authorities in this field, including industry experts, legal and consulting firms and academic bodies.

Thank You

LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

APEC-Lima-12-08-08.

Prof. Lourdes Zamudio Salinas

Objetivo

Que el intercambio transfronterizo de información no pueda verse limitado por la legislación nacional de protección de datos, pero al mismo tiempo, que se garantice la adecuada protección de este derecho fundamental.

¿Hacia un marco homogéneo de regulación del derecho a la protección de datos personales?

Prof. Lourdes Zamudio Salinas

Vías complementarias:

-Instrumentos supranacionales de carácter vinculante.

-Leyes nacionales que consagren y garanticen el contenido esencial de este derecho.

Escenario supranacional general pertinente

-ONU. Resolución 45/95

-OCDE. Organización para la Cooperación y el Desarrollo Económico: Directivas relativas a la protección de la privacidad y flujos transfronterizos de datos personales.

-Acuerdo general sobre comercio en servicios (GATS). artículo XIV- c – ii.

-APEC. Foro de cooperación Asia-Pacífico. Marco de privacidad.

ACUERDOS Subregionales o bilaterales

-Acuerdo de diálogo político y cooperación entre la Unión Europea y sus estados miembros, por una parte, y las Repúblicas de Costa Rica, El Salvador, Guatemala, Honduras, Nicaragua y Panamá, por otra parte.

- Acuerdos de Asociación económica, concertación política y cooperación entre la Unión Europea con México (Art. 51) y Chile (Art.30) .

Instrumentos internacionales que involucran a Estados L.A. y que contienen disposiciones sobre privacidad e intimidad.

-Declaración universal de los derechos humanos. Art. 12.

-Pacto internacional sobre derechos civiles y políticos. Art. 17.

-Convención americana sobre derechos humanos. Art. 11.

PROTECCIÓN DE LOS DATOS PERSONALES A NIVEL DE LA LEGISLACIÓN INTERNA EN AMÉRICA LATINA.

Prof. Lourdes Zamudio Salinas

Características de la regulación protectora en América Latina (AL)

a) **Situación de asimetría.**

b) **Consideración política del tema a nivel regional.**

c) **Prevalencia inspiradora del modelo europeo.**

a) Situación de asimetría.

- La mayoría de los Estados LA reconocen, por referencia directa de su Constitución, o como consecuencia de las decisiones adoptadas por sus órganos jurisdiccionales, el derecho a la protección de datos de carácter personal, esencialmente mediante el reconocimiento del recurso al "*habeas data*", mediante el cual el titular podrá tomar conocimiento de los datos referidos al mismo y de la finalidad para la que están siendo tratados por un determinado responsable del tratamiento, pudiendo en su caso instar su rectificación, cancelación o actualización.

… a) Situación de asimetría.

- El ejercicio de este derecho ha dado lugar a una rica jurisprudencia que ha evolucionado hacia el reconocimiento de una serie de principios a los que deben someterse las Administraciones Públicas y las entidades privadas que tratan datos de carácter personal. (Red Iberoamericana de Protección de datos).

b) Consideración política del tema a nivel regional.

XIII Cumbre Iberoamericana en Santa Cruz de la Sierra, (Bolivia) Jefes de Estado y de Gobierno de 21 países iberoamericanos (noviembre de 2003). Declaración de Santa Cruz de la Sierra : "45. *Asimismo somos conscientes de que la protección de datos personales es un derecho fundamental de las personas y destacamos la importancia de las iniciativas regulatorias iberoamericanas para proteger la privacidad de los ciudadanos contenidas en la Declaración de La Antigua por la que se crea la Red Iberoamericana de Protección de Datos, abierta a todos los países de nuestra Comunidad*".

c) Prevalencia inspiradora del modelo europeo.

- El Convenio 108 del Consejo de Europa y su Protocolo Adicional de 2001, así como la Directiva Comunitaria sobre Protección de Datos Personales, contienen una serie de principios que gozan en la actualidad de general aceptación y suponen una guía para los Estados latinoamericanos a la hora de emprender la regulación legal de esta materia.
- Adecuación y autorizaciones .

- Red Iberoamericana de Protección de datos.

Situación legislativa asimétrica

I.- País con Ley de Protección de datos de carácter especial y con autoridad de control administrativa.

ARGENTINA

- Ley N° 25326, sancionada el 4 de octubre del 2000 y posteriormente reglamentada por el Decreto N° 1558/2001.
- Comisión Europea consideró, en su Decisión 2003/490/CE del 30 de junio de 2003, que la legislación argentina ofrecía un nivel de protección de datos adecuado.

…Ley Argentina: Contenido

-Principios generales de protección de datos.

-Los derechos de los titulares de datos.

-Las obligaciones de responsables y usuarios de datos.

-El órgano de control.

-La sanciones.

y el procedimiento del recurso judicial habeas data.

…Argentina. Transferencia internacional: Art. 12

Es prohibida con países u organismos internacionales o supranacionales, que no proporcionen niveles de protección adecuados.

No rige la prohibición:

Art. 12, numeral 2 de la ley y Art. 12 del Reglamento.

La DNPDP está facultada para a evaluar, de oficio o a pedido de parte interesada, el nivel de protección proporcionado por las normas de un Estado u organismo internacional.

(…Argentina) La **DNPDP**

En caso que una base de datos no cumpla con los requisitos que establece la ley para la protección de sus datos personales, el titular podrá ejercer las siguientes acciones:

-Denunciar el hecho ante la DNPDP. sanciones administrativas al registro, archivo, base o banco de datos. (Ley Nº 25.326 Art. 31). Apercibimiento, suspensión, multa, clausura o cancelación del archivo, registro o banco de datos.

-Acción Judicial de Hábeas Data.

II. Legislaciones con protección legislativa parcial y explícita.

MÉXICO

- Existe regulación para el sector público.
- Hay regulación parcial para el sector privado con diversas autoridades.
- La ley federal de transparencia y acceso a la información pública contiene un capítulo de protección de datos personales aplicable al sector público a nivel federal con una autoridad independiente en el Poder Ejecutivo que es el IFAI.

CHILE

- **Ley Nº 19628 sobre protección de la vida privada (publicada 28-agosto-99).**
- **Regula a los bancos de datos a cargo de organismos públicos o de particulares.**
- **Reconoce los derechos de información o acceso, modificación, cancelación o bloqueo de sus datos personales, pero ante la no atención de los mismos por parte del responsable del registro o del banco de datos, no hay una autoridad de control administrativa, ni sanciones de este tipo, sino que debe recurrirse al poder judicial (juez civil) para iniciar una acción de amparo que ha venido a denominarse jurisprudencialmente como el Hábeas Data.**

II. a) Países con reconocimiento constitucional explícito del derecho a la protección de datos personales

-México Art. 6.

-Panamá. Art. 41 A.

-Perú. Art. 2, inciso 6).

II. b) Países con reconocimiento constitucional explícito del recurso del Hábeas Data.

-Bolivia. Art. 23.

-Panamá. Art. 44 C.

-Perú. Art. 200, numeral 3).

-Colombia. Art. 15 (Pero como derecho fundamental).

-Brasil. Art. 5, LXXII.

II. b) Países con reconocimiento constitucional explícito del derecho a la intimidad y/o a la privacidad.

- Nicaragua. Art. 26, inciso 1).
- Honduras. Art. 73.
- Costa Rica. Art. 24.
- Brasil. Art. 5, X.

LOS QUE NO TIENEN EXPRESAMENTE RECONOCIDOS EL DERECHOA A LA INTIMIDAD O EL ESPECÍFICO DE LA PROTECCIÓN DE LOS DATOS PERSONALES SUELEN DECIR LO SIGUIENTE:

Sí existe protección de manera implícita a través de la integración de los principios consagrados en los tratados internacionales, ratificados por cada país como parte del ordenamiento jurídico nacional;

en estos países, puede hacerse valer el derecho jurisdiccionalmente a través del recurso general del Amparo.

Es común la referencia legislativa parcial, sectorial y dispersa en los ordenamientos jurídicos Latinoamericanos. Leyes (de) :

-Centrales privadas de información crediticia.
-Transparencia y acceso a la información.
-Protección al consumidor.
-Telecomunicaciones.
-Salud.
-Sistema estadístico.
-Sistema de identificación de las personas.
-Spam.

… común la referencia legislativa parcial, sectorial y dispersa en los ordenamientos jurídicos Latinoamericanos. Leyes (de) :

-Código Penal.

-Código de niños, niñas y adolescentes.

-Código Tributario.

……..

Algunos Proyectos de ley en curso

URUGUAY

Proyecto de ley “Protección de bases de datos personales”. Aprobado.

PERÚ

“Proyecto de ley de protección de datos personales”.

AUTORREGULACIÓN

- Existen documentos internacionales que promueven el uso de instrumentos de autorregulación en el ámbito de la protección de datos personales.
- Normas nacionales generales:

-Argentina: Artículo 30 de la ley 25326 de 2000.

-Perú: Disposición segunda complementaria final del Reglamento de la ley 28493 que regula el spam.

Muchas gracias

mariadelourdes.zamudio@gmail.com

Inquisidora2006@yahoo.es

Approaches to Cross-Border Data Privacy

Brenda Kwok
Chief Legal Counsel
Office of the Privacy Commissioner for Personal Data,
Hong Kong, China

at Second Technical Assistance Seminar
on the International Implementation of the
APEC Privacy Framework 2008
Lima, Peru
12 & 13 August 2008

香港個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data, Hong Kong

Hong Kong Data Protection Law

- **Personal Data (Privacy) Ordinance**
- **Enacted in 1995**
- **Core provisions came into effect on 20 December 1996**

Hong Kong Data Protection Law (Con't)

- **Data users shall observe six data protection principles:-**
  - ✧ **data collection**
  - ✧ **accuracy & retention**
  - ✧ **use**
  - ✧ **security**
  - ✧ **privacy policy**
  - ✧ **access and correction**

Hong Kong Data Protection Law (Con't)

- **Establishment of the Office of the Privacy Commissioner for Personal Data**
- **Privacy Commissioner is independent**
- **Powers to carry out investigation of complaints and to undertake enforcement actions**

Transfer of Personal Data to a place outside Hong Kong

- **Section 33 of the Ordinance not yet effective**
- **Cover:-**
  - ✧ **transfers of personal data from Hong Kong to a place outside Hong Kong; and**
  - ✧ **transfers of personal data between two other jurisdictions where the transfer is controlled by a Hong Kong data user.**

Transfer of Personal Data to a place outside Hong Kong (Con't)

- **Prohibit the transfer of personal data outside Hong Kong unless one of the following requirements is satisfied:-**

  (a) the place to which the data are transferred has in force any law which is substantially similar to or serves the same purposes as the Ordinance. The Privacy Commissioner may specify a place satisfying this requirement by notice in the gazette;

Transfer of Personal Data to a place outside Hong Kong (Con't)

(b) the data subject has consented in writing to the transfer;

(c) the data user has reasonable grounds for believing that the transfer is for the avoidance or mitigation of adverse action against the data subject; it is not practicable to obtain the data subject's consent, but if practicable, such consent would be given;

Transfer of Personal Data to a place outside Hong Kong (Con't)

(d) the data are exempt from data protection principle 3 by virtue of an exemption under the Ordinance; and

(e) the data user has taken all reasonable precautions and exercised all due diligence to ensure that the data will not be dealt with in a manner that would constitute a contravention of the Ordinance.

