



Asia-Pacific
Economic Cooperation

**APEC Symposium on Information Privacy Protection
in
E-Government and E-Commerce**

**Ha Noi, Viet Nam
20 – 22 February 2007**

**APEC Electronic Commerce Steering Group
APEC Telecommunications and Information Working Group**

April 2006

Note: Some of the terms used here do not conform to the APEC Style Manual and Nomenclature. Please visit http://www.apec.org/apec/about_apec/policies_and_procedures.html for the APEC style guide.

Reproduced electronically in April 2006

© 2006 APEC Secretariat

Produced for
APEC Secretariat
35 Heng Mui Keng Terrace Singapore 119616
Tel: (65) 67756012 Fax: (65) 67756013
Email: info@apec.org Website: www.apec.org

APEC#206-TC-04.1

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce

Horison Hotel, Hanoi, 2006 Feb 20-22

AGENDA

Feb 20, morning

- 8:30 – 9:00: Registration

Opening

Moderator: **Le Hai Khoi**, Director of Institute of Information Technology, Vietnamese Academy of Science and Technology

- 9:00 – 9:10 *Welcome remark:* **Nguyen Khoa Son**, Vice President of Vietnamese Academy of Science and Technology
- 9:10 – 9:20 *Opening address:* **Le Danh Vinh**, Deputy Minister of Trade of Viet Nam
- 9:20 – 9:30 *Opening remark:* **Jesus Orta**, ECSG Chair
- 9:30 – 10:10 *Keynote speech:* *APEC Information Privacy Framework (review, impact, and progress)*, **Malcolm Crompton**, Managing Director of Information Integrity Solutions Pty Ltd, Former Federal Privacy Commissioner of Australia

10:10 – 10:30 *Coffee Break*

Section 1: General Issues of Information Privacy in E-Government and E-Commerce

Chair: **Malcolm Crompton**, Managing Director of Information Integrity Solutions Pty Ltd, Former Federal Privacy Commissioner of Australia

Speakers:

- 10:30 – 10:50 **Michael Lewis**, Vice President and General Counsel, Warner Bros. Online
- 10:50 – 11:10 **Alex Waibel**, Professor, Carnegie Mellon University
- 11:10 – 11:30 **Pauline Reich**, Professor, Waseda University, School of Law

11:30 – 12:00 *Discussion*

Feb 20, afternoon

Section 2: Legal Regulatory Environment for Protecting Personal Information of Customers and Citizens

Chair: **Patricia M. Sefcik**, U.S. Department of Commerce, International Privacy Representative, OECD & APEC

Speakers:

- 13:30 – 13:50 **Maureen Cooney**, Acting Chief Privacy Officer of the U.S. Department of Homeland Security
- 13:50 – 14:10 **Mai Anh**, Director of Informatics Center, Ministry of Science and Technology, Viet Nam
- 14:10 – 14:30 **YU Yin-ching**, Woman Chief Inspector of Police, Hong Kong Police Force

14:30 – 14:50 ***Coffee Break***

- 14:50 – 15:10 **Nguyen Ai Viet**, Deputy Director General, Standing Office, National Steering Committee for ICT, Viet Nam
- 15:10 – 15:30 **Martin Abrams**, Director, Center for Information Policy Leadership at Hunton & Williams LLP
- 15:30 – 15:50 **Seong Jin Choi**, Senior Prosecutor, Director of High-Tech Crime and Financial Crime Investigation Division, Central Investigation Department, Supreme Prosecutors' Office

15:50 – 16:20 ***Discussion***

Feb 20, evening

Welcome Reception

Place: Somerset, Grand Hanoi (Hanoi Tower), 49 Hai Ba Trung street, Ha Noi

- 18:30 – 18:35 *Welcome speech:* **Le Danh Vinh**, Deputy Minister of Trade of Viet Nam
- 18:35 – 18:45 *Speeches of sponsors*
- 18:45 – 21:00 *Welcome party*
- 21:15 – 23:00 *Water puppet show and Hanoi night tour*

Feb 21, morning

Section 3: Role of Technology in Information Privacy Protection

Chair: **Peter Ferguson**, Director, Electronic Commerce Policy, Electronic Commerce Task Force, Industry Canada

Speakers:

- 8:30 – 8:50 **Meng Chow Kang**, Chief Privacy and Security Advisor for Asia-Pacific, Microsoft
- 8:50 – 9:10 **Ho Tu Bao**, Professor, Japan Advanced Institute of Science and Technology
- 9:10 – 9:30 **Joseph Fong**, General Manager Government & Public Affairs, Asia Pacific & Japan, Hewlett Packard Company
- 9:30 – 9:50 **Martin Abrams**, Director, Center for Information Policy Leadership at Hunton & Williams LLP

9:50 – 10:20 *Coffee Break*

10:20 – 11:10 *Discussion*

Feb 21, afternoon

Section 4: Lessons Learned from APEC Framework Implementation

Chair: **David Loukidelis**, Information and Privacy Commissioner for British Columbia, Canada

Speakers:

- 13:30 – 13:50 **Heather Black**, Assistant Privacy Commissioner of Canada
- 13:50 – 14:10 **Nguyen Chi Cong**, Chief Consultant, Steering Committee of the National Project for Vietnam Digital Administrations
- 14:10 – 14:20 **Alberto Cerda**, Ministry of Economy, Chile
- 14:20 – 14:30 **A. N. Andy Laksmana**, Directorate of Asia-Pacific and African, Intra Regional Cooperation Department of Foreign Affairs, Indonesia
- 14:30 – 14:40 **Rafael Muenta Schwarz**, Manager of National E-Government Office of Minister Council's Presidency, Peru

14:40 – 15:00 *Coffee Break*

- 15:00 – 15:10 **Jorge Luis Irey Nuñez**, SUNAT - National Intendancy of Information Systems, Peru
- 15:10 – 15:20 **Maria Lourdes A. Yaptinchay**, Director of Department of Trade and Industry - Office of Policy Research, Philippines

- 15:20 – 15:30 **Rosemarie S. Ramos**, Department of Foreign Affairs - Office of the Undersecretary for International Economic Relations and APEC National Secretariat, Philippines
- 15:30 – 15:40 **Natalia Makarycheva**, Director of International Projects, Department of International Affairs, Russian Information Technology Association, Russian
- 15:40 – 15:50 **Alexey Sabanov**, Commercial Director of JSC Aladdin Security Solutions, Russian

15:50 – 16:20 *Discussion*

- 16:20 – 16:30 Wrap-up: **Peter Ferguson**, Director, Electronic Commerce Policy, Electronic Commerce Task Force, Industry Canada
- 16:30 – 16:40 Closing remark: **Le Hai Khoi**, Director of Institute of Information Technology, Vietnamese Academy of Science and Technology

Feb 22, morning

Section 5: Tutorial on Information Privacy (Optional for Experts)

Chair: **Pham Ngoc Khoi**, Deputy Director, CMT Hanoi Company

Speakers:

- 8:30 – 9:30 **David Loukidelis**, Information and Privacy Commissioner for British Columbia, Canada
- 9:30 – 9:45 *Summarization*: **Pham Ngoc Khoi**

9:45 – 10:00 *Coffee break*

- 10:00 – 11:00 **Katitza Rodríguez**, Director of CPSR-Perú
- 11:00 – 11:15 *Summarization*: **Pham Ngoc Khoi**



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/002

Agenda Item: 1

APEC Information Privacy Framework (review, impact, and progress)

Purpose: Information
Submitted by: Australia



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



INFORMATION
INTEGRITY
SOLUTIONS

Malcolm Crompton

APEC Information Privacy Framework: review, impact, & progress

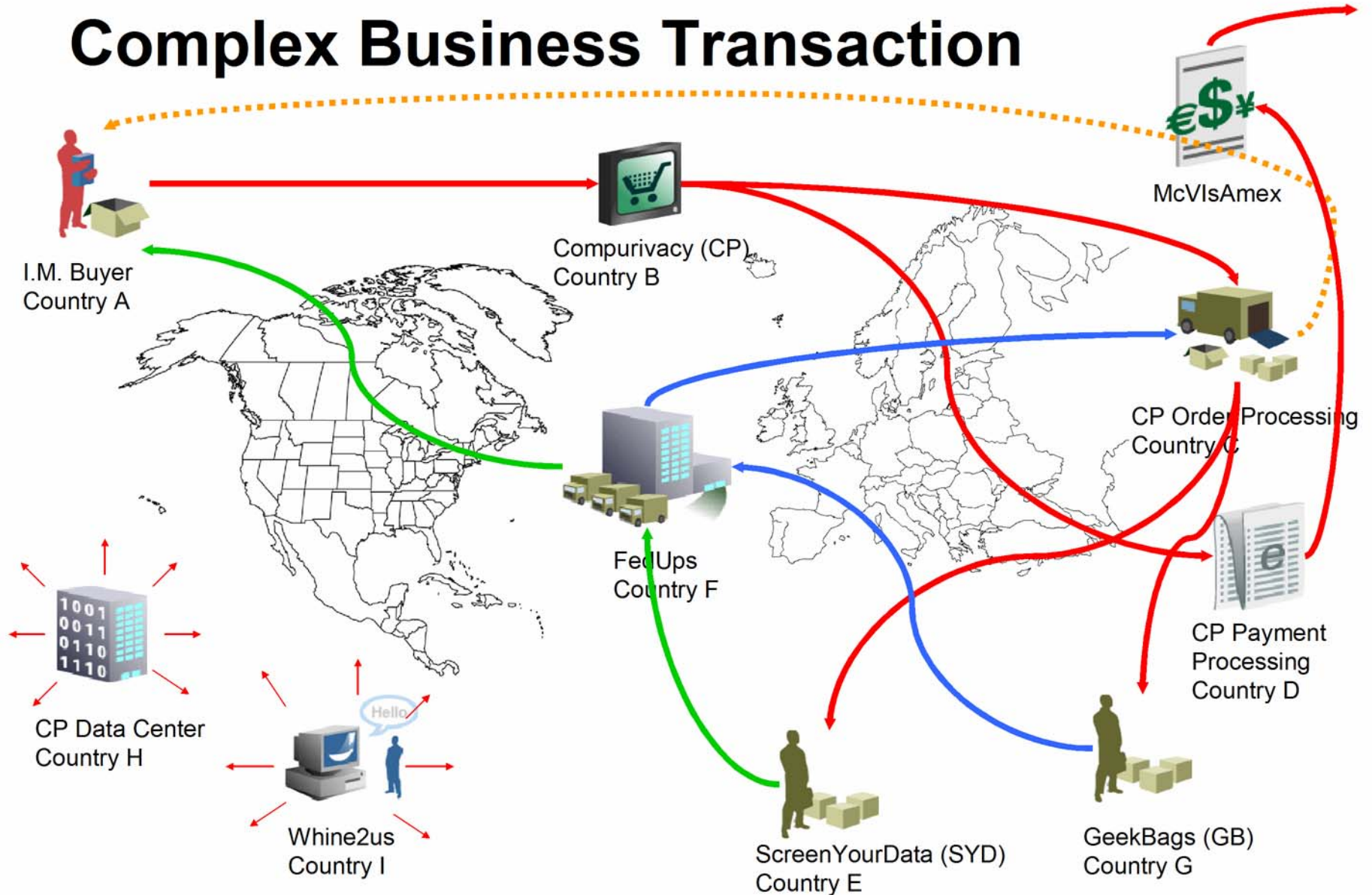
APEC Symposium on Information Privacy
Protection in E Government & E Commerce