Transfer of Personal Data to a place outside Hong Kong (Con't)

- **At present, transfer of personal data outside Hong Kong should comply with data protection principle 3**

- **Data users state explicitly in its personal information collection statement the purpose of use and the intended transfer outside Hong Kong**

Outsourcing

- **Businesses outsource their functions and activities to other companies outside Hong Kong**
- **Vicariously liable for any act done or practice engaged in by their agents**

Outsourcing (Con't)

- **Matters to note:-**

  - ✧ **customers be informed of the data processing agent as a class of persons to whom data are intended to be transferred;**

  - ✧ **select a reputable contractor or agent;**

  - ✧ **limit disclosure of data to the extent that are necessary for the purpose;**

Outsourcing (Con't)

- **Contractual obligations:-**
  - ✧ **obliging the outsourced contractor or agent to comply with the requirements of the Ordinance;**
  - ✧ **prohibit the contractor or agent to use or disclose the data for other purpose;**
  - ✧ **require a timely retrieval or return or destruction of the customers' personal data no longer required;**

Outsourcing (Con't)

- ✧ **oblige the contractor or agent to undertake adequate security measures;**
- ✧ **require the immediate reporting of any sign of abnormalities and security breaches;**
- ✧ **prohibit sub-contracting of services except with consent;**

- **Implement control measures to ensure that the outsourced contractor or agent has performed the terms of the contract**

International Approach

- **Technological advancements - calls for higher level of personal data privacy protection and stronger sanction and legislation**

- **A consistent global privacy approach is desirable**

APEC Privacy Initiative

- **Since 2003, the HK Privacy Commissioner's Office has been participating in the APEC project initiative**
- **APEC Privacy Principles are by and large consistent with the six data privacy principles under Hong Kong law**
- **ECSG Data Privacy Subgroup is now working on cross border privacy rules (CBPRs)**

APEC Privacy Initiative (Con't)

- **APEC Privacy Framework encourages cross border co-operation amongst the participating economies on enforcement of privacy rights**
- **A successful APEC model will help to provide insights for tackling the question of transborder data flow in a wider context**

Legal Obstacles

- **Secrecy requirement**

- **Section 46(1) of the Hong Kong data protection law prohibits the Privacy Commissioner or his prescribed officers from disclosing information that comes to their actual knowledge in the performance of their functions and the exercise of their powers**

Legal Obstacles (Con't)

- **Exceptions:-**

  (a) disclosure in the course of proceedings for an offence under the Ordinance;

  (b) reporting evidence of crime to such authority as the Commissioner or prescribed officer considers appropriate; and

  (c) disclosure to a person on matter which the Commissioner or prescribed officer opines may be a ground of complaint by that person.

Legal Obstacles (Con't)

- **Breach of secrecy – a criminal offence liable on conviction to a fine and imprisonment**
- **Restriction on investigative assistance**
- **No provision permitting a data user to provide personal data pursuant to the requests made by foreign regulatory or law enforcement bodies – except Mutual Legal Assistance**

~ End ~

How Stakeholders Understand Data Privacy

Claro V. Parlade

Cyberspace Policy Center for Asia Pacific

Privacy in the Philippines

- Implied in Constitution
- Not defined by law

Data Privacy Survey

- Meant to provide a snapshot of the private sector's understanding of the concept of "data privacy" and its scope, the desirability and form of regulation, and the government's role in data privacy regulation.
- Initial target consisting of ICT and business associations, including banking and financial services

Focus on

- Concept of Data Privacy
- Opinion on need for notice and/or consent
- Need for regulation
- Form of regulation
- Implementing Agency
- Breach notification

What is data privacy?

- Despite absence of any law defining data privacy, stakeholders believed it to be an integral part of a right to privacy
- This right imposes certain limitations on the use by the government of citizens' personal data (including name, personal circumstances, contact information).
- Stronger support for limitations on the collection and use by private individuals of an individual's personal data (including name, personal circumstances, contact information, credit card).

Notice and Consent

- There is strong support, across all respondent associations except for one, for the principle that a person ought to be notified of use of his or her personal information by third parties for *commercial and non-commercial* purposes by third parties.
- Considering, however, that all associations showed even greater support for the proposition that the *consent* should be required prior to use of personal information either for commercial and non-commercial purposes, it appears that disagreement by some with the notice principle is indicative of support for the stricter consent principle.

Need for Regulation

- There was overwhelming support for the adoption of comprehensive rules on all use of personal information by third parties so as to achieve a balance between privacy rights and the free flow of information required by businesses.

Form of regulation

- Most believe that privacy regulation should be in the form of law (93%), although 71% also believe that administrative regulation is appropriate.
- Nevertheless, a healthy 89% believe that private industries should adopt self-regulatory measures to protect data privacy, even as 81% believes that government action is necessary.
- Governmental action includes adoption of legislated or government imposed security standards (90%).

Implementing Agency

- Very strong support for commissioner model
- Unusual support for privacy commissioner with power to investigate, prosecute and resolve violations of data privacy, as well as power to impose fines and damages, and to publicize violations of data privacy.
- Similarly, there is very strong support for imposing criminal penalties for violation of data privacy rights.

Breach Notification

- A surprising 92% favored the imposition by law of obligation upon businesses to report breach of security of information systems or theft or personal information.

Thank You!

For questions, email me at:

Claro V. Parlade

cparlade@cpcap.org

cvparlade@phpeplaw.com

Data Privacy as understood by ~~Latin Americans~~ *Peruvians*

apece

Asociación Peruana de Comercio Electrónico

Limitations for e-commerce in Peru:

Insufficient legislation on issues of Privacy and Data Protection;

Insufficient Internet connections;

Low income and low penetration of banking and credit cards;

Low literacy in computing and net surfing;

Great sense of distrust of businesses and technology among consumers;

Informality and little or no legal security to customers.

Why should we care about Data Protection?

It ranks high in today's international agenda;

Is important to society, and, therefore, is crucial for business;

We have no systematized information in Peru regarding Data Privacy;

Personal data is a commodity transacted everyday by the informal sector and, to some degree, by the formal as well

Understanding Data Privacy in Peru: Legislation

The Political Constitution of Peru (Chapter I)

Article 2.6
Citizens have the right to prevent information services, public or private, from giving away information that may affect their personal or familiar intimacy.

Article 2.7
Citizens are entitled to personal honor and good reputation, to personal and familiar privacy and to their voice and personal image.

Any individual affected by the media may demand an immediate rectification.

Understanding Data Privacy in Peru: Legislation

Law 27489

Regulates private credit-information agencies;

Supreme Decree 052-2008-PCM

Published on July 19th 2008, it approved the third draft of the regulations for the Law of Digital Signatures and Certificates.

Understanding Data Privacy in Peru: Research & perception

Interest among scholars

No research dealing with Data Privacy has been conducted nationally.

Some valuable reports and comparative legislative analysis done at regional level that include Peru have been produced.

General perception of Data Privacy in Peruvian society

The most complex and least researched.

No scientifically collected data to draw from.

An indirect approach is required by considering certain key cultural traits.

Understanding Data Privacy in Peru: Key Cultural Traits

A postcolonial society, with some of its population immersed in Western thought and culture and a large population of native tradition.

A social order based in the rule of law evenly shared by everyone is an alien notion to us (no real “civil society”; instead, a “political society”).

A large number of groups competing for political power to foster their claims outside the boundaries of the establishment.

Democracy is just another means, one that hardly works efficiently due to the lack of trust.

Understanding Data Privacy in Peru: Consequences

1. We don’t have much faith in the system, and, as a result, do not have a well established sense of citizenship.

2. As individuals, we do not make claims easily through regular channels, not having a culture that supports consumer rights.

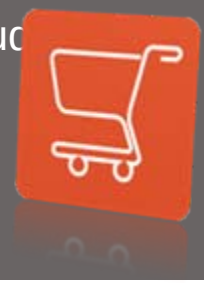
It is not difficult to see why Data Privacy is not an extensive practise, and why legislation needs to be enforced and society empowered.

Is everything regarding Data Privacy that negative?

Recent facts.

A few months ago, the academic achievements as a young student of a prominent authority were leaked to the media from a leading university, compromising an important measure to be enforced at the time.

Some companies, like Ontrack Peru, this year's winner of APEC's Digital Opportunity Centre Award for its good commercial practices and use of IT&C, are showing a change of attitud



APECE’s policy on Data Privacy

Data Privacy means good business.

We need to build trust on Peruvian e-commerce, something to happen by the strict observation of solid policies.

Civil society must be fortified by every means possible.

We will foster APEC’s guidelines on Data Privacy and will demand from Government the approval of the bill mentioned before.

Reasons to be optimistic

Natives leaving the highlands for the big cities embrace modernity, a fact that will have an impact on how we understand Data Privacy.

The law on digital signatures brings about protection and liabilities.

Peru is today open to commerce and investment, as well as to new demands, trends and ideas.

Free trade agreements with the US, Canada, Europe and China will help shape the way we regard and protect personal da

Final thoughts

The lack of civic awareness, the low level of schooling and the pervasive informality will demand a multidisciplinary and long term approach.

There is no alternative to good education if we want the empowerment of society.

This process will certainly take its time in light of Peruvian idiosyncrasy.

How to reach us

Los Negocios 151,
Surquillo
Lima 34, Perú
(511) 222 7811
info@apece.org.pe
www.apece.org.pe

VNTRUST AND THE ISSUE OF DATA PRIVACY IN VIETNAM

VIETNAM E-COMMERCE AND IT AGENCY
MINISTRY OF TRADE AND INDUSTRY

Content

- Stakeholders' perspectives of data privacy issue in Vietnam
- Legal framework for privacy protection
- TrustVn – a new approach to data privacy in Vietnam

I / Stakeholders' perspectives of data privacy issue in Vietnam

History

- Cultural background
  - Confucian morals -> downplay individual selfishness
  - Commune based society -> “closed” to the outsider but complete “open” within the community
  - Agriculture-based economy -> shared resources and shared information

  -> privacy is quite an alien concept
- Social conduct
  - Public possession (especially of intangible assets, e.g. information, intellectual property) is a strong notion until recently
  - Personal information is freely shared and widely circulated (at least among one’s circle of acquaintance)
    - Health conditions
    - Salary, income
    - Personal facts