Hanoi
20 February 2006



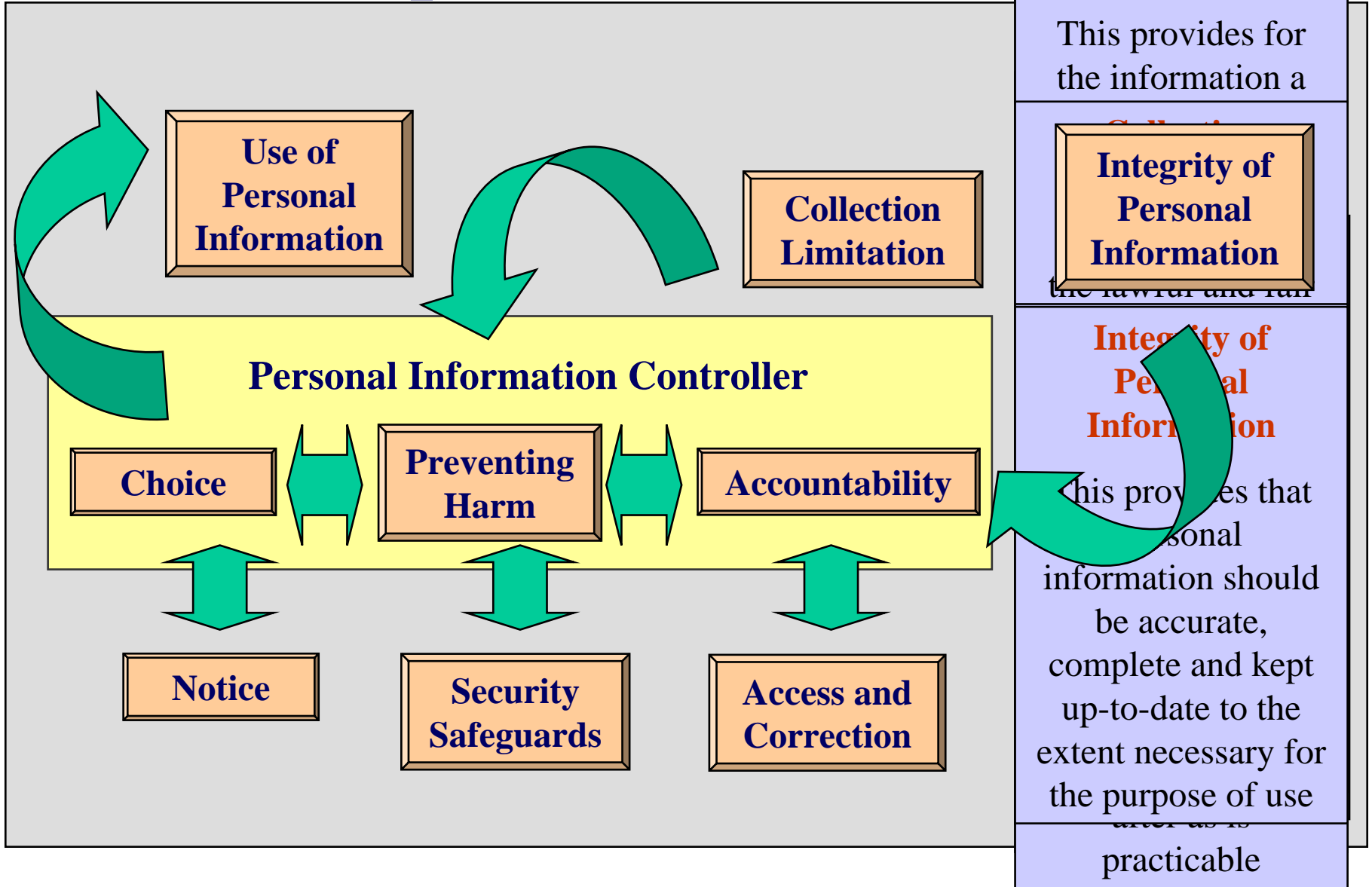
Why is 'Privacy' on the
APEC agenda?

Complex Business Transaction



The APEC Privacy Framework

APEC Privacy Principles: Relationship



Nine APEC privacy principles

1. Preventing Harm – privacy protections should focus on preventing harm and misuse
2. Notice – clear & easily accessible
3. Collection Limitation – collect what's relevant in a lawful & fair manner
4. Uses of Personal Information – for expected and compatible purposes, with consent, or where necessary
5. Choice – where appropriate, provide clear, accessible mechanism to exercise choice

Nine APEC privacy principles

6. Integrity – personal information should appropriately accurate, complete and up-to-date
7. Security – appropriate safeguards to protect against unauthorized access, use, modification or disclosure
8. Access & Correction – important (but not absolute) rights
9. Accountability – controllers are accountable for compliance with all Principles and must use reasonable steps to ensure that recipients of personal information also comply

The APEC Insight

Insight in Principles 1 & 9

Principle 1

- Proportionality: focus effort on where harm greatest



Principle 9

- ‘Accountability follows the data’



Where did we get to last
time?

What is the problem?

- Complex business transactions makes privacy compliance more difficult
- Many laws, many regulators
 - Hard for anybody to see the whole
- Effective resolution of complaints
 - Cost to business; cost to consumer
- Justification introducing privacy regime for a small economy not a small task
 - International trade argument very strong

Immediate action

- Consumer empowerment
 - Improved Privacy Notices
- Education – effort from Govt; business; hot topics like ID theft
 - Consumers
 - Business, especially small business
- Privacy Regulators encouraged to coordinate more
- Business to pay more attention to flows of personal information in their business and with their business partners
- But turn this into a strategy – How?

Implementation

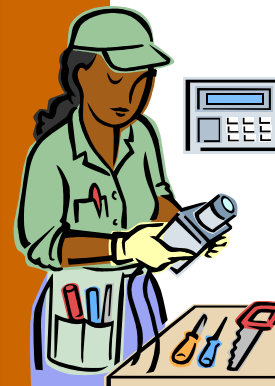
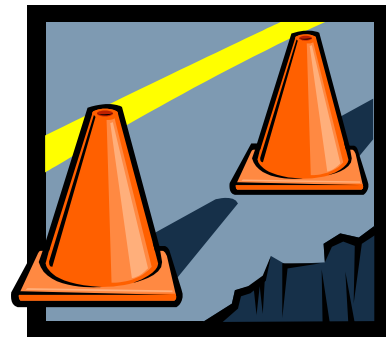
Governance

‘Safety begins at home’

- those directly handling the data to respect and abide by that framework

Internal Privacy Governance Framework

- A high level policy
- Standard operating procedures
- Recommended measures & best practices
- Training ,communication & compliance tools
- Assurance functions



Domestic

- 6 APEC Member Economies have broad based privacy law
- 1 has sectoral law
- 1 has voluntary framework
- At least 5 drafting a privacy framework

Consistency with APEC Privacy Framework varies

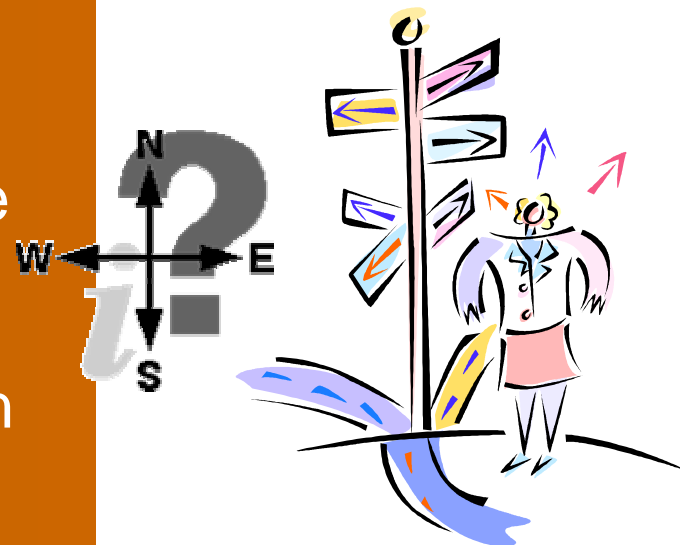
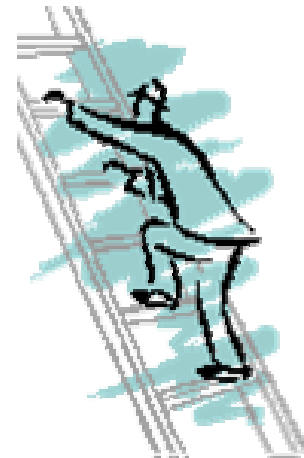


International

APEC Member Economies have most to do here

Options

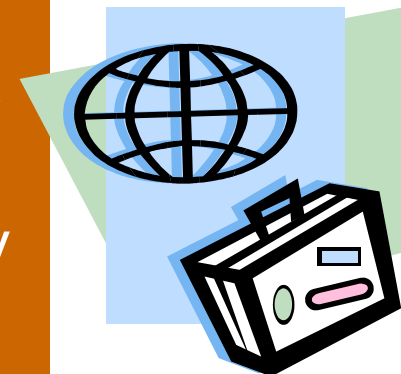
- ‘APEC Privacy Commission’
- NGO equivalent, either one or more
- Binding corporate rules
- Cooperative arrangements between existing privacy regulators



International

Part B:

- “44. Member Economies should ... facilitate cross-border cooperation in the enforcement of privacy laws
- “46. Member Economies will endeavor to support the development and recognition or acceptance of organizations’ cross-border privacy rules across the APEC region ... that ... adhere to the APEC Privacy Principles.”



Further work

Build on 2005

- See consultants' Final Report

Facilitate Binding Corporate Rules

- a. Industry accountability checklist
- b. Process for “approvals” of rules
- c. International trust on enforcement

Information Privacy Individual Action Plans

OECD privacy law enforcement survey



The Wrap

APEC has come a
long way in 3 yrs

Now for more

**INFORMATION
INTEGRITY
SOLUTIONS**

Malcolm Crompton

Managing Director

53 Balfour Street

Chippendale NSW 2008

+61 407 014 450

MCrompton@IISpartners.com

www.IISpartners.com



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/003

Agenda Item: 1

APEC Information Privacy Framework (review, impact, and progress)

Purpose: Information
Submitted by: Australia



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

**APEC Information Privacy Framework (review, impact,
and progress) – Keynote speech**

Malcolm Crompton

**Managing Director, Information Integrity Solutions Pty Ltd; and
Federal Privacy Commissioner of Australia, 1999-2004**

**APEC Symposium on Information Privacy Protection in
E-Government and E-Commerce**

Horison Hotel, Hanoi, 20-22 February 2006

APEC Information Privacy Framework (review, impact, and progress)

Introduction – purpose of this paper

The purpose of this paper is to review briefly the history of privacy in an APEC context and outline the challenges of the future.

This is the third privacy seminar that APEC has sponsored. The first two seminars were held in June and September, 2005.

Many excellent papers were presented at the two seminars. They provide an excellent resource for business, policy makers and regulators operating in APEC Member Economies. These papers are available online at the following URLs:

Technical Assistance Seminar: Domestic Implementation of the APEC Privacy Framework, 1-2 June 2005, Hong Kong, China
www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEMHK

2nd Technical Assistance Seminar on Implementation of APEC Privacy Framework: International Implementation Issues, 5-6 September 2005, Gyeongju, Korea
www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEM

There is no need to repeat here the material presented in the papers presented to the first two seminars. Instead, this paper draws a brief road map through the issues and draws the attention of participants to relevant papers already presented.