Business practice of collecting and using personal information

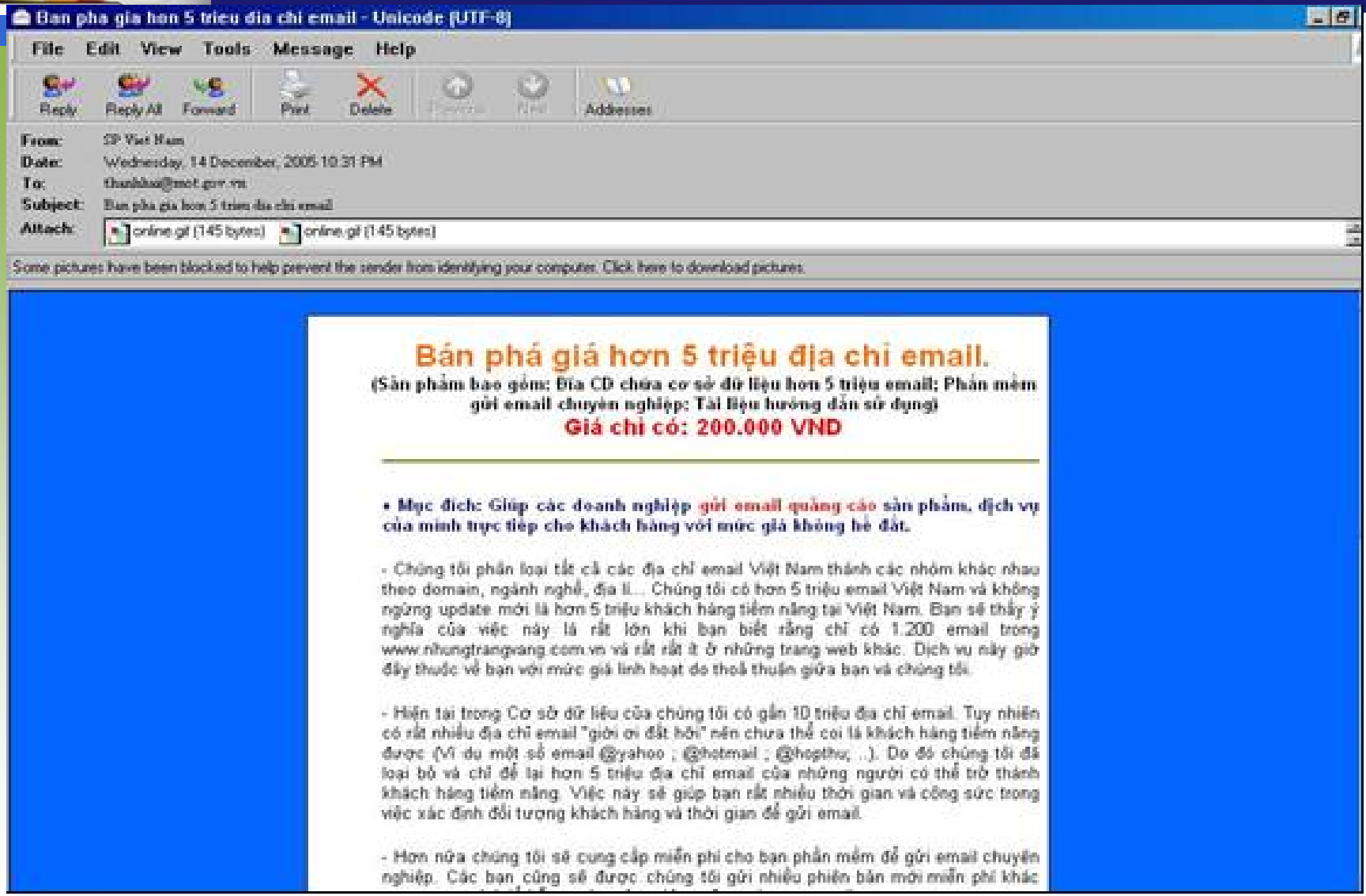
- A majority of businesses are SMEs
  - Less than 10 employees: 51%
  - Less than 500 employees: 98%

  -> doing business in the “traditional way”

  -> dealing with small groups of customers

  -> acquiring customer’s personal information on a person-to-person basis
- Practice of collecting mass customers’ data: quite a new practice (≈15 years)
- Awareness of privacy issues: used to be low and starts to rise in the recent years
- Awareness of businesses’ responsibility in protecting customers’ data privacy: still low
- International practice: a strong drive for the adoption of a “new” practice

An advertisement for sales of 5 mil. e-mail address database



Business perspective on information security

Obstacles to e-commerce development	Level of concern		
	2005	2006	2007
Social awareness	3.32	3.23	2.74
E-payment system	3.27	3.19	2.84
Information security	-	2.78	2.90
Legal framework	3.11	2.64	2.55
Business practice	3.09	2.45	2.48
Human resources	2.95	2.45	2.54
ICT infrastructure	2.81	2.22	2.32

Consumer perspective on data privacy

- ***Consumers' practice of providing personal information online***

(Survey of 500 individuals frequently using the Internet)

Information providing behaviors	Percentage
Having filled in online forms	81%
Reading terms of agreement when filling online forms	74%
Being concerned when providing personal information	48%
Providing truthful information	57%

Consumer perspective on data privacy

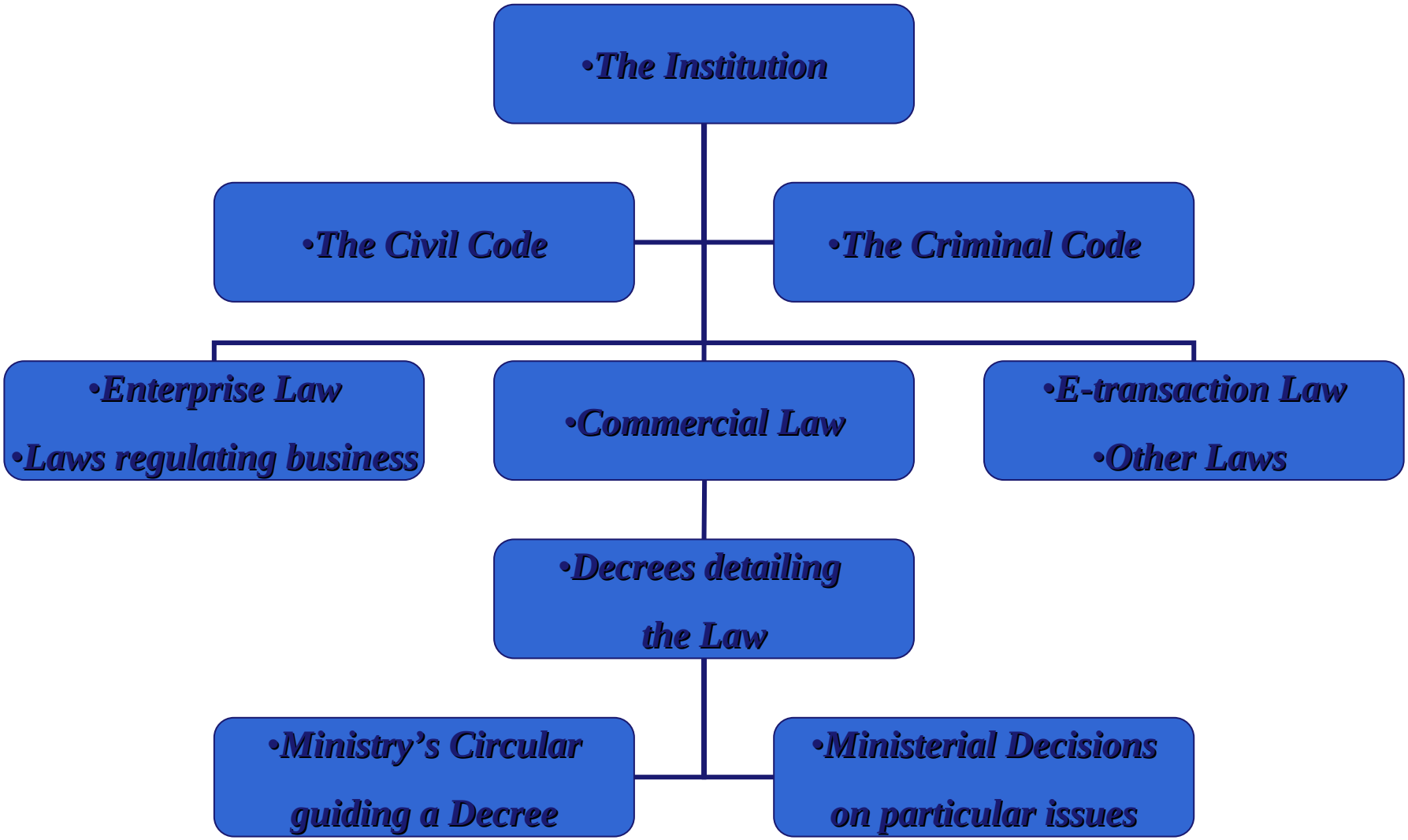
- ***Level of expectation on data privacy protection measures***

(Survey of 500 individuals frequently using the Internet)

Measures	Expectation
Legal regulations	1.79
Technical measures	1.38
Business policy	1.21

II/ Legal framework for privacy protection

Legal system of Vietnam



Legal framework for privacy protection

- Civil Code (2001): Article 38. Right on personal life confidentiality

  This article stipulate that right on personal life confidentiality is to be respected and protected by law. The collection, disclose of information on the private life of a person must be under his/her agreement or consent.

- Law on E-Transactions (2005): Article 46. Information confidentiality in e-transactions

  1. Agencies, organizations and individuals shall have the right to select security measures in accordance with the provisions of the law when conducting e-transactions.

  2. Agencies, organizations and individuals must not use, provide or disclose information on private and personal affairs or information of other agencies, organizations and/or individuals which is accessible by them or under their control in e-transactions without the latter's consents, unless otherwise provided for by law.

Legal framework for privacy protection

Law on Information Technology (2006) Article 21

1. Organizations and individuals collecting, processing, and using personal information of a person in the network environment must acquire that person's consent before doing so, except otherwise stipulated by law
2. Organizations and individuals collecting, processing, and using personal information of a person are obliged to:
   - Inform that person of the method, scope, and purpose of information collection, processing, and usage;
   - Use the information for the acclaimed purpose and store that information within a certain time frame as stipulated by law or as agreed between the parties;
   - Adopt the necessary management and technical measures to ensure that personal information is not missing, stolen, altered, or destroyed;
   - Instantly take actions upon receiving request of information recheck, modification, or destruction as stipulated by item 1 of Article 22 of this Decree;
3. Organizations and individuals are entitle to collecting, processing, and using personal information of a person without that person's consent in the following cases:
   - To sign, modify, or perform contracts of supplying information, goods, or services in the network environment;
   - To calculate the price or charges for information, goods, or services usage in the network environment;
   - To conduct other obligations as stipulated by law.

Legal framework for privacy protection

- Amendments of the Criminal Code 1999: Article 226

1. Whoever conducts one of the following acts that harm the interests of organizations or individuals and result in severe consequence shall be subject to financial penalty of VND 10 to 100 mil., 3-year probation, or imprisonment of 6 months to 3 years:

a) Uploading to the computer networks or telecommunication networks information that is not allowed by law

b) Trading, offering, or publishing information of other organizations and individuals on computer networks or telecommunication networks without the consent of the information's owner

c) Unlawful collection of other organizations and individuals' information

d) Other conducts of illegal use of information on computer networks or telecommunication networks

2. For the circumstances below, the sentence shall be raised to 2 - 7 years imprisonment

a) Organized crime

b) Crime committed by the network administrator

c) Benefit yielded from the crime equals VND 100 mil. or more

d) The crime results in highly or extremely severe consequences

III/ TrustVn – a new approach to data privacy enforcement in Vietnam

trustVN

Giới thiệu Quy trình Danh bạ Tiêu chí

Gắn nhãn website **thương mại điện tử** uy tín

Đăng ký

Giới thiệu

Pháp luật Việt Nam đã chính thức thừa nhận giá trị pháp lý của thông tin dưới dạng điện tử. Số lượng website thương mại điện tử và giao dịch kinh doanh trên môi trường Internet đang tăng nhanh

Lợi ích khi tham gia TrustVn

Xây dựng sự tin tưởng của khách hàng, đối tác trong giao dịch trực tuyến khi họ nhìn thấy nhãn tín nhiệm trên trustVN website.