Why is ‘Privacy’ on the APEC agenda?

There is widespread recognition that a widely accepted and practical international standard of privacy protection is needed if e-commerce is to flourish.¹

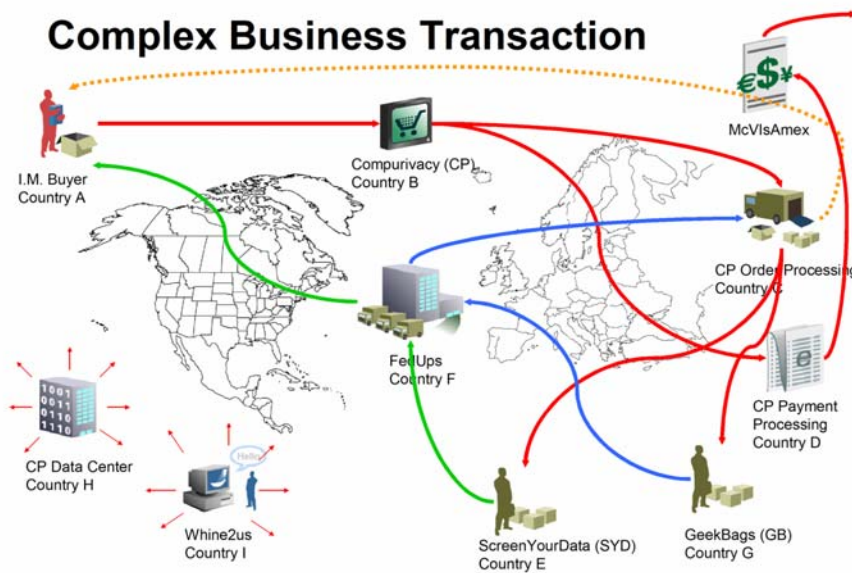
Today, flows of personal information can be rapid (or instantaneous), cross between the jurisdictions of many economies and be part of very complex transactions.

The following diagram was presented in the first Technical Assistance Seminar² to demonstrate this point.

¹ The underlying reasons are developed further in “APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific” in APEC E-Newsletter Vol 7, January 2006, online at: www.apec.org/apec/enewsletter/jan_vol7/onlineenewsd.html

² “Data Flows and Business Models: Distributing Information Flows and Business Functions”, Paper 2005/ECSG/SEM/005 presented to the 1st Technical Assistance Seminar and online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005/MediaLibDownload/v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf/Par.0103.File.v1.1

Complex Business Transaction



In 1998, when endorsing the 1998 Blueprint for Action on Electronic Commerce, APEC Ministers acknowledged that the potential of electronic commerce cannot be realised without government and business cooperation “to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy...”. The lack of consumer trust and confidence in the privacy and security of online transactions and information networks is one element that may prevent Member Economies from gaining all of the benefits of electronic commerce.

Almost everyone has a stake in privacy policy. Obviously, consumers are concerned to protect their personal information and business must be sensitive to the concerns of its customers. Governments have broad responsibilities for the social and legal environment in which commerce takes place, for encouraging electronic commerce and for safeguarding security, including law enforcement, within their societies.

Privacy policy cannot be considered in isolation but needs to take account of a range of twenty-first century problems such as identity fraud. It also needs to address the use of electronic technology to commit traditional crimes in novel ways.³

A history of Privacy in APEC

Following workshops in Mexico in 2002 and Thailand in 2003, APEC Ministers endorsed the need to develop APEC data privacy principles. These principles are designed to help APEC Member Economies to develop privacy laws and regulations that achieve a balance between effective privacy protection and the continuity of cross-border information flows, thus promoting electronic commerce.⁴

³ These thoughts are developed further in “APEC Privacy Framework June 2005 Domestic Implementation”, Paper 2005/ECSG/SEM/003 presented to the 1st Technical Seminar and online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005/MediaLibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0101.File.v1.1

⁴ A brief history is also presented in “APEC Privacy Framework: Facilitating Business and Protecting Consumers Across the Asia-Pacific” in APEC E-Newsletter Vol 7, January 2006, online at: www.apec.org/apec/enewsletter/jan_vol7/onlinenewsd.html

The development of the APEC Privacy Framework was given to a Data Privacy Subgroup of the Electronic Commerce Steering Group (ECSG) of the Senior Officers Meeting (SOM). The Subgroup completed the first part of this task in 2004 when APEC Ministers endorsed Part A of the APEC Privacy Framework.⁵

Part B of the Framework was completed and endorsed by Ministers in 2005.⁶

The Framework sets out a good, 'common practice' guide for Member Economies. Consistent with the APEC way, the Framework is aspirational, with individual Member Economies encouraged to develop ways of protecting personal information within an economy and when it moves between economies or is accessible in more than one economy.

The APEC Privacy Framework

The complete APEC Privacy Framework is readily available online.⁷ There are nine principles in the APEC Privacy Framework:

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

These principles reflect and build on many of the privacy frameworks developed in other parts of the world. For example, all of the principles in one of the most widely respected frameworks, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data first published in 1980⁸, are reflected in the APEC Privacy Framework.

The way that the APEC principles work together is described extremely clearly in a paper presented to the first Technical Seminar in 2005.⁹ In the simplest of terms:

⁵ See "APEC Ministers Endorse the APEC Privacy Framework", Media Release, Santiago, Chile, 20 November 2004, online at: www.apec.org/apec/news_media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html

⁶ See "Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information, Busan, Korea, 16 November 2005, online at: www.apec.org/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframework.html

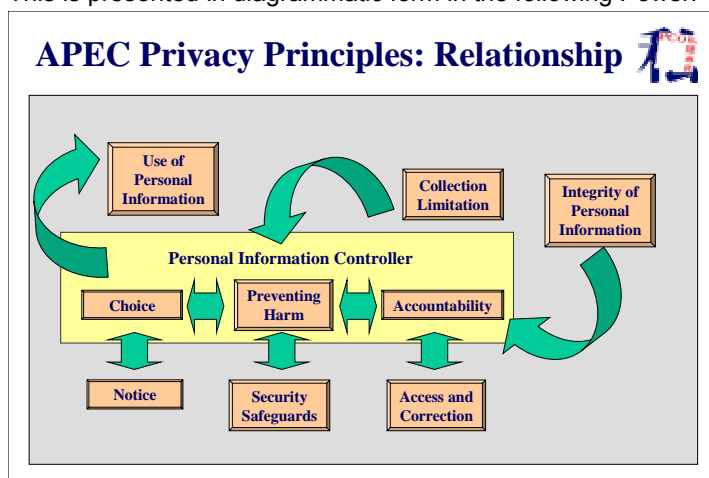
⁷ The "APEC Privacy Framework" as endorsed by Ministers in November 2005 is online at: http://203.127.220.112/content/apec/news_media/2005_media_releases/161105_kor_minsapproveapecprivacyframework.downloadlinks.0001.LinkURL.Download.ver5.1.9

⁸ The "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" endorsed by the Council of the Organisation for Economic Co-operation and Development (OECD) in September 1980 are available online at: www.oecd.org/document/18/0,2340,en_2649_34255_1815186_119820_1_1_1,00.html

⁹ "An Overview of the Principles Established by the APEC Privacy Framework" Paper 2005/ECSG/SEM/006, presented to the 1st Technical Seminar and online at: http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0104.File.v1.1

- An organisation that has control of personal information (the 'data controller') is required to handle that information in a way that prevents harm (Principle 1) and gives the individuals involved some choices about the uses of that data (Principle 5)
- A key component of preventing harm is that the data controller must also put in place security safeguards to protect the data (Principle 7)
- In order to give individuals choice, they must be given notice about the collection of the personal information (Principle 2)
- To be effective, the data controller is also held accountable for abiding by the privacy framework (Principle 9) and an important component of accountability is to provide individuals with access to information held about them and to correct any errors (Principle 8)
- Finally, as an input, the collection of personal information must be limited to information that is relevant to the purposes for which it is being collected (Principle 3) while there are corresponding limitations on output so that the personal information should only be used for the purposes for which it was collected (Principle 4).

This is presented in diagrammatic form in the following PowerPoint slide:¹⁰



[If reading this in Microsoft Word format, double click on the slide to see how each of the components link to each other.]

The APEC insight

The APEC privacy framework is nevertheless different from other privacy frameworks such as the EU Privacy Directive in the way it protects personal information when it is being processed and in the way it provides for the free movement of such data¹¹. These departures from other frameworks are crucial and seek to recognise the way personal information is already being handled and will be handled in the future. The key differences are to be found in Principles 1 and 9 of the Framework.

APEC Principle 1 extends the concept of proportionality that permeates a lot of thinking in the design of EU frameworks. In particular, it extends the concept of proportionality to apply in the

¹⁰ In the Microsoft Word version of this document, double click on the diagram to see the way these components build up.

¹¹ The full title is "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data" and it is online at:

area of redress ('let the punishment fit the crime') so that it gives guidance to regulators in focusing their activities. To put it another way, the principle is an explicit recognition of the reality that most organisations, regulators or otherwise, have limited resources at their disposal and have to prioritise. The key will be to ensure an appropriately broad approach to the concept of 'harm' to ensure that it extends beyond immediate harm that is measurable only in financial terms to include other less tangible social harms some of which can be very hurtful.

Principle 9 is the most important innovation in the APEC Privacy Framework. In effect, this Principle is saying that 'accountability should follow the data'. Once an organisation has collected personal information, it remains accountable for the protection of that data. Just because personal information is passed on to another organisation or moves from one jurisdiction to another does not change that. Other frameworks tend to focus on border controls – in particular, whether the data moving from one jurisdiction which has 'adequate' data protection to another that has 'adequate' protection.

Implementation of Privacy Principles – governance

When it comes to implementing the APEC Privacy Framework, it is always important to focus on the outcomes. The APEC Privacy Framework is seeking effective privacy protection that is efficient for business to implement. In the near future at least, the Framework will operate in the context of existing or imminent domestic privacy and other law.

Regardless of this position, the first and best approach to implementing any framework including the APEC Privacy Framework is for those directly handling the data to respect and abide by that framework on their own initiative. This means that good governance by individual businesses and government agencies is critical. Papers presented to the second Technical Assistance Seminar covered governance issues well.

First, the basic components of a good internal Privacy Governance Framework should include a number of components:¹²

- A high level policy
- Standard operating procedures
- Recommended measures and best practices
- Training ,communication and compliance tools
- Assurance functions

Second, there is good evidence that leading companies are working on putting good internal Privacy Governance Frameworks in place. In a survey of a select group of mostly US based companies with customers and data processing in the US and elsewhere, all had a privacy officer, other privacy staff and procedures. Most were able to ensure that their 'downstream' vendors etc were also meeting privacy requirements.¹³

www.europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett

¹² "Internal Privacy Governance Frameworks", Paper 2005/SOM3/ECSG/SEM/010, presented to the 2nd Technical Assistance seminar, online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0080.File.v1.1

¹³ "Corporate Privacy Governance – A Prerequisite For APEC Implementation", Paper 2005/SOM3/ECSG/SEM/011, presented to the 2nd Technical Assistance seminar, online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0081.File.v1.1

Equally importantly, these companies are approaching governance in a multi jurisdiction context. They are doing this through internal networks and reporting structures. Their approach provides an example of how multi jurisdiction application of the APEC Privacy Framework might be enforced. For example, where such a company's internal Privacy Governance Framework meets the standards set by the APEC Privacy Framework, one option is for such companies to 'bind' themselves legally to abiding by that framework. To be 'binding', such an arrangement would have to be enforceable in law one way or another and include ways of addressing complaints by aggrieved individuals. This arrangement will not be practicable for the vast majority of companies operating in APEC, but it is an option for leading global corporations to show their bona fides as 'good corporate citizens'.