Top B2C tiêu biểu 2007

- www.pacificairlines.com.vn
- www.123mua.com.vn
- www.travel.com.vn
- www.megabuy.com.vn
- www.golmart.com.vn
- www.thegioididong.com
- www.ben.com.vn
- www.vinabook.com
- www.saigontourist.net
- www.25h.vn

Nhận bản tin từ Trustvn

Email Đăng ký

Đối tác

ecomViet Công tác số cho doanh nghiệp

Vietnam E-commerce Association VECOM

ATA Asia-Pacific Trustmark Alliance

TrustVn – Trust program for Vietnam e-commerce websites

- Background
  - Conducted since 2005
  - Previously: Trusted Website Program
  - 2007: TrustVn
  - Sponsored by Ministry of Trade and Industry
  - Conducted by Vietnam E-commerce Association (Vecom)
- Objective
  - Provide official guidelines for consumers and institution buyers in seeking “trust-worthy” websites to do transactions
  - Promote good practice among e-commerce website owners
  - Raise awareness of data privacy issues and other issues related to conducting online business
- Criteria

1. Website owner identification
2. Terms of use
3. Mechanism for reviewing contracts
4. Personal information policy and personal information protection measures
5. Interface and technical functions

Procedures of the Trustmark Program

- Step 1: Contact the TrustVn Program: online or by mail
- Step 2: Fill in the form “Self-assessment of data privacy policy”
- Step 3: Send the form, together with a copy of its data privacy policy, to TrustVn
- Step 4: TrustVn evaluate the website and suggest changes in compliance with TrustVn criteria
  - APEC Data Privacy Framework
  - Vietnam regulations on information disclosure and e-contracting on e-commerce websites
- Step 5: Make necessary changes according to TrustVn recommendations
- Step 6: Sign agreement on the use of TrustVn logo
- Step 7: Pay service fee
- Step 8: TrustVn “seal” the logo on the website

-> frequent compliance evaluation and monitoring by TrustVn

TrustVn – a new approach to data privacy enforcement in Vietnam

- Adoption of foreign approach and model
- First self-regulatory mechanism for businesses in the e-commerce area
- Better role of business associations and other interest groups
- Less intervention of the state
- Promotion of good practice instead of imposing legal sanctions

-> Impacts of APEC and other international organizations' policy recommendations

THANK YOU!

Data Privacy and the APEC Privacy Initiative - A Civil Society stakeholder perspective

Nigel Waters. Privacy International

Second Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework 2008

12-13 August 2008, Lima, Peru

Outline of presentation

- Different perceptions
- Overlapping objectives
- The role of the Pathfinder projects
- Emphasis within the Pathfinder
- Stakeholder consultation

Different perceptions

- *"a shaky foundation ... far weaker than Europe's traditional approach"(Pounder 2007)*
- *"Perhaps ... the first step towards a truly global standard for data protection" (Tan 2008)*
- *"... The lowest standards of any international privacy agreement; and it has no meaningful enforcement requirements" but also "...it could still play a useful role in the gradual development of higher privacy standards" (Greenleaf 2008)*
- *"The APEC Framework is no longer capable, if it ever was, of being a 'trojan horse' for self-regulation. It may however provide one route amongst many towards effective privacy protection." (Waters 2008)*

Overlapping Objectives

- Civil Society: effective and enforceable privacy protection in all countries and applying to cross border data transfers
- APEC: sufficient protection to facilitate cross border transfer, particulary commercial
- APEC Principles set a minimum standard – arguably lower than other privacy instruments
- Civil Society will push for higher standards, but APEC better than nothing

The role of the APEC Pathfinder

- CBPR approach only one mechanism
- Also domestic law – should remain at least an equal focus of the Privacy Subgroup
- Welcome clear statement that Pathfinder will not undermine existing domestic law
- Means that must be legislative support in all participating economies

Emphasis within the Pathfinder

- Projects 1-3
  - Practical implementation becoming clearer
  - Will require more proactive privacy compliance than current legal requirements in any APEC member economy - welcome
  - Civil Society can support in principle – but must ensure high standards + compatibility with any domestic requirements

Emphasis within the Pathfinder

- Project 4 – Directory
  - Critical to transparency and success
  - Must include name, contact details and direct links to CPBR
- Projects 5-8 – Cross border enforcement
  - Can be independent of CBPR and support all implementation mechanisms
  - Civil Society strongly supports but must ensure not limited to CBPR or private sector

Emphasis within the Pathfinder

- Project 9 – Trial
  - Will be critical – will monitor with interest
- 'Friends of Chair' communications group
  - Outreach critical - strongly support
- Civil Society input as far as resources allow

Stakeholder Consultation

- Growing recognition of need for, and value of, Civil Society input on privacy
- Still no independent Civil Society voice on the Privacy Subgroup to balance business interests
- Applications for guest status pending
  - by Privacy International (PI) and Electronic Privacy Information Centre (EPIC)
- Consultation with Civil Society in all member economies also desirable
- Consultation with OECD and APPA welcome – also needed with EU and CoE

Ministerio de Relaciones Exteriores del Perú

Corporate Social Responsibility in the Asia Pacific

Luis Quesada
APEC Senior Official for Peru

What is Corporate Social Responsibility?

Corporate social responsibility is the commitment of business to contribute to sustainable economic development—working with employees, their families, the local community and society at large to improve the quality of life, in ways that are both good for business and good for development.

The World Bank's working definition of corporate social responsibility

The business case for CSR

- The business case for investment in CSR activity can be linked to a range of issues including the pursuit of new business opportunities through social and environmental innovation, improving competitiveness, attracting investment, reputational risk management, campaign pressure from nongovernmental organizations (NGOs) or trade unions, media exposure of business practices etc.

Source: Ward, Halina (2004) 'Public Sector roles in Strengthening CSR: Taking Stock' (World Bank).

Why promote CSR?

- CSR helps improve financial performance, enhance brand image and increases the ability to attract and retain the best workforce – contributing to the market value of the company by up to 30 per cent. All of these translate into better client and customer satisfaction, improved customer loyalty and ultimately into lower cost of capital as a result of better Risk Management. Finally from a national standpoint, a good reputation for CSR will help Malaysian companies compete in world markets by resolving the potential concerns end users may have in developed markets.

Deputy Prime Minister of Malaysia, June 2004

CSR in the Asia Pacific

- There is an emerging level of CSR activity in the private sector in the majority of APEC economies. This is a result of an increasing level of awareness by the business sector of the importance of CSR issues to long term corporate strategies.
- CSR has been developing at different speeds and in different directions within APEC economies over recent years with each approach reflecting local factors, distinct business cultures and economic structures.
- Nearly all governments in APEC economies have recognized the implications of CSR for public policy but there is often no integrated CSR public policy framework.
- Public policies on CSR in APEC economies vary widely in the level of sophistication and implementation.

Conclusions of APEC Survey

- CSR activity is strong and growing in APEC but the level of awareness and the application of CSR principles in both the private and public sectors is far from universal.
- CSR is of relevance to public sector agencies as they can often lead the way in setting standards for good corporate practice such as managing relations with stakeholders, promoting sustainable development and transparency.
- APEC (especially through ABAC) could play a facilitating role in promoting CSR awareness and capability in both the public and private sectors.

Voluntary strategies to promote CSR by public, private and civil society actors

- **Transparency:** To identify voluntary programs to certify processes or products, and ensure transparency in the processes in which SMEs are involved.
- Facilitating: To enable or increase the adoption of management tools such as voluntary product labeling schemes and guidelines for company management systems or reporting. It may include fiscal incentives or specific procurement procedures.
- Improving Promotion and Advocacy: To enhance CSR awareness through conferences, workshops, training programs, baseline indices, etc.
- Partnering: To tackle complex social issues by initiating and managing public and private stakeholder partnerships that combine complementary skills.
- Endorsing: To include CSR in the political agenda and demonstrate the success of CSR management by recognizing the efforts of companies, for instance, through awarding schemes.

CSR Snapshot – United States

- The US federal government has over 50 programs, policies, and activities at 12 agencies that are related to global CSR. These programs include those that may affect U.S. corporations' CSR efforts overseas, including their supply chains, and those that touch on key components of CSR, such as labor, environment, human rights, community development and corporate governance.
- **Endorsing:** The U.S. government endorses CSR by providing awards to companies, such as the Department of State's Award for Corporate Excellence.
- **Facilitating:** Federal programs facilitate CSR by such activities as providing information or providing funding to engage in CSR. For example, a Department of Commerce program facilitates CSR by providing training on corporate stewardship.
- **Partnering:** Some agencies partner with corporations on specific projects related to their core mission. For example, the U.S. Agency for International Development (USAID) partnered with one U.S. corporation operating in post-war Angola to build up the country's business sector and workforce.
- **Mandating:** Other agencies, such as the Overseas Private Investment Corporation, mandate CSR by requiring companies to meet CSR-related criteria to obtain their services.

CSR Snapshot – China

- State-owned enterprises (SOE) are the backbone of China's national economy and most of them are under the supervision of the State Assets Supervision & Administration Commission (SASAC).
- The SASAC attaches great importance to corporate social responsibilities undertaken by the SOEs.
- On 4 January 2008 SASAC promulgated *Guidelines on CSR Undertaken by the Centrally Owned and Managed Enterprises*".
- It is the first document of its kind introduced by a ministerial agency in China and urges SOEs to embed corporate social responsibility into their practices and establish a CSR reporting system.

Some possible elements of an APEC Agenda on CSR could include the following:

- A strong political commitment from APEC Leaders to raise CSR awareness in 2008 including recognition of relevant APEC and ABAC work in this area.
- Diagnostic of APEC structure to identify areas of expertise in committees and working groups to include in an APEC CSR framework.
- Mapping of CSR linkages across the APEC agenda.
- APEC CSR Resource Centre (through ABAC) including an inventory of resources on CSR practices and the most relevant CSR principles & standards for the Asia-Pacific.
- APEC CSR regional network of business organizations and experts.
- Survey of APEC CSR public policies and possible capacity building needs.
- Business outreach and promotion of CSR best practices in APEC.

Data Protection & Corporate Responsibility

Lima
12, August 2008

ERICSSON
TAKING YOU FORWARD

About corporate responsibility

- **What is corporate responsibility (CR)?**

  An umbrella term referring to how Ericsson works with:
  - Environmental performance
  - Social equity
  - Economic prosperity
    - Also known as the triple bottom line
    - CR is not charity

- **What is Ericsson's approach?**
  - To maintain the necessary controls to minimize risk
  - To create positive business effects

- **How?**
  - By linking our products and services to an overall business goal of sustainable growth

Why is this important?

- Stakeholder engagement
  - 25+ investor surveys/inquiries last year
  - Major customers want to trace environmental, ethical and social accountability
- Gives us a competitive edge
  - Develops new business opportunities
  - Supports sustainable business solutions
- Supports our core strategy and vision
  - Prime driver
  - Communication for all
  - Sustainable energy solutions
- Role of our industry
  - ICT sector has ability to affect change by addressing:
    - Environmental issues
    - Socioeconomic development