Implementation of the APEC Privacy Framework – domestic

For some years now, an increasing number of Member Economies have implemented privacy law, many of them comprehensive and at the national level. Other economies have encouraged good practice codes in various ways.

The table below briefly summarises the situation.¹⁴

Country name	Privacy/Data Protection Law Status
<i>Australia</i>	<ul style="list-style-type: none"> • Comprehensive national laws, National Privacy Principles (NPPs) and privacy codes and some state laws • Companies can gain approval of a code to replace the NPPs, which are then enforceable as law; codes must be 'at least the equivalent' of the NPPs • Independent Privacy Commissioner at federal level and some states enforces compliance
<i>Canada</i>	<ul style="list-style-type: none"> • Comprehensive national laws, provincial and territorial laws • Independent Privacy Commissioners at both federal and provincial levels enforce compliance
<i>China</i>	<ul style="list-style-type: none"> • No comprehensive law/regulations • Work on drafting has started
<i>Hong Kong-PRC</i>	<ul style="list-style-type: none"> • Comprehensive laws and codes of practices • Independent Privacy Commissioner enforces compliance
<i>Indonesia</i>	<ul style="list-style-type: none"> • No comprehensive law • Broad privacy right provision in the Electronic Transaction Bill
<i>Japan</i>	<ul style="list-style-type: none"> • Comprehensive national law, several guidelines and ordinances based on the law, prefectural and local laws • Responsible ministries/agencies enforce based on guidelines published respectively
<i>Malaysia</i>	<ul style="list-style-type: none"> • Drafted a comprehensive national data protection bill • The bill includes appointment of a Commissioner

¹⁴ The author takes responsibility for any errors in this table and apologises in advance for any such errors.

Country name	Privacy/Data Protection Law Status
Mexico	<ul style="list-style-type: none"> • Data protection law only applicable to the government • Currently drafting a data protection bill that includes an appointment of a Commissioner
Philippines	<ul style="list-style-type: none"> • No comprehensive national laws • Currently developing data protection guidelines for the private sector
Singapore	<ul style="list-style-type: none"> • Voluntary private sector model code • Debating on whether to initiate legislation
South Korea	<ul style="list-style-type: none"> • Existing national law only applicable to certain industries • Currently drafting a restrictive data protection bill applicable to all industries • Currently compliance enforced by the Personal Information Dispute Mediation Committee which is supported by the Korea Information Security Agency
Taiwan	<ul style="list-style-type: none"> • Comprehensive national law • Bill with expanded scope submitted
Thailand	<ul style="list-style-type: none"> • Draft comprehensive national data protection bill under inter-agency review
U.S.A	<ul style="list-style-type: none"> • No comprehensive national laws, but sector-specific laws, state laws, and Federal Trade Commission law/regulations
Vietnam	<ul style="list-style-type: none"> • No comprehensive national laws • Privacy provision in the Electronic Transaction bill

From a privacy perspective, the spread of privacy protection legislation must be welcomed where it is having material effect on improving individual privacy. However, inconsistencies between these laws make it more difficult for a business to operate across economies in the APEC region as the number of such laws grows. This has the potential to reduce the impact of the law in any one economy compared with what is possible with close harmonisation. Europe is already feeling the effects of insufficient harmonisation and continues to seek ways of alleviating them. On the other hand, individual Member Economies will continue to address data protection in ways that they see as appropriate to their circumstances and cultures. Respect for each economy's approach on these matters has been a key component of the APEC way.

In addition to putting in place privacy law, privacy codes or other mechanisms to encourage respect for privacy consistent with the APEC Privacy Framework, many economies also have programs to engage business and the public in helping them understand the privacy framework in place in their economy.

Implementation is likely to comprise a series of components such as:

- Engagement and Education
 - Making sure that individuals and organisations are aware of the issues and the benefits (including commercial benefits) of respecting individuals and the personal information about them

- Making sure that they are aware of good practice, relevant legislation and the APEC Privacy Framework
- Assistance to business and to government agencies when they face challenges in implementing the Framework
 - Consultation with officials and others should be based on solving problems not finding wrong doers when the business or organisation is clearly indicating good will and best endeavours
- Encouragement of low key, direct settlement of disputes between parties
 - Starting with effective, internal dispute resolution procedures
 - Low cost, credible alternative dispute resolution mechanisms provided by trusted public sector or private sector tribunals that are simple to use for all parties
- Enforcement
 - Always as a last resort
 - Always there as a credible threat in case all other options fail
 - Could involve one off or regular audits, official investigation of incidents
 - Includes remedies for the aggrieved party

Implementation of the APEC Privacy Framework – international

As mentioned earlier, the APEC Privacy Framework is also intended to address the privacy of personal information when it moves between APEC Member Economies or is accessible in more than one economy.

Indeed, the seriousness of intent among Member Economies is best seen in the following extracts from Part B of the APEC Privacy Framework:

44. Taking into consideration existing international arrangements and existing or developing self-regulatory approaches (including those referenced in Part B. III., below), and to the extent permitted by domestic law and policy, Member Economies should consider developing cooperative arrangements and procedures to facilitate cross-border cooperation in the enforcement of privacy laws.

.....

46. Member Economies will endeavor to support the development and recognition or acceptance of organizations' cross-border privacy rules across the APEC region, recognizing that organizations would still be responsible for complying with the local data protection requirements, as well as with all applicable laws. Such cross-border privacy rules should adhere to the APEC Privacy Principles.
47. To give effect to such cross-border privacy rules, Member Economies will endeavor to work with appropriate stakeholders to develop frameworks or mechanisms for the mutual recognition or acceptance of such cross-border privacy rules between and among the economies.
48. Member Economies should endeavor to ensure that such cross-border privacy rules and recognition or acceptance mechanisms facilitate responsible and accountable crossborder data transfers and effective privacy protections without creating unnecessary barriers to cross-border information flows, including unnecessary administrative and bureaucratic burdens for businesses and consumers.

This aspect is where APEC Member Economies still have the most work to do. In the near future at least, this will have to be developed in the context of existing or imminent domestic privacy and other law.

In broad terms, issues involved in implementing the APEC Privacy Framework at the international level will be legal, technical, or policy oriented.¹⁵

More specifically, mechanisms have to be found that ensure that when more than one jurisdiction is involved, the personal information neither suffers from more and more rules applying to it nor loses any of the protection it had when it was first collected. In other words, consistent with APEC Privacy Principle 9, accountability follows the data – no more, no less.

Building on the wording of Part B of the APEC Privacy Framework, there are a number of options for achieving this objective, including:

- A single, government backed authority such as an ‘APEC Privacy Commission’ that can engage, encourage, assist and enforce the Framework when more than one Member Economy is involved
- One or more Non Government Organisation (NGO) that offer similar services to an official ‘APEC Privacy Commission’¹⁶
 - Such bodies would need to work very hard to establish their authority and credibility
 - Government backing of some sort would almost certainly be essential to establish this authority and credibility
 - They would require subscribing organisations to commit to a set of Privacy Principles that meet the requirements of the APEC Privacy Framework, have suitable quality assurance processes in place and an easy to use dispute independent resolution mechanism
- Binding corporate rules
 - This is the approach foreshadowed earlier in the paper, under which a company would establish internal corporate rules that meet the requirements of the APEC Privacy Framework, and then legally ‘bind’ itself to those rules in an enforceable way
 - Enforcement mechanisms, including an independent dispute resolution, would need to be established
- A cooperative arrangement between the regulators in Member Economies who have responsibility for enforcing privacy standards for enforcing the APEC Privacy Framework in a way that makes sure that ‘accountability follows the data’ in such a way that personal information being handled in more than one jurisdiction neither suffers from more and more rules applying to it nor loses any of the protection it had when it was first collected.

This list is by no means exhaustive. Each Member Economy is also likely to have its own opinion on which option it prefers. However, for the APEC Privacy Framework to be credible for

¹⁵ “Issues to be Considered in the International Implementation of APEC Privacy Framework”, Paper 2005/SOM3/ECSG/SEM/009 presented to the 2nd Technical Assistance Seminar and online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0079.File.v1.1

¹⁶ A description of key requirements of such a body are set out in “Web Seals: A Review of Online Privacy Programs”, Paper 2005/SOM3/ECSG/SEM/008 presented to the 2nd Technical Assistance Seminar and online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0078.File.v1.1

personal information being handled in more than one jurisdiction, it will be essential to find some common ground.

There are some precedents and the beginnings of a solution emerging. For example, the *Privacy Act 1998* in Australia¹⁷ allows a company or groups of companies to obtain approval for privacy codes that requires “at least the equivalent of all the obligations” set out in the National Privacy Principles established by the Act. Such codes then replace the National Privacy Principles and are enforceable under the Act. A code can also gain approval to have its own independent adjudicator.¹⁸ In theory at least, similar legislation in other economies could allow a company to ‘join the dots’ between economies to get a single code approved. This is one possible mechanism to support Binding Corporate Rules or to support an NGO model.

Some of the privacy regulators in Member Economies have also begun informal discussion about the level of cooperation that they can undertake within their current legal frameworks. A survey of international data transfer provisions was also prepared for the 2nd Technical Assistance Seminar in 2005.¹⁹ The US Federal Trade Commission also shared its experiences on resolving complaints in an international context, including its “SAFE WEB” proposals at the 2nd Technical Assistance Seminar.²⁰

In addition to the direct work that APEC is undertaking on privacy, other APEC forums are addressing privacy in the work that they are doing such as the development of a Regional Movement Alert List (RMAL) multi-lateral framework.²¹

On a separate but related front, the Organisation for Economic Cooperation and Development (OECD) is about to conduct a survey cross-border co-operation in privacy law enforcement. OECD is very keen to include the responses of economies that are not members of OECD.

¹⁷ The *Privacy Act 1988* is online at:
www.comlaw.gov.au/ComLaw/Management.nsf/current/bytitle/32AA97DFE9AA8326CA256F7100071D25?OpenDocument&VIEW=compilations

The most relevant part of the Act is Part IIIAA ‘Privacy codes’, online at:
www.comlaw.gov.au/ComLaw/Legislation/ActCompilation1.nsf/bodylodgmentattachments/6BD809D508C0AF75CA2570CA0011DAF1?OpenDocument#para2.959

¹⁸ For more detail on privacy codes, adjudicators etc, see the Privacy Codes page of the Privacy Commissioner’s website at:
www.privacy.gov.au/business/codes/index.html

¹⁹ “A Survey of International Data Transfer Provisions in Existing Data Protection Legislation – Case Studies”, Paper 2005/SOM3/ECSG/SEM/005 presented to the 2nd Technical Assistance Seminar and online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0075.File.v1.1

²⁰ “Resolving Complaints In An International Context – FTC Experience with International Cooperation in Law Enforcement”, Paper 2005/SOM3/ECSG/SEM/012 presented to the 2nd Technical Assistance Seminar and online at:
www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf.Par.0082.File.v1.1

²¹ “Regional Movement Alert List (RMAL)”, Paper 2005/SOM3/CTTF/027 presented to the Counter Terrorism Task Force III meeting, 10-11 September 2005, Gyeongju, Korea, online at:
www.apec.org/apec/documents_reports/counter_terrorism_task_force/2005.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/cttf/mtg/2005/pdf.Par.0087.File.v1.1

Further work

At the end of the 2nd Technical Assistance Seminar, the Consultants to the Seminar tabled a report on the two seminars which was formally tabled at the ECSG meeting.²² A copy of the Executive Summary of the report is set out in the [Appendix](#). The list of action items set out in the Executive Summary reflected all the work of the Seminar and the Data Privacy Subgroup. It presents a good starting point for further work by APEC on implementing its Data Privacy Framework over the next year or two.

Industry, regulators with privacy enforcement responsibilities and government policy makers will need to work together to deliver on the action list.

In one area in particular, there is willingness to pioneer a solution. Some leading global businesses want to establish corporate rules that apply the APEC Privacy Framework meaningfully. It has been suggested that the three key next steps for them to do so involve:

- a. Creating a checklist for industry accountability as a precursor for leading businesses to put together corporate rules that apply the APEC Privacy Framework
- b. Development of process for “approvals” of such rule sets
- c. Creation of international trust on enforcement of such rules

The achievements by APEC to date lay a very solid foundation for such pioneering work to be carried forward over the next year or two, right up to the point of actual implementation.

Further work could be identified in the Information Privacy Individual Action Plans that the Data Privacy Subgroup is considering asking Member Economies to complete. A draft template for such plans will be considered when the Subgroup meets on 22 February 2006.

Member Economies are strongly encouraged to participate in the OECD survey cross-border co-operation in privacy law enforcement. The survey and proposals for further cooperation have great potential to assist in improving the care of personal information world wide.

Concluding remarks

Over the last three years since APEC commissioned the Data Privacy Subgroup to develop an APEC Privacy Framework, there has been remarkable progress. Working quietly in the background, this group has proceeded with great determination and great speed to cover a lot of ground. Rarely has a task as difficult as establishing a regional privacy framework been achieved in such a short time.

Moreover, Member Economies have already started discussing the implementation of the Framework at both the domestic and international levels, starting with the two Technical Assistance Seminars in 2005 and this Seminar at the start of 2006.

Member Economies have built a lot of momentum. The challenge now will be to maintain this momentum, including in finding the APEC way of respecting personal information when it is handled in more than one jurisdiction.

²² “Final Report of the 2nd Technical Seminar on APEC Privacy Framework”, Paper 2005/SOM3/ECSG/021, tabled at the ECSG meeting of 8 September 2005, online at: www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2005/MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2005/pdf/Par.0047.File.v1.1

Report of Second Technical Seminar on APEC Privacy Framework

Gyeongju, Korea

5-6 September 2005

Executive Summary

This executive summary is submitted by consultants to facilitate discussion in meetings subsequent to the Seminar. It represents no more than the consultants own summing up of the lessons of the Seminar.

Framework considerations

- Consistent with the original mandate for developing the APEC privacy framework, focus on implementation models that facilitate international trade through the safe, efficient movement of personal information that is an integral component of business transactions
 - Recognise that in many economies, ‘privacy’ is not a strong public policy issue, with little public demand for action
 - Also recognise that for economies where there is a concern for the protection of personal information supported by legislative frameworks, they are seeking ways of protecting the personal information of their citizens when it is processed in other APEC economies
- Focus on accountability for personal information, wherever it happens to go, as the basis for safe, efficient flow of personal information between economies, consistent with Principle 9, rather than control of personal information at the point of it crossing the border from one economy to the next
- Framework action should recognise two complementary components
 - Governance
 - establishment of systems in businesses that demonstrably comply with APEC principles and the clearly articulated needs of regulators
 - in particular, Business gets uniform rules for back end and can get compliance mechanism efficiently approved in the region
 - Remedy
 - Use of company complaint resolution processes as a first resort

Simple, effective remedy for consumers, preferably through a ‘one stop shop’ contact point in their own economy that does not depend on the consumer having to chase ‘data trails’

Regulator remains domestic authority but gains cooperation across borders

- ‘Think big; act small’ strategies
 - Develop solutions consistent with existing laws and mandates where possible

Action Steps for the year ahead

- Working groups of the Privacy sub group of ECSG be formed to carry forward work in particular areas including
 - Cooperation between developed and developing economies in the introduction of education and training programs
 - Cooperation among developed economies to explore mechanisms for compliance with the APEC Privacy Framework in cross-border transfers of information
 - Policy initiatives to find solution paths for business and government

Particular objectives that the working groups would facilitate should include:

- Continue outreach activities to those economies without their own privacy frameworks who are seeking to implement the APEC privacy framework, whether applied to domestic or international transfers of personal information
 - This might include seminars, workshops or developing educational resources and exchanges of policy information with key economy stakeholders such as policy makers, business and consumer groups
- A development program for staff of regulatory authorities with a focus on reaching a common understanding of the mandate of individual regulator/agencies
- APEC Privacy regulatory authorities develop more effective ways of consulting with each other, perhaps drawing on the ‘London Action Plan’ and methods of interaction developed in other forums such as ICPEN
 - All economies to identify agencies/regulators that need to be involved, if any
- Business, perhaps through representative bodies, to establish dialogue with regulatory authorities also acting in concert
 - Developing a stronger common understanding of global business information flows, drawing on the data flow modelling already under way
 - Focusing on internal governance and accountability

- Exploring the potential for non-government dispute resolution and trustmark bodies to contribute to efficient and effective governance and remedy arrangements
 - Clear government support for the action of these bodies may need to be considered
- Continued progress of Multi-Layered Privacy Notices in the APEC region
 - Complete and circulate “Ten Steps to an Effective Privacy Notice” as a collaborative effort between data protection authorities, consumer organisations and the private sector

Action over the longer term

- Economies to consider whether legislative change is needed to facilitate cooperative work between regulatory authorities
- Public engagement and education strategies, focusing on consumers and small business



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/004

Agenda Item: 2

General Issues for Information Privacy in E-Commerce

Purpose: Information

Submitted by: Warner Bros. Online



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

A stylized, metallic-looking tower with the Warner Bros. shield logo and the text "WARNER BROS. STUDIO" on its side. The tower is positioned on the left side of the slide, with a yellow wavy line extending from its base towards the right.

General Issues for Information Privacy in E-Commerce

Michael Lewis

VP, General Counsel and CPO

Warner Bros. Online



Guiding Principle

Respecting the privacy rights of individuals while encouraging economic growth and development



The Global Marketplace

- Methods and touch-points for data collection are evolving
- Distribution territories do not match political borders
- Customers are best served by easy but safe cross-border data flow



Lessons Learned

- Good privacy is good business
- Policy + Technology = Good Privacy
- Consumers respond to transparency, simplicity and control



Benefits of Principles

- Flexible and proportionate requirements lead to better products and services
- Principles can be applied to changing technologies
- Privacy becomes integral to the business



That's All, Folks!



LOONEY TUNES, characters, names and all related indicia are trademarks of Warner Bros., © 2003



Thank You

Michael Lewis

VP, General Counsel and CPO

Warner Bros. Online

michael.lewis@warnerbros.com



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/005

Agenda Item: 3

Human-Human Communication in Globalizing & Computerized World

Purpose: Information
Submitted by: United States



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Human-Human Communication in a Globalizing & Computerized World

February. 20, 2006

Alex Waibel

International Center for
Advanced Communication Technologies

Carnegie Mellon University

University of Karlsruhe

<http://www.interact.cs.cmu.edu>



....will know more about us
....should know more about us

... to serve us better.



- InterACT
 - International Center for Advanced Communication Technologies
 - Joint Center between Carnegie Mellon and University of Karlsruhe
 - Emerged from 15 year Collaboration
 - Launched January, 2004
- Mission of Center
 - To Develop Advanced Communication Technologies
 - To Facilitate Student Exchange and Training
- Major Ongoing Projects
 - CHIL – Computer Supported Human-Human Interaction
 - TC-STAR & STR-DUST & TRANSTAC & GALE –
Speech Translation
 - TIDES & ASSIST &... - Text, Image Translation

Phone Calls During Meetings



Phone Calls During Meetings





JEFF'S CONTEXT INFO														
Context	environment	UNKNOWN												
	environment model													
	in smartroom? situation	YES MEETING												
Current State	MEETING													
Availability	<table border="1"> <thead> <tr> <th>Contact</th> <th>Talk</th> <th>Message</th> </tr> </thead> <tbody> <tr> <td>personal</td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td>business</td> <td><input type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>VIP</td> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>	Contact	Talk	Message	personal	<input type="checkbox"/>	<input type="checkbox"/>	business	<input type="checkbox"/>	<input checked="" type="checkbox"/>	VIP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
	Contact	Talk	Message											
	personal	<input type="checkbox"/>	<input type="checkbox"/>											
business	<input type="checkbox"/>	<input checked="" type="checkbox"/>												
VIP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>												
Phone Alert	<table border="1"> <tbody> <tr> <td>personal</td> <td>MUTE</td> </tr> <tr> <td>business</td> <td>MUTE</td> </tr> <tr> <td>VIP</td> <td>EXCLUSIVE</td> </tr> </tbody> </table>	personal	MUTE	business	MUTE	VIP	EXCLUSIVE							
personal	MUTE													
business	MUTE													
VIP	EXCLUSIVE													

Memory Jog

....What was his name? ...Where did I meet him? ...What did we discuss last time?

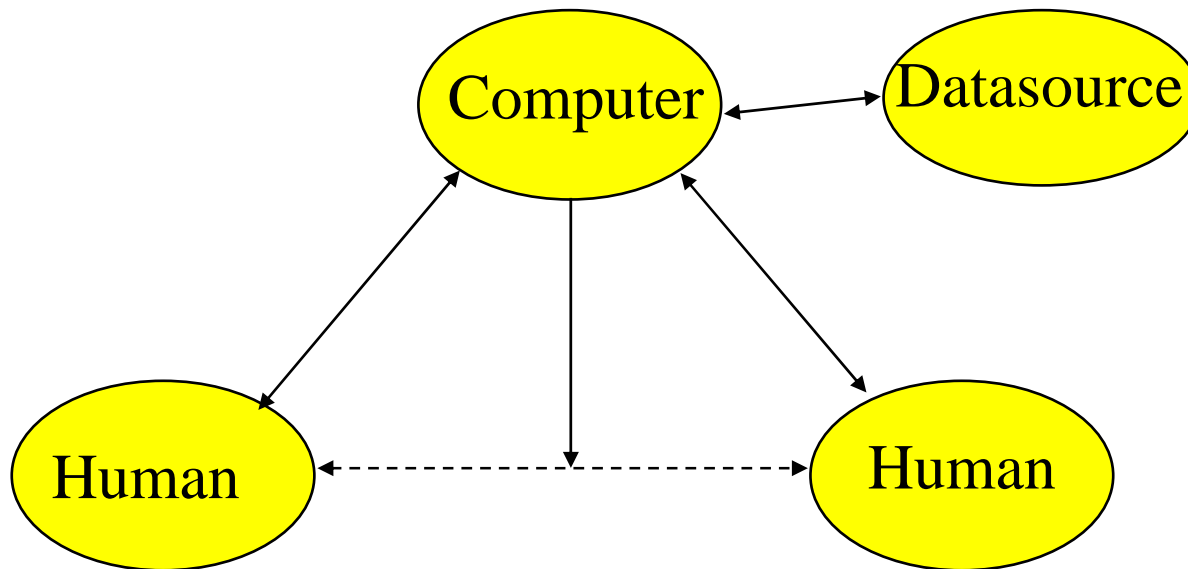




....and what is he saying?