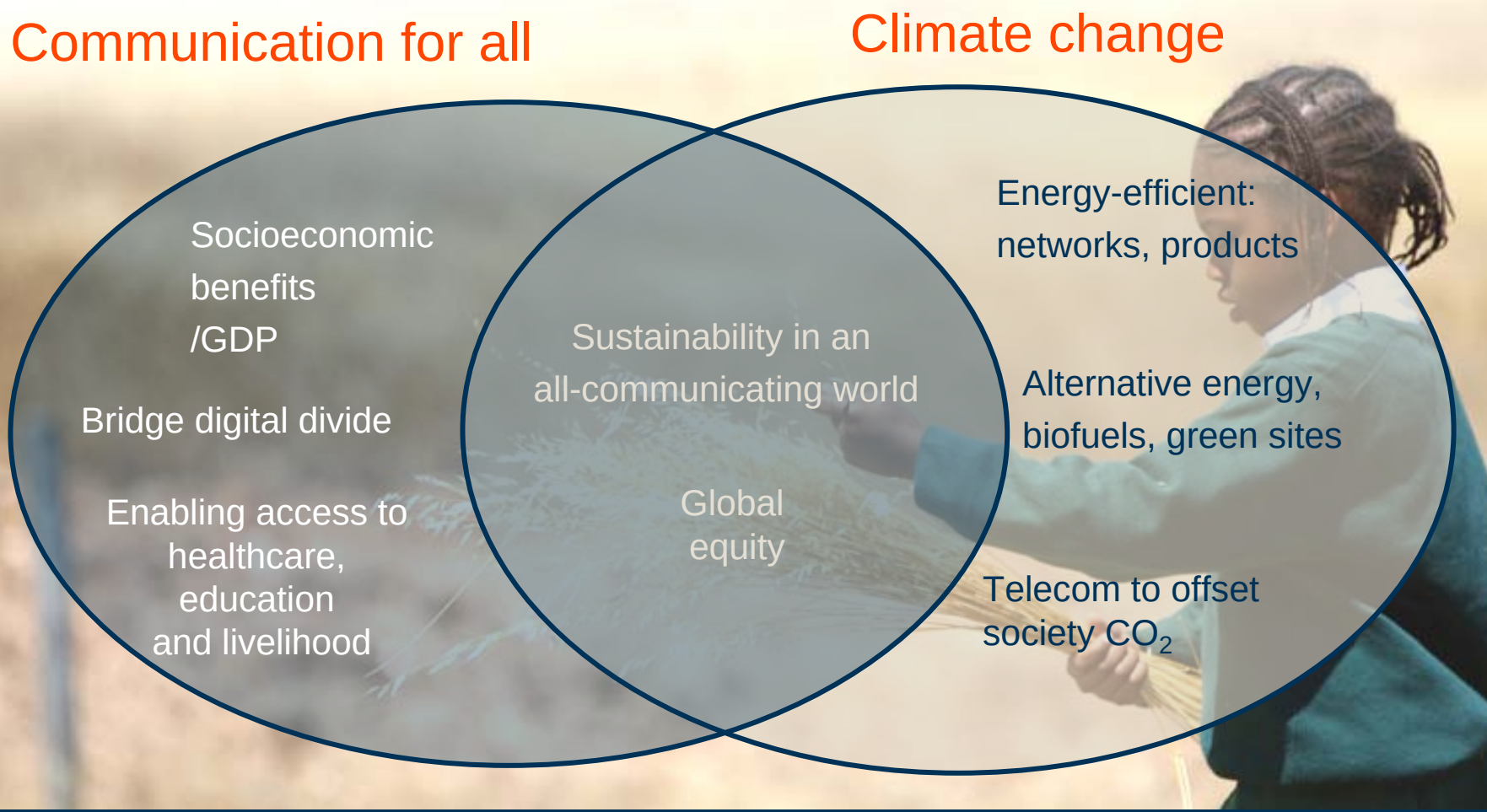
How Ericsson operates responsibly

- **Governance**
- **Key policies**
  - Code of Conduct
  - Environmental Policy
  - Code of Business Ethics
- **Environmental management**
  - Design for Environment
  - Hazardous substances
  - Energy efficiency
  - Product take-back
- **Human rights**
  - Global Compact
  - BLIHR
  - Fair labor practices

Ericsson requires all suppliers and their subcontractors to comply with the Code of Conduct

Creating positive impact

Key focus areas



Our core technology is our contribution

Energy and climate change

Ericsson's approach

- Sphere of influence
- Life-cycle assessment
- Reducing carbon footprint
- Sustainable energy solutions

In every area through our sphere of influence, energy optimization is Ericsson's core strength. Our unique ability is to take complex telecommunication systems and optimize energy use at every step, focusing not just on one product, but on a total-cost-of-ownership reduction with the lowest possible energy impact and carbon footprint.

2007 Corporate Responsibility Report

Contributing to sustainable societies

Communication for all

- **6.5 billion mobile subscriptions predicted by 2013**
  - Emerging markets to drive growth
  - Role of telecom central to stimulating social and economic development
  - Linked to Ericsson's core business
- **Telecom can:**
  - Close the digital divide
  - Build society
  - Boost GDP
  - Help offset effects of climate change
- **Supports human rights**
  - Right to a livelihood, healthcare, education, security

Ericsson's core business brings socioeconomic benefits to society

Ericsson’s commitment

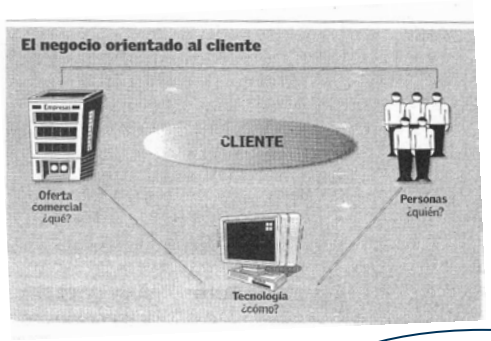
Millennium Villages

- Helping rural African communities lift themselves out of extreme poverty
- Voice and internet to 400,000 people in 10 countries
- Ericsson is customizing telecom solutions to support education healthcare, agriculture and infrastructure
- Partnering with UN, operators, NGOs, local communities and Earth Institute at Columbia University

Lake Victoria

- Preventing deaths by extending mobile coverage across the lake
- Introducing voice and data services
- Partnering with operator and GSMA Development Fund

About Data Privacy



La protección de datos

Millones de datos personales están amenazados por los piratas informáticos. El último escándalo en Estados Unidos ha afectado a 40 millones de usuarios de tarjetas de crédito, en su mayoría de MasterCard y Visa, con ramificaciones en otros países, como Japón. Pero ha habido muchos más agujeros informáticos que han dejado al alcance de casi cualquiera datos personales o bancarios susceptibles de ser usados de forma fraudulenta.

En España las empresas están obligadas a proteger los datos de sus clientes. En los últimos años ha aparecido un seguro específico para cubrir las sanciones y reclamaciones por incumplimiento de la Ley de Protección de Datos. En este sentido sólo existe en el mundo un sindicato dependiente del Lloyd's, que es el mercado de seguros mundial, que lo ofrece. Para hacernos una idea el coste de este seguro sería tan elevado que en el caso de una Administración como la española no podría pagarlo, aceptando como mejor opción el pago por reclamaciones.

Seguridad → **"Razonable"**

Cumplimiento de Políticas de Seguridad y Medidas

problema «personal»

problema «organizativo»

Regulación aplicable

- **Normas laborales**
- **Régimen Disciplinario.**

Política de Data Privacy

Complementos de temporada

Cualquier riesgo puede ser cubierto por un seguro. Desde la pierna de un futbolista hasta un edificio de oficinas. Las novedades en el mercado español, con poca cultura aseguradora, tienen una demanda mínima, pero creciente. En las empresas destacan los productos que cubren riesgos informáticos o malas prácticas laborales.

La protección de datos

Millones de datos personales están amenazados por los piratas informáticos. El último escándalo en Estados Unidos ha afectado a 40 millones de usuarios de tarjetas de crédito, en su mayoría de MasterCard y Visa, con ramificaciones en otros países, como Japón. Pero ha habido muchos más agujeros informáticos que han dejado al alcance de casi cualquiera datos personales o bancarios susceptibles de ser usados de forma fraudulenta.

En España las empresas están obligadas a proteger los datos de sus clientes. En los últimos años ha aparecido un seguro específico para cubrir las sanciones y reclamaciones por incumplimiento de la Ley de Protección de Datos. En este sentido sólo existe en el mundo un sindicato dependiente del Lloyd's, que es el mercado de seguros mundial, que lo ofrece. Para hacernos una idea el coste de este seguro sería tan elevado que en el caso de una Administración como la española no podría pagarlo, aceptando cómo mejor opción el pago por reclamaciones.


Complementos de temporada

Cualquier riesgo puede ser cubierto por un seguro. Desde la pierna de un futbolista hasta un edificio de oficinas. Las novedades en el mercado español, con poca cultura aseguradora, tienen una demanda mínima, pero creciente. En las empresas destacan los productos que cubren riesgos informáticos o malas prácticas laborales.

PAZ ESCRIBANO/ELA

Los nuevos seguros contemplan, entre múltiples coberturas, las lesiones de los futbolistas.

ALEJANDRO PUEBLA

La protección de datos

Millones de datos personales están amenazados por los piratas informáticos. El último escándalo en Estados Unidos ha afectado a 40 millones de usuarios de tarjetas de crédito, en su mayoría de MasterCard y Visa, con ramificaciones en otros países, como Japón. Pero ha habido muchos más agujeros informáticos que han dejado al alcance de casi cualquiera datos personales o bancarios susceptibles de ser usados de forma fraudulenta.

En España las empresas están obligadas a proteger los datos de sus clientes. En los últimos años ha aparecido un seguro específico para cubrir las sanciones y reclamaciones por incumplimiento de la Ley de Protección de Datos. En este sentido sólo existe en el mundo un sindicato dependiente del Lloyd's, que es el mercado de seguros mundial, que lo ofrece. Para hacernos una idea el coste de este seguro sería tan elevado que en el caso de una Administración como la española no podría pagarlo, aceptando cómo mejor opción el pago por reclamaciones.

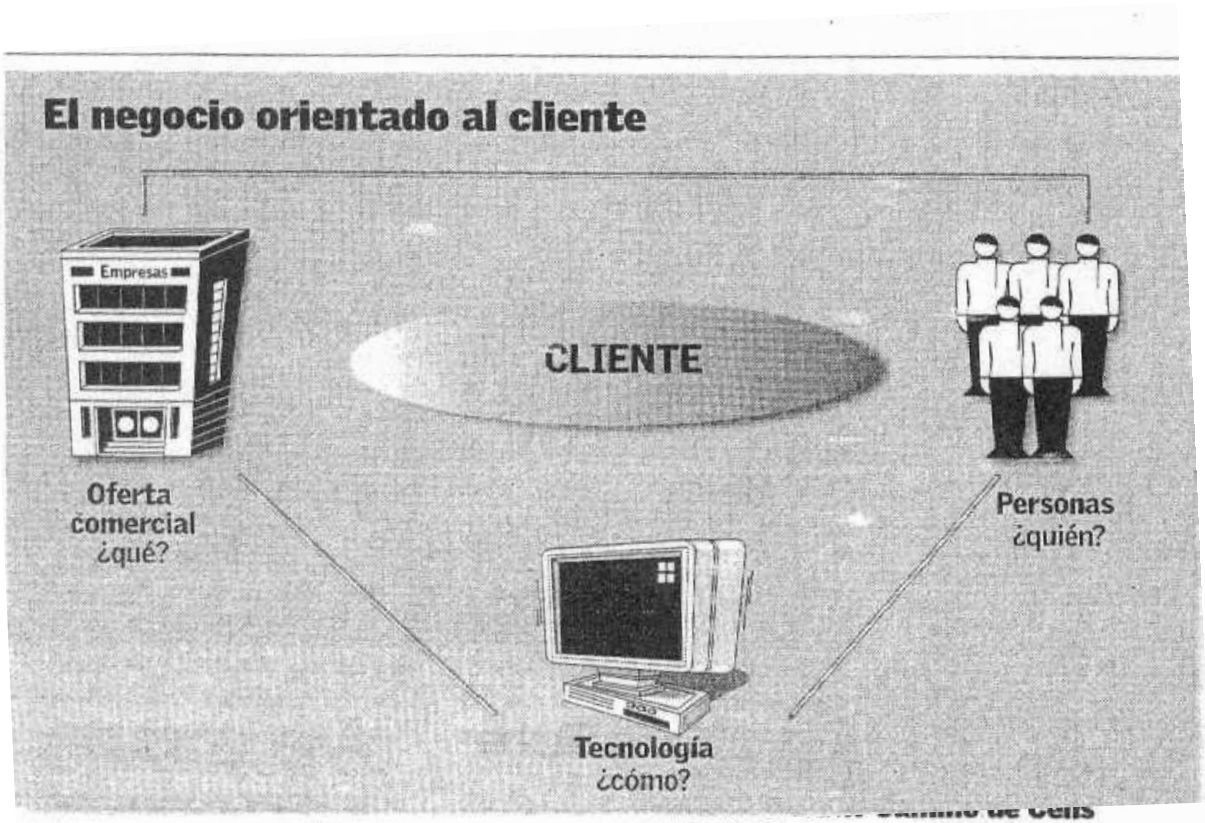
Hay un seguro que cubre el 'mobbing' cuya prima máxima son 10.000 euros

Diario

EL PAIS

(3-7-2005)

What is trigger issue?



Diario
5 Días
(3-7-2007)

Cuidar al cliente para dar valor al accionista

OPINIÓN

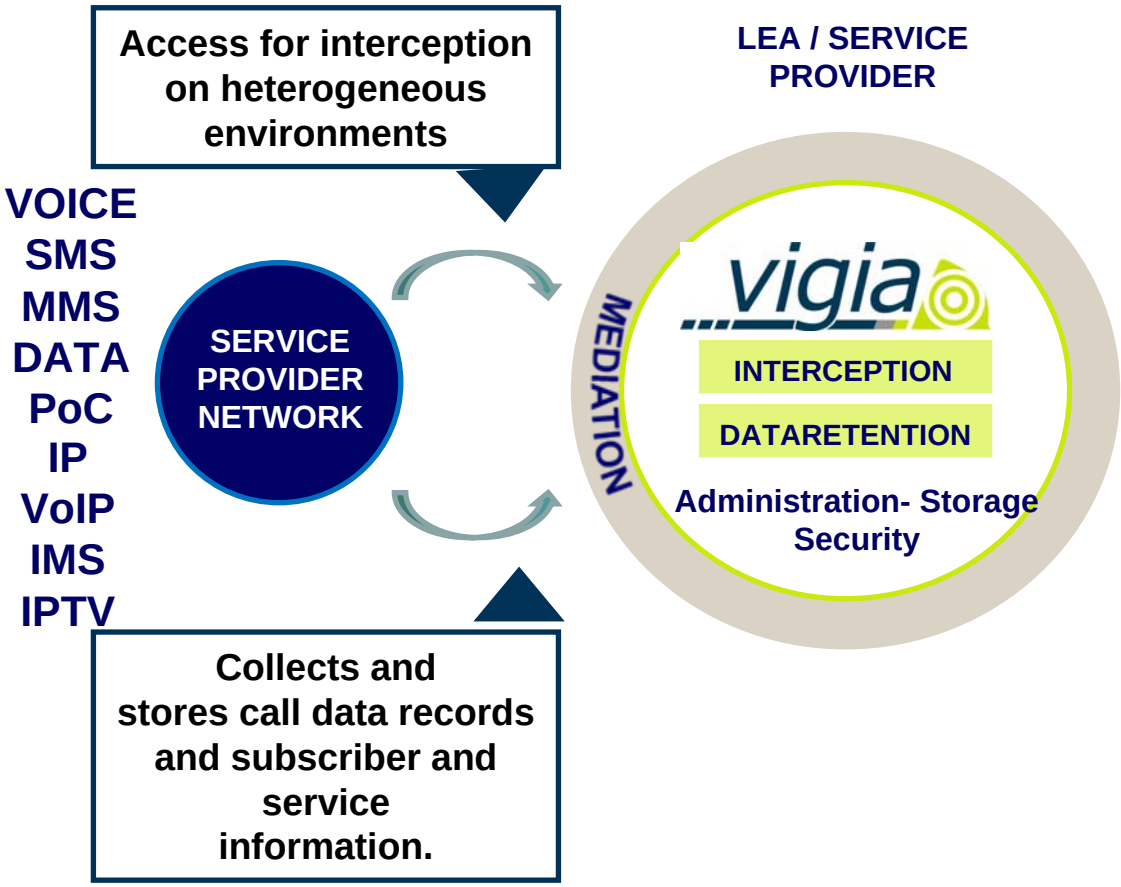
Jorge Parra
Senior manager de PricewaterhouseCoopers

Reputación y fidelización

lidad de la actividad que la empresa lleva a cabo. No debe olvidarse que los clientes son cada vez más sensibles a aspectos como la protección medioambiental, el respecto a la diversidad y los derechos humanos, la seguridad y la salud laboral, entre otros, que quedan englobados en el concepto de reputación corporativa. Según estudios empíricos realizados por British Telecom, un 42% del grado de satisfacción de los clientes se explica por la imagen o reputación que la compañía tiene, existiendo una relación directa entre ambos conceptos.

En una investigación de mercado realizada por el Instituto MORI a 12.000 consumidores de 12 países europeos en el año 2000, el 70% de los encuestados afirmaba que la responsabilidad social de una compañía es un factor importante que influye en su decisión de compra. Asimismo, el número de consumidores dispuesto a penalizar a compañías no responsables ha aumentado en más de un 10% entre el año 2001 y 2002, tanto en Estados Unidos como en Europa (según el *2002 CSR Monitor*, Environics International).

Lawful Interception & Data Retention Overview



ETSI / CALEA Compliance Multiple advantages for Emerging Countries

About Data Privacy

- **Facilitate the relationship between Carriers and Law Enforcement Agencies (LEAs)**
- **Assures compliance with any legislation (CALEA, EU Directives, others)**
- **Diminishes the chances of fraud or erroneous procedures.**

About Data Privacy

- **Manage the entire process of Lawful Interception and Data Retention.**
- **Intercept communications on virtually any type of network.**
- **Based on the most up-to-date technologies and standards in the world, such as ETSI.**
- **The system standardizes procedures and creates a work methodology.**

Corporate Responsibility summary

- Controls are in place to minimize risk
- Our business creates positive impacts in the socioeconomic and environmental areas
- For more information: www.ericsson.com/ericsson/corporate_responsibility


ERICSSON
TAKING YOU FORWARD

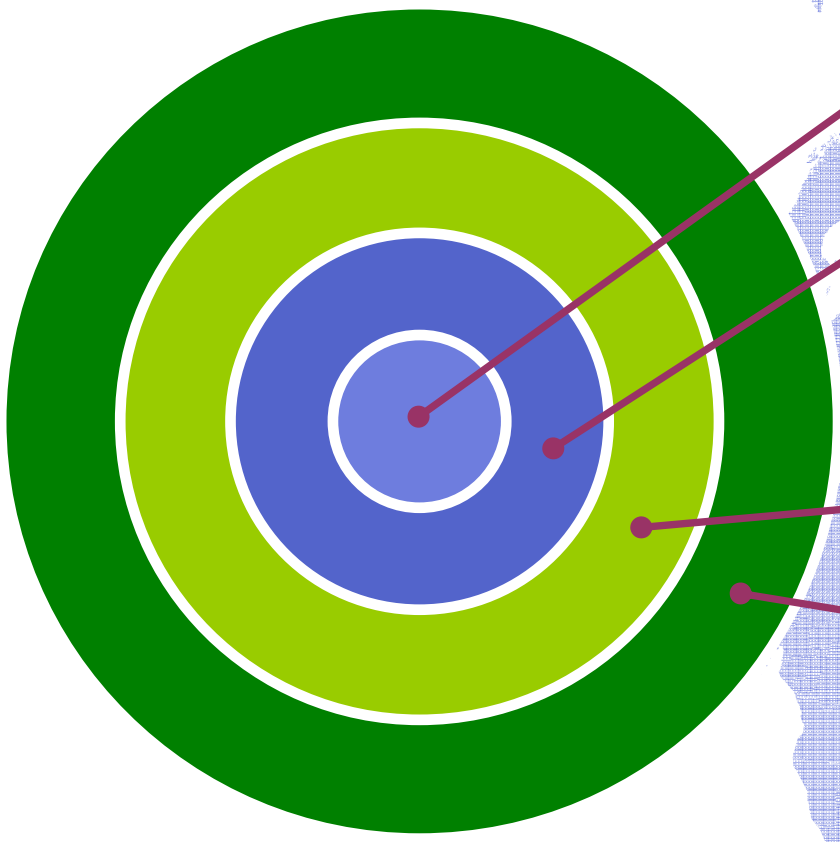
Building Social Responsibility and Accountability into Privacy Decisions

APEC Privacy Sub-Group Meeting
Lima, Peru - August 2008

Situation

- Global data flows are growing more complex
- Advances in technology and analytic techniques are straining traditional compliance frameworks
- Laws are critical but often lag practical realities
- Companies need to build mechanisms to ensure they can balance the tensions of using information robustly while ensuring those decisions are responsible and accountable
- To support CPBRs, we need tangible proof points that will demonstrate a company's character and capacity to uphold their obligations

Accountability Model Structure



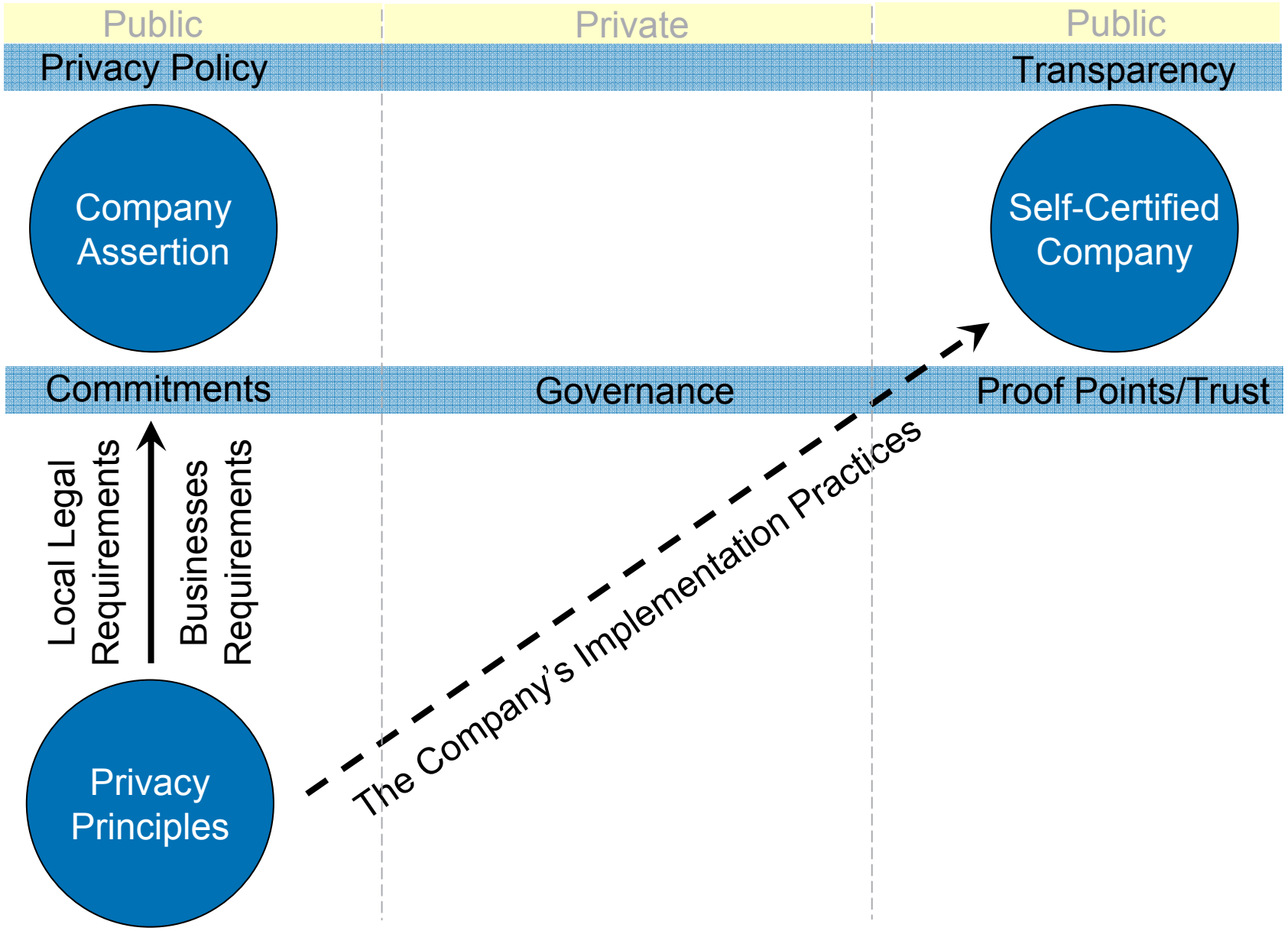
Liability-Based:

- Privacy Laws & Regulations
- Case Law Interpretation, Codes of Conduct, Safe Harbor, Contracts

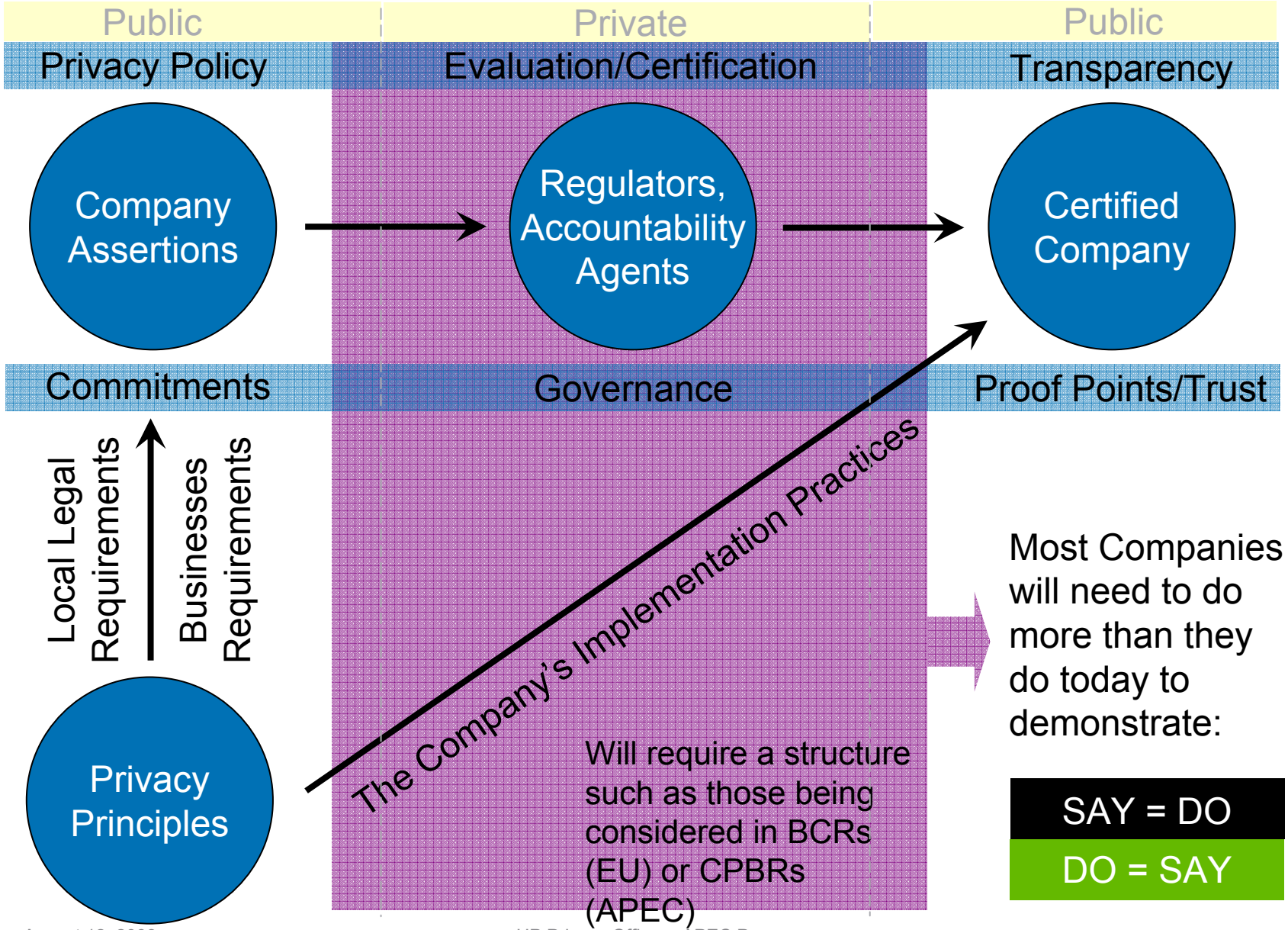
Accountability-Based:

- HP Assertions, Promises, Policies
- Ethics- and Values-driven Considerations & Decision Making

Accountability Landscape Vision



Accountability Landscape Vision



Privacy Accountability in HP's View

1. A New approach to privacy compliance
2. Decision makers made accountable
3. Ethics & values decision making
4. Risks fully considered

A New Privacy Framework
Accountability Integrated Formally

Is it Legal

Is it Secure

Does it meet our Privacy Promises

Ethics

- Is it Fair
- Not misleading
- Is it right by the customer
- Is it right by HP
- Is it right by other stakeholders
- Is it transparent

+

Values

- Standards of Business Conduct
- Corporate Policies
- Key Company Values:
  - Integrity
  - Trust
  - Respect

+

Risks

- Will it affect HP's reputation?
- Will privacy developments affect your investment?
- Are you afraid to make decisions due to privacy, legal considerations?
- Will decision impact normal day to day running of HP?
- Will your decisions compound to create risk to HP?

Accountability Model

Accountability Model Tool
Operation

Questionnaire
- Project Profile
- Detailed Questions
- Harms
- Security & Integrity
- Benefits

Rules Engine

Knowledgebase
- Rules – HP Policies
- Rules – HP Privacy Rulebook
- Rules – Country Legal Requirements
- Rules – Regulator Guidance

Feedback/Monitoring
- Reports 
- Informational User Messages
- Instant Feedback
- Checklists
- Ongoing Assurance Monitoring

In Conclusion

- Tangible proof points that demonstrate a company's willingness and capacity to uphold their obligations will facilitate workable compliance models.
- The Accountability Decision Tool is HP's solution to drive responsible decision-making internally and to provide a mechanism for external agents to judge our capacity.
- This tool is part of the HP way - other companies are building solutions that drive accountability that match their corporate cultures.
- What is needed is for companies to make these solutions visible to the regulators/agents to assist them in judging or certifying a company.

Privacy Commissioner
Te Mana Matapono Matatapu

APEC Privacy Pathfinder Projects 5,6 and 7: Cross-border Cooperation in Investigation & Enforcement

Blair Stewart
Assistant Privacy Commissioner
New Zealand

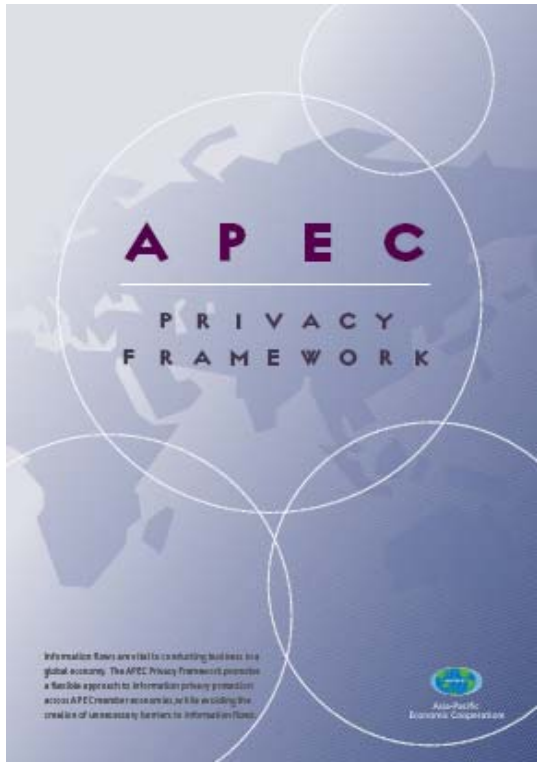
2nd Technical Assistance Seminar on the International Implementation of the APEC Privacy Framework

APEC RU 2008

12 & 13 August 2008
Lima, Peru

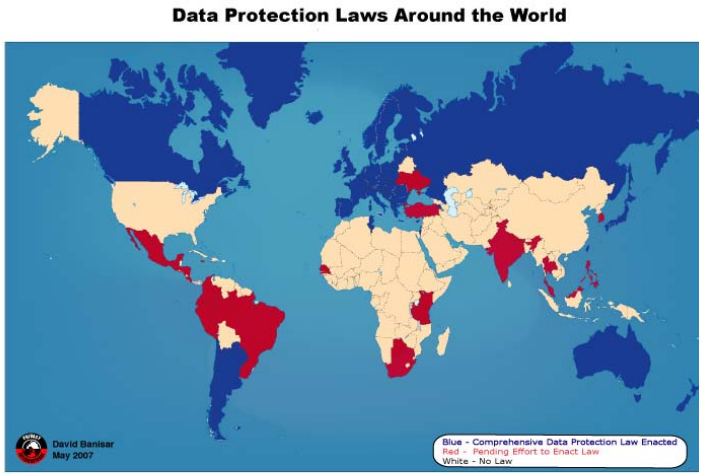
Outline of Presentation

- Context of projects
- The projects
- Outstanding issues



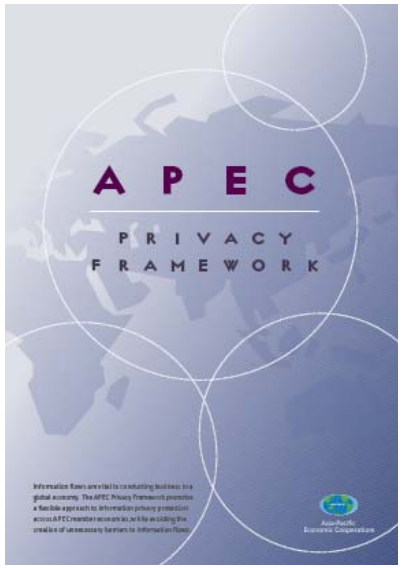
Context

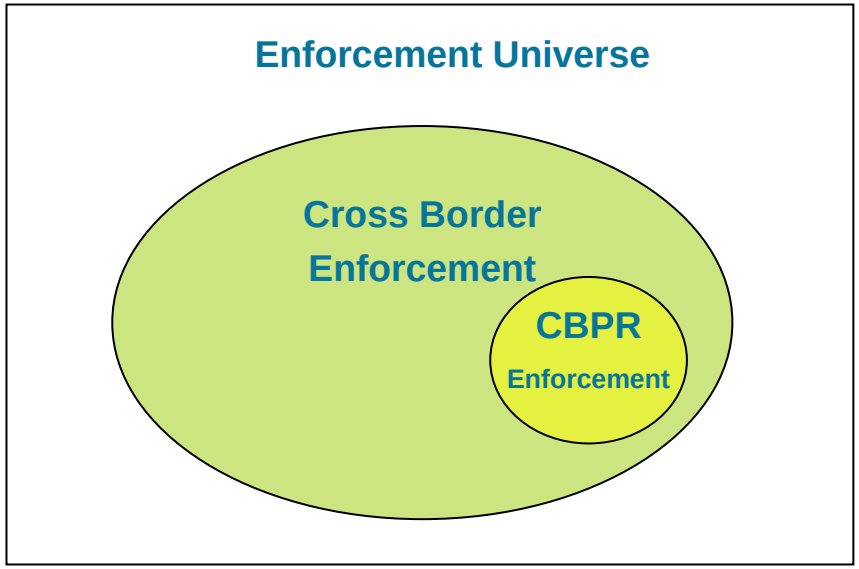
- APEC Privacy Framework Part B II & III
- OECD Recommendation on Cross-border Cooperation in the Enforcement of Laws Protecting Privacy