你们的评估准则是什么



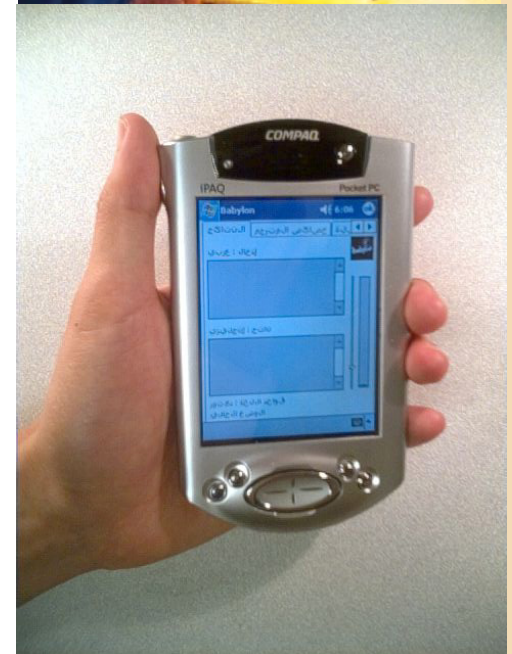
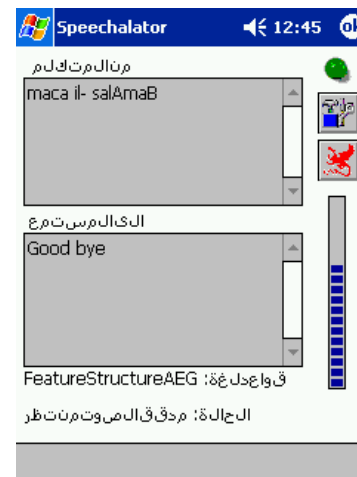
Goal: Technology to Improve Human Communication

- Making Computer Services Implicit/Invisible
 - Computers in the Human Interaction Loop
 - Implicit Computing Services Supporting Human Communication
 - Observe, Use, Understand Human Communicative Context
 - Projects: CHIL
- Speech Translation to Bridge the Language Divide
 - From Domain Limited Fieldable Systems to Domain Unlimited Speech Translation
 - Usable by Anyone to Communicate Anywhere with Anyone
 - Projects: STR-DUST, TC-STAR, GALE
- Support
 - European Commission FP-6, Integrated Projects
 - US: NSF, DARPA

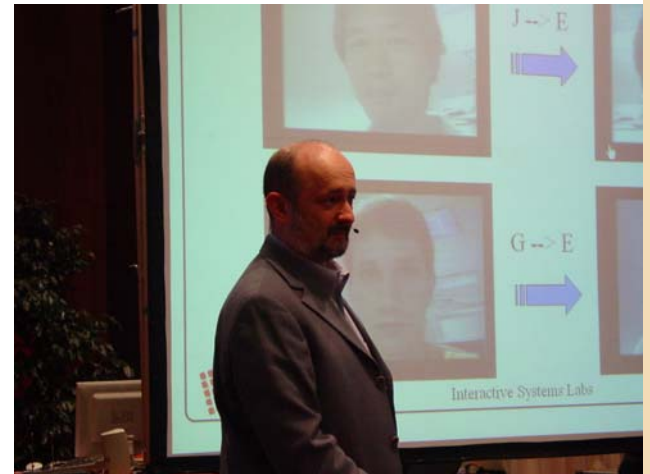
Fieldable Systems:

PDA Speech Translators

- Tourism
 - Conferences
 - Business
 - Olympics
- Humanitarian
 - Refugee Registration
 - First Responder
 - Healthcare
 - USA, Latino Population
 - Europe, Expansion
 - Third World
- Government
 - Peace Keeping, Police



- Applications:
 - TV, Radio, Lectures, Speeches, Meetings,...
- Technical Difficulty:
 - Open Domain, Open Vocabulary, Open Speaking Style
 - Spontaneous Speech, Disfluencies, Ill-Formed Sentences
 - Too Complex to Program Rules
- How it is Done:
 - Develop Statistical Learning Algorithms
 - Learn Speech and Translation Mappings from Large Example Corpora
 - With Increasing Data on the Internet, Improving Performance & Generalization
- Performance:
 - Depends on Language, but already Generally Understandable



Translation of Speeches



MR PRESIDENT

señor presidente

“Why did Joe get angry at Bob about the budget ?”

Need Recognition and Understanding of Multimodal Cues

- Verbal:

- Speech
 - Words
 - Speakers
 - Emotion
 - Genre
- Language
- Summaries
- Topic
- Handwriting

- Visual

- Identity
- Gestures
- Body-language
- Track Face, Gaze, Pose
- Facial Expressions
- Focus of Attention



We need to understand the: **Who, What, Where, Why and How !**

- **Who & Where ?**

- Audio-Visual Person Tracking
- Tracking Hands and Faces
- AV Person Identification
- Head Pose / Focus of Attention
- Pointing Gestures
- Audio Activity Detection

- **What ? (Input)**

- Far-field Speech Recognition
- Far-field Audio-Visual Speech Recognition
- Acoustic Event Classification

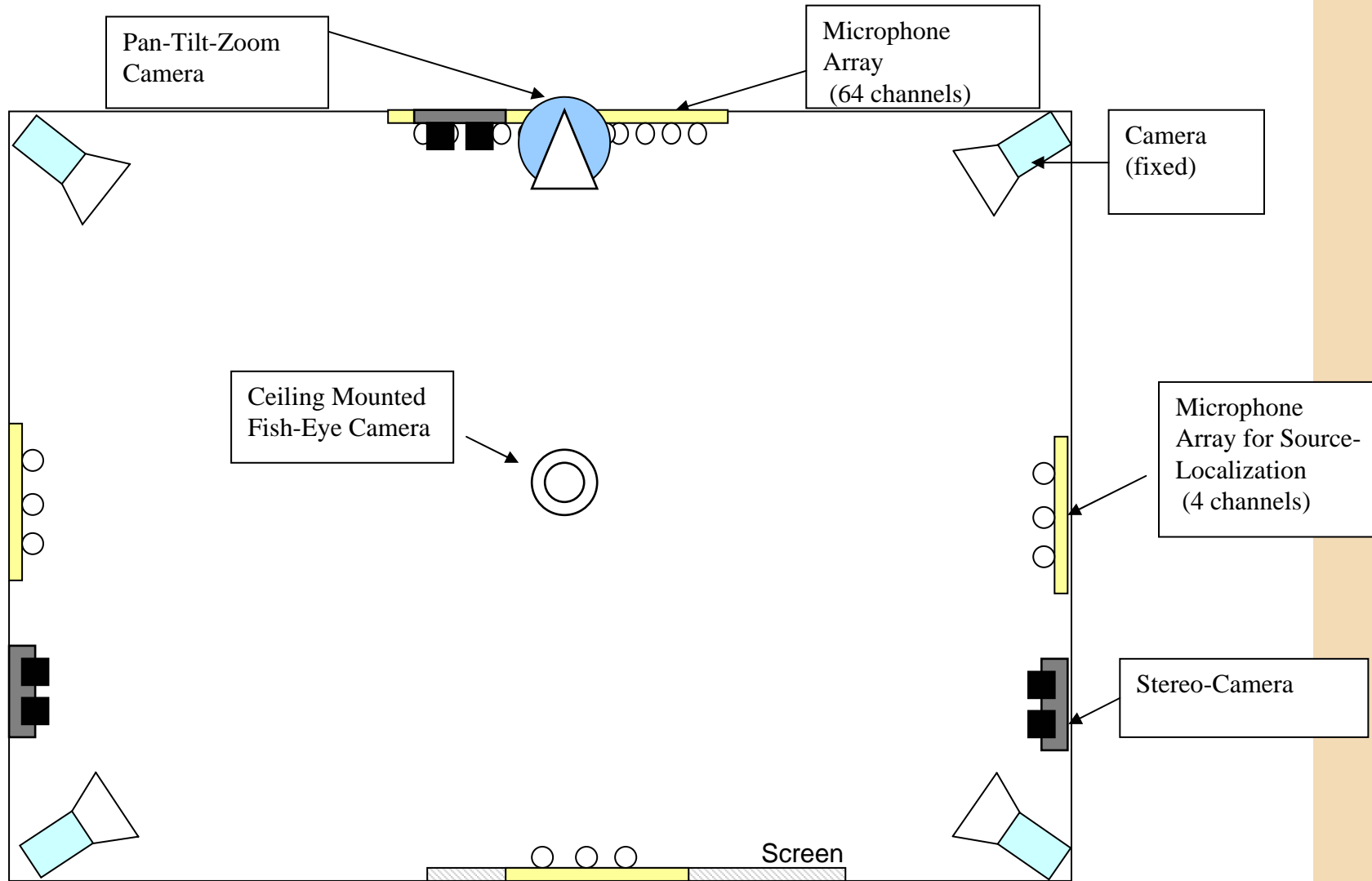
- **What ? (Output)**

- Animated Social Agents
- Steerable targeted Sound
- Q&A Systems
- Summarization

- **Why & How ?**

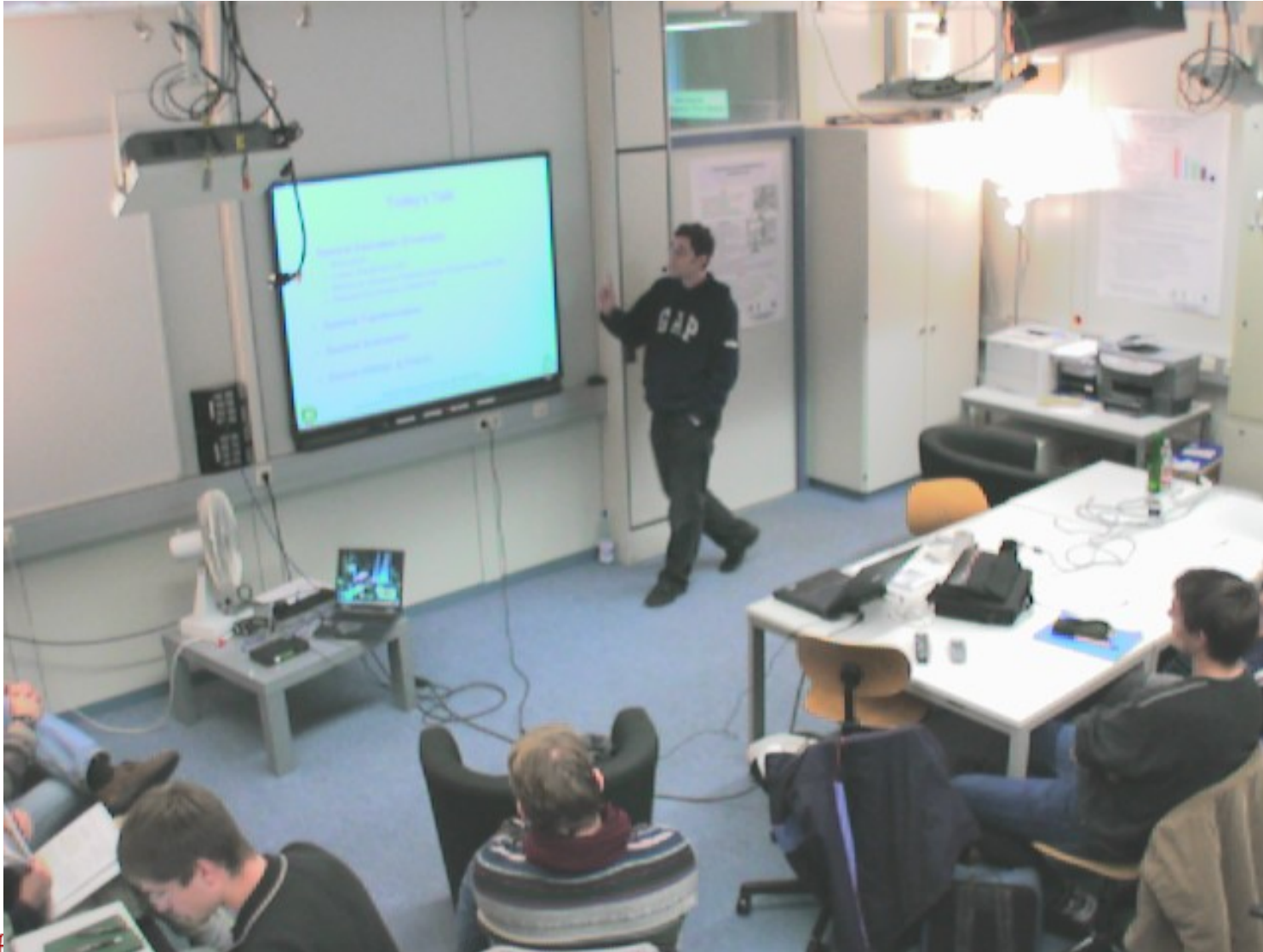
- Classification of Activities
- Emotion Recognition
- Interaction & Context Modelling
- Vision-based posture recognition
- Topical Segmentation