Context: **APEC Privacy Framework, Part B**

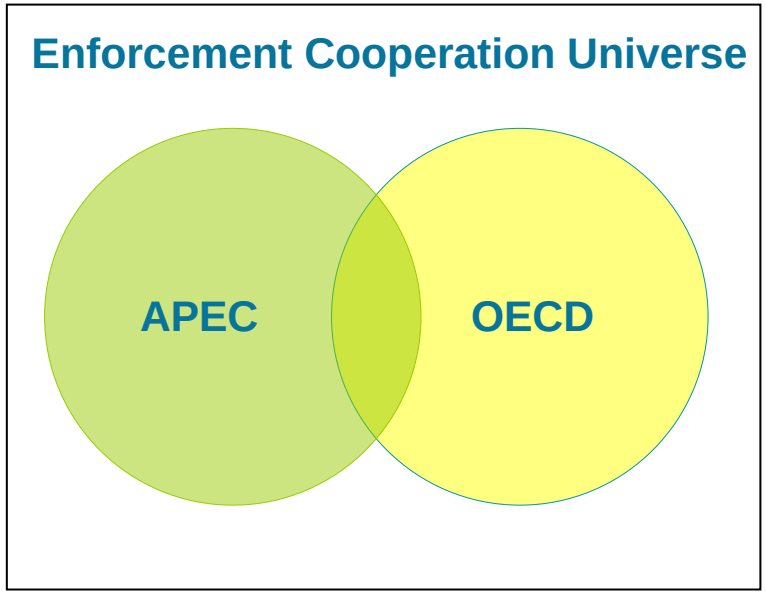
- **Part B II**: Cross-border cooperation in investigation and enforcement – Projects 5, 6 and 7 respond to general need for effective cross-border cooperation and are not dependent on CBPRs
- **Part B III**: Cooperative development of cross-border privacy rules – effective enforcement cooperation underpins CBPRs





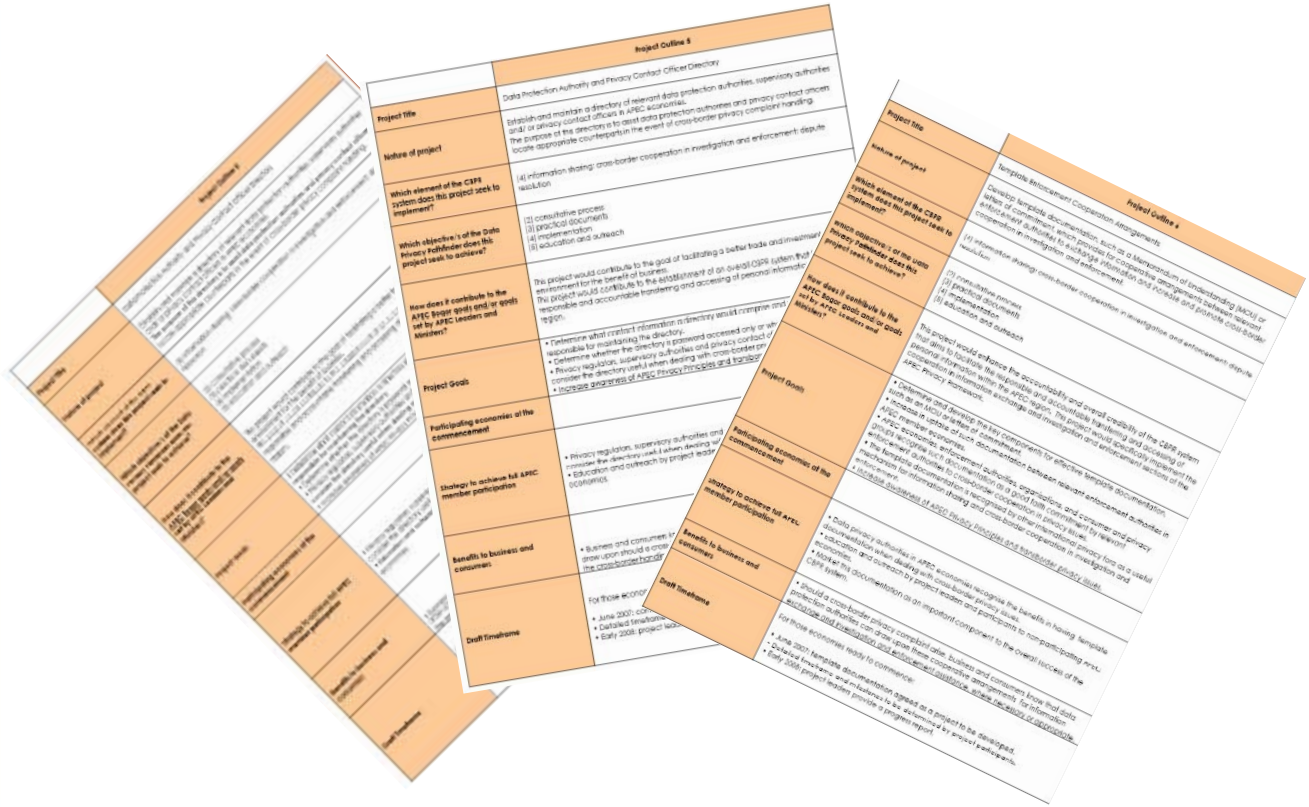
Context: **OECD Recommendation on Cross-border Cooperation in Enforcement of Privacy Laws**

- OECD WPISP has worked on the issue for several years, their analysis and approach a valuable starting point
- Compatibility between enforcement cooperation frameworks is desirable
- Simplify processes for 7 APEC economies that are also members of OECD
- Step towards global, rather than merely regional, cooperation



The Enforcement Cooperation Projects

- Project 5: Data Protection Authority & Privacy Contact Officer Directory
- Project 6: Template Enforcement Cooperation Arrangements
- Project 7: Template Cross-border Complaint Handling Form



Project 5: Data Protection Authority & Privacy Officer Contact Directory

- Project: establish a directory of DPAs, supervisory authorities and/or privacy contact officers
- Purpose: to assist privacy enforcement authorities to locate counterparts in the event of cross-border complaints
- Contact point designation form: single contact point approach
- Compatible with OECD approach – shared or common directory is a possibility for future
- Initial focus on a closed list for privacy enforcement authorities, more ambitious and resource intensive possibilities for the future may include public lists including privacy contact officers

Project 6: Enforcement Cooperation Arrangement

- Project: develop template documentation for cooperation arrangements between enforcement authorities
- Objective: to facilitate exchange of information for enforcement and increase and promote cross-border investigation and enforcement cooperation
- Approach of project: multilateral MOU
- Core focus on requesting and providing assistance in investigation and enforcement but framework able to expand to wider areas of enforcement cooperation
- More details below

Project 7: Request for Assistance Form

- Project: develop a template enforcement ‘request for assistance’ form
- Objective: to facilitate the seeking and providing of assistance in efficient and appropriate form, allowing for low level resolution and responsive regulation
- Closely modelled on OECD form, tailored for APEC Privacy Framework

Integration of Projects 5, 6 and 7

- Key document is APEC cooperation arrangement (project 6) which incorporates contact point form (project 5) and request for assistance form (project 7)
- Common terminology consistent with APEC Privacy Framework:

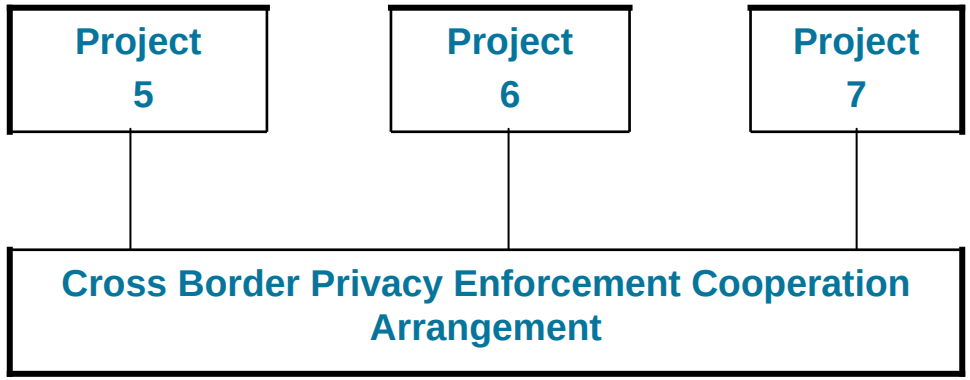
  - key new term ‘privacy enforcement authority’

  - other terms such as ‘participant’, ‘request for assistance’, ‘receiving authority’, ‘requesting authority’ etc
- Key Players:

  - privacy enforcement authority

  - administrator

  - contact points



Cooperation Arrangement Outline

1. Objectives
2. Outline
3. Commencement
4. Definitions
5. Role of administrator
6. Effect of document
7. Limits on assistance
8. Subscribing to the arrangement
9. Cross-border cooperation
   - prioritisation
   - cooperation with non participating organisations
   - steps prior to requesting assistance
   - requesting assistance
   - use of information obtained during cross-border cooperation
   - notice of possible breaches in other jurisdictions
10. Confidentiality
11. Information sharing
12. Staff exchanges
13. Costs
14. Disputes
15. Review and update

Selected Aspects of the Cooperation Arrangement - #1

Joining and leaving the framework:

- A privacy enforcement authority can opt in by applying to the administrator
- Administrator verifies that the body is a privacy enforcement authority
- Administrator publishes a directory of subscribers
- Process for withdrawal

Selected Aspects of the Cooperation Arrangement - #2

Requesting assistance:

- Form facilitates and standardises requests for assistance
- Requests may include investigative assistance, joint investigation, transfer of complaint, etc
- Framework assists privacy enforcement authorities knowing who to deal with in another jurisdiction through network of subscribers, contact point directory, etc
- Arrangement encourages easier access to information on how counterpart enforcement authorities may or may not be able to assist: notably through transparent statement of enforcement practices
- Authorities are under no obligation to assist but arrangement provides tools and an environment whereby in appropriate cases assistance can be provided effectively and efficiently

Selected Aspects of the Cooperation Arrangement - #3

General cooperation beyond particular cases

- While the arrangement focuses in most detail on particular enforcement cases, it also provides a framework for general cooperation
- The administrator must perform core tasks to enable the arrangement to come into effect and operate but may also, if participants wish, perform additional functions (e.g. promote initiatives such as teleconferences, seminars and cooperation with other enforcement networks)

A work in progress

- The arrangement will be a significant step forward for general enforcement cooperation (desirable in the global digital economy) regardless of the pace of development of CBPRs or the particular direction that CBPRs might take in an individual economy or across APEC
- The arrangement has been prepared while conceptual and developmental work is ongoing on CBPRs – while the arrangement anticipates and address CBPRs there may be room for improvement as other parts of the CBPR framework becomes clearer
- Some matters of detail yet to be worked through and agreed before the arrangement is piloted

Thank You

Blair Stewart, Assistant Commissioner
PO Box 466, Auckland 1140
New Zealand
Tel: +64 9 302 8680

Email: blair.stewart@privacy.org.nz