Sensors in the CHIL Room



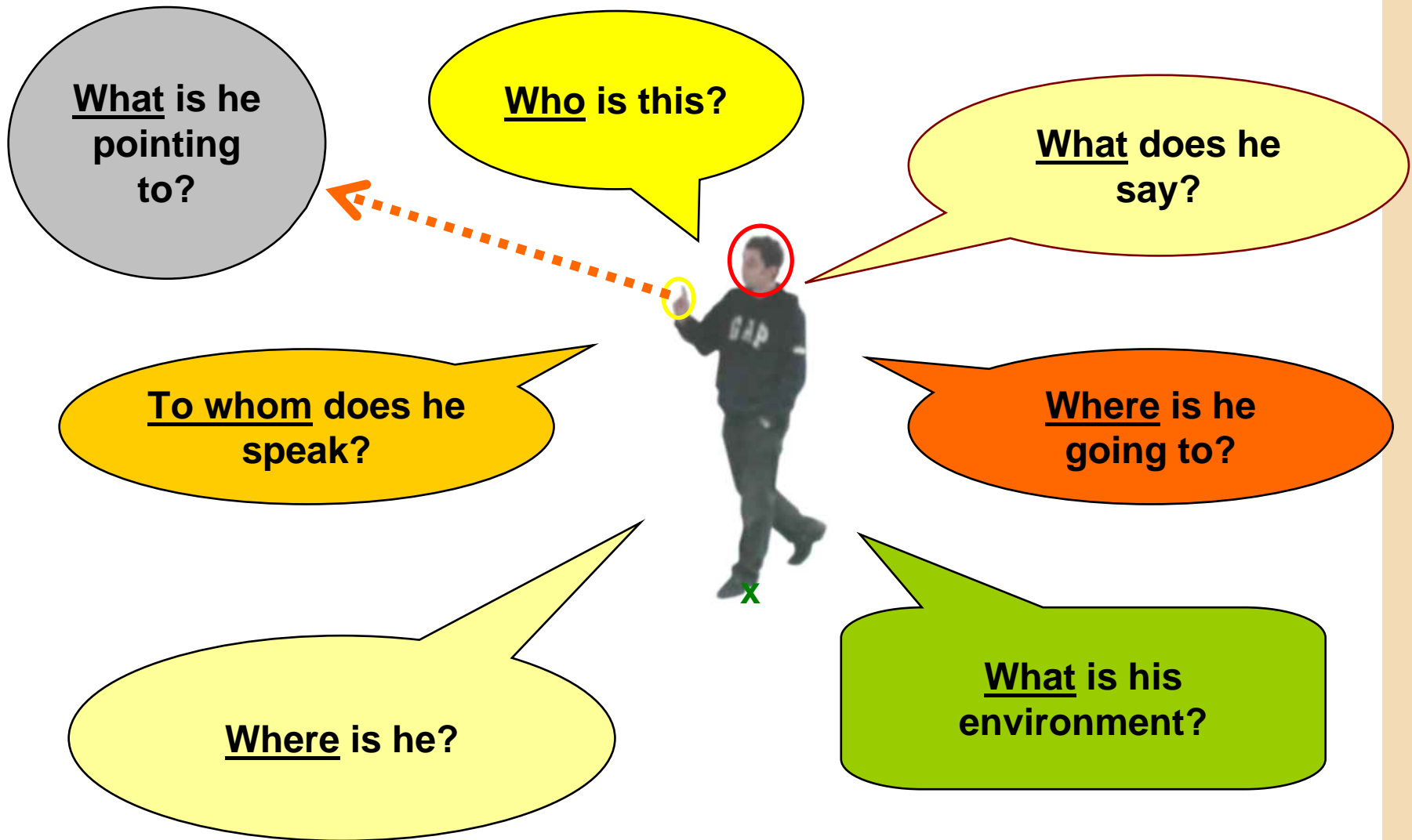
Scenario 1: Seminars/Lectures

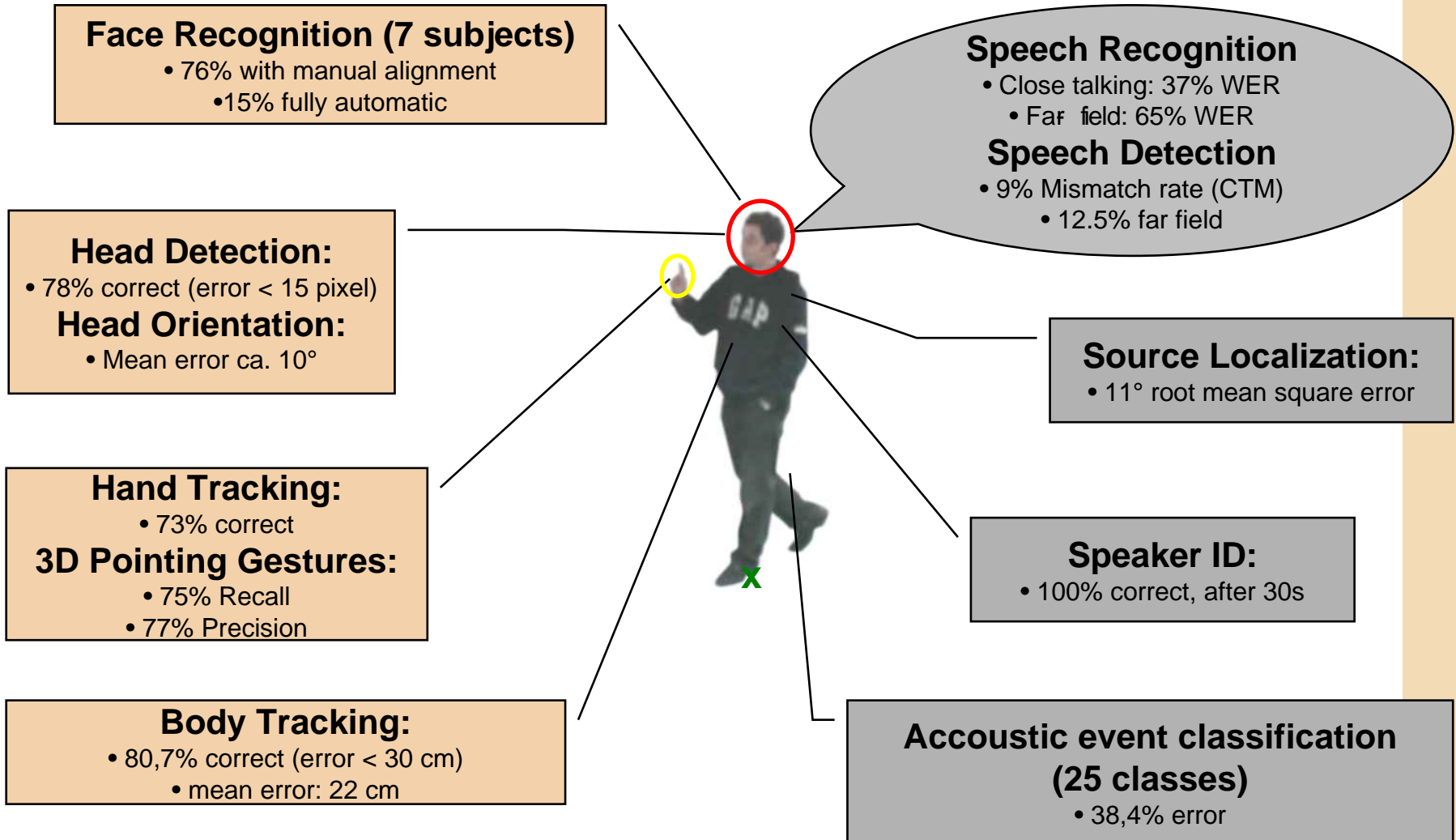




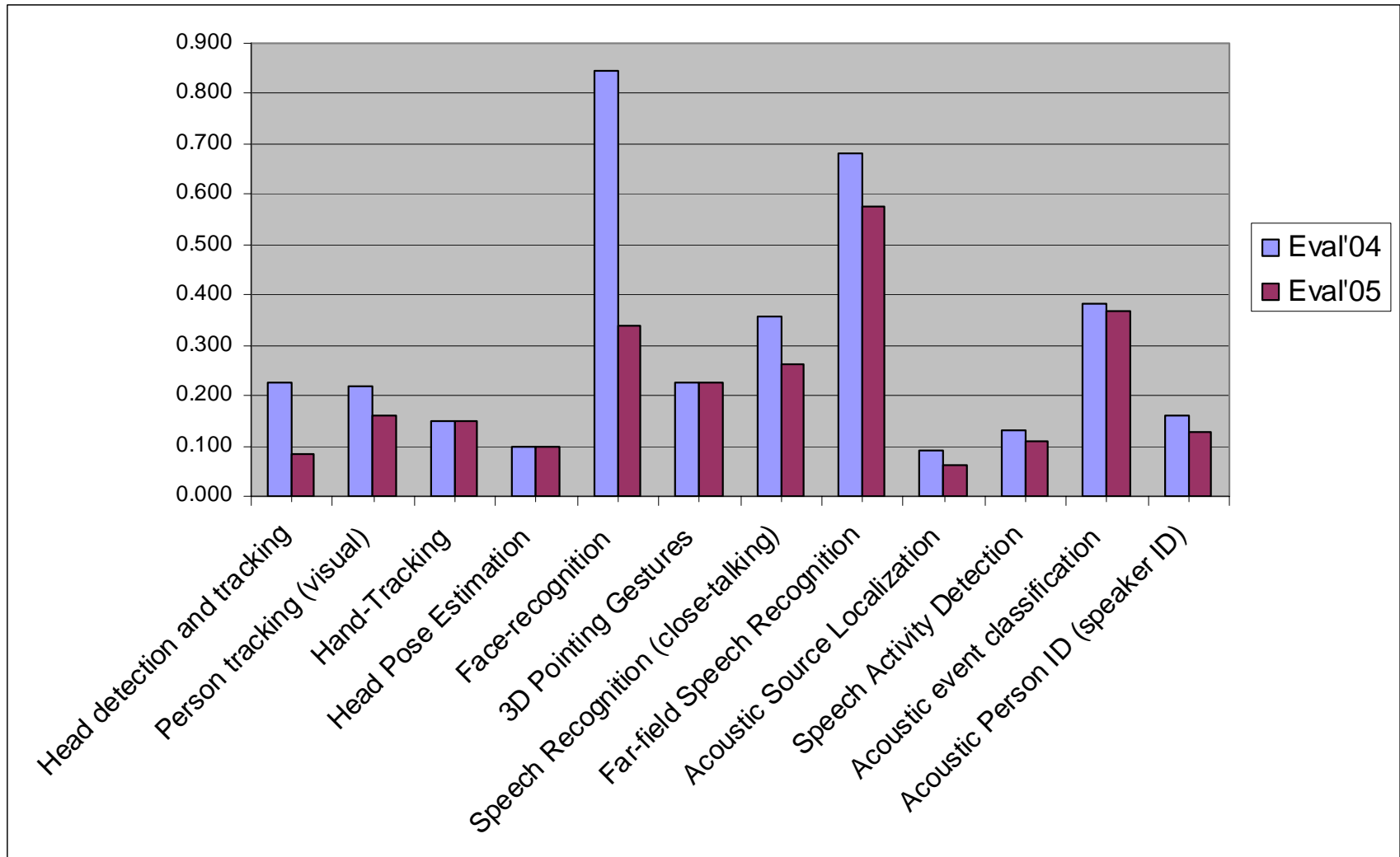
Describing Human Activities







1-Year: Results and Progress



Joint US (NIST) and EC Programs

- RT-Meeting'06 – Rich Transcription
 - Emerges from established DARPA activity
 - MLMI Workshops, AMI/CHIL
 - Evaluated Verbal Content Extraction
 - Chair: Garofolo (NIST)

- CLEAR'06 –

Classification of Locations, Events, Activities, Relationships

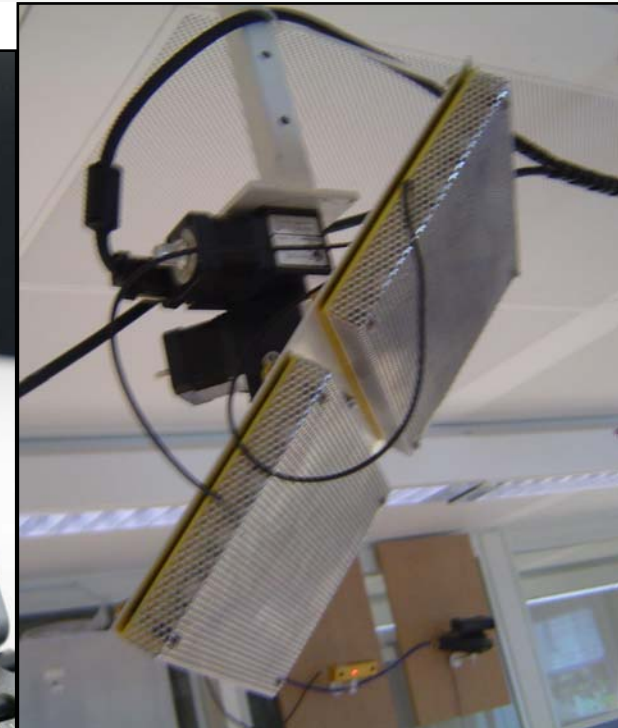
- Emerging from European program efforts (CHIL, etc.) and US-Programs (VACE,..)
- First Joint Workshop to be Held in Europe
after Face & Gesture Reco WS, April 6 & 7, Southampton
- Chair: Stiefelwagen (UKA)



- **Connector**
 - Connects people through the right device at the right moment
- **Memory Jog**
 - Unobtrusive service. Helps meeting attendees with information
 - Provides pertinent information at the right time (proactive/reactive)
 - Lecture Tracking and Memory
- **Attention cockpit**
 - Informs the current speaker about interest/boredom of audience
- **Socially Supportive Workspaces**
 - Physically shared infrastructure aimed at fostering collaboration
- **Simultaneous Translation Services**
 - Detect Language Need and Deliver Services Inobtrusively

Private and Public Information Delivery

- CHIL phone
- Steerable Camera Projector
- Targeted Audio
- Retinal and Heads-Up Displays



- Trust
 - Is Translation/Information Believable?
 - Must Measure and Communicate Confidence
- Control
 - Is Implicit Service Correct/Desired/Wanted?
 - Must Occasionally Control, Communicate Intent
 - Balance Between Autonomy and Control
- Privacy
 - Is Information Secure and Private?
 - Personalized
 - Access Control

Interactive Machine Learning a Key Technology!

Human-Human Communication Technologies

- Paradigm Shift in Human-Computer Interaction
- Potential for Significant Improvements for
 - Productivity Improvements
 - Comfort, Convenience, Safety
 - Humanitarian, Social, Multi-Cultural Integration
- Must Study Social Issues and Trade-Offs
 - Privacy, Trust, Control



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/006

Agenda Item: 4

An Overview of Information Privacy Issues Relevant to the APEC Region

Purpose: Information

Submitted by: Japan



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

An Overview of Information Privacy Issues Relevant to the APEC Region

Professor Pauline C. Reich, J.D., M.A.
Director, Asia-Pacific Cyberlaw, Cybercrime and Internet Security
Research Institute
Waseda University Faculty of Law
Tokyo, Japan



- ❖ Cultural notions of personal privacy vary within the APEC region
- ❖ See the film - "A Great Wall" (1985) by Peter Wong for cultural differences between Chinese from PRC and visiting Chinese-American relatives (first U.S.-China production made in China)
- ❖ The notion of privacy guaranteed by law also varies within the region
- ❖ Some economies are moving in the direction of providing privacy rights guaranteed by law, e.g. Japan
- ❖ Some economies are moving or attempting to move in the opposite direction with resistance from human rights groups, e.g. U.S., Australia, UK, often using the rationale of national security for the use of technology to erode traditional privacy rights from a non-digital age
- ❖ Some economies are actively working to preserve traditional privacy rights, e.g. Canada
- ❖ Some economies are new to the concept of privacy guaranteed by law, and actively use blocking, monitoring, filtering technologies, web cams to monitor who is using cyber cafes, etc.
- ❖ Some economies are affected by the Digital Divide and have not yet formulated privacy policies or laws

- ❖ E-government and privacy
- ❖ Trust us with your data = ????
- ❖ Attacks on critical information infrastructure
- ❖ Government databases, e.g. for medical records
- ❖ Data mining, data matching
- ❖ Government requests for and retention of traffic data, etc. – Google case

- ❖ E-commerce and privacy
 - ❖ Issues for multinational corporations doing business across borders
 - ❖ Intellectual Property protection
 - ❖ National security issues
 - ❖ Protection of individual consumer data
- 2005 was a bad year, with a proliferation of identity theft cases in the U.S., for example

A PARADIGM SHIFT DUE TO NEW TECHNOLOGIES?

- ❖ Susan W. Brenner comments
- ❖ Justice Sandra Day O'Connor comments
- ❖ PRESERVATION OF EXISTING CONSTITUTIONAL PROTECTIONS OF PRIVACY VIA USE OF TECHNOLOGY?
- ❖ K.A. Taipale comments

RESOURCES FOR FURTHER THOUGHT AND DISCUSSION

FILM: "A Great Wall", Directed by Peter Wang, Produced by Shirley Sun (1985). W&S Productions/Nanhai Film Co., MGM Home Entertainment –DVD 2002.

First American feature film shot in the People's Republic of China.

For a review, see www.timeout.com/film/70542.html

BOOKS

- ❖ J.C. Cannon, PRIVACY – What Developers and IT Professionals Should Know (Pearson Education, 2005) Catalog can be found at <http://www.awprofessional.com>
- ❖ Jeffrey Rosen, THE UNWANTED GAZE – The Destruction of Privacy in America (Random House, 2000)
- ❖ Tara M. Swaminatha and Charles R. Elden, WIRELESS SECURITY AND PRIVACY – Best Practices and Design Techniques (Addison Wesley- Pearson Education, 2003) [http:// www.awprofessional.com](http://www.awprofessional.com)

Daniel J. Solove and Marc Rotenberg, INFORMATION PRIVACY LAW (Aspen Publishers, 2003)
Catalog can be found at www.aspenpublishers.com (U.S. perspective only)

❖ LAW JOURNAL ARTICLES

- ❖ Susan W. Brenner, "Symposium: The Search and Seizure of Computers and Electronic Evidence: The Fourth Amendment in an Era of Ubiquitous Technology," 75 Mississippi Law Journal 1 (Fall, 2005)
- ❖ Gayle Horn, "Note: Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines," 60 New York University School of Law Annual Survey of American Law 735 (2005)
- ❖ Jeremy Moseley, "Symposium on Security and Liberty: Note: The Fourth Amendment and Remote Searches: Balancing the 'Protection of the People' with the Remote Investigation of Internet Crimes," 19 Notre Dame Journal of Ethics and Public Policy 355 (2005)
- ❖ David Steinbock, "Data Matching, Data Mining and Due Process," 40 Georgia Law Review 1 (Fall, 2005)
- ❖ John T. Soma, Maury M. Nichols, Stephen D. Rynerson, Lance A. Maish, Jon David Rogers, "Balance of Privacy vs. Security: A Historical Perspective of the USA PATRIOT Act," 31 Rutgers Computer and Technology Law Journal 285 (2005)

- ❖ K.A. Taipale, "Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data," Columbia Science and Technology Law Review, Volume 5, page 1 (2003)
- ❖ K.A. Taipale, "Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd," 9 International Journal of Communication Law and Policy 8, (Winter, 2004/2005)

- ❖ NONPROFIT ORGANIZATION ARTICLE

- ❖ Ellen Alderman, "Homeland Security and Privacy: Striking a Delicate Balance," Carnegie Reporter (Carnegie Foundation of New York), Fall 2002, <http://www.carnegie.org/reporter/05/homeland/>

- ❖ GOVERNMENT PUBLICATIONS

- ❖ David Loukidelis, "Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing," available online and in Pauline C. Reich, General Editor, CYBERCRIME AND SECURITY (Oceana, a Division of Oxford University Press) (multiple volume looseleaf series) (CANADA)

- ❖ ASSOCIATION POSITION PAPERS RE: ONLINE PRIVACY
- ❖ Position paper from the Japan Federation of Bar Associations to the 11th United Nations Congress on Crime Prevention and Criminal Justice, March 17, 2005, <http://www.nichibenren.or.jp/en/activities/statements/20050317.html> (privacy and Council of Europe Cybercrime Convention concerns)
- ❖ American Bar Association- Letter from the President of the ABA to President George W. Bush February 13, 2006
- ❖ http://www.abanet.org/op/greco/memos/aba_domsurv_ltr_whthouse-0206.pdf (Patriot Act/government surveillance)
- ❖ American Library Association
<http://www.ala.org/ala/washoff/WOIssues/civilliberties/theusapatriotact/usapatriotact.htm>



RELEVANT WEBSITES

- ❖ Reporters without Borders
- ❖ Privacy International
- ❖ See Briefing for Members of the European Parliament on Data Retention Sept. 26, 2005 for a contrast with U.S. view [http://www.privacyinternational.org/article.shtml?cmd\[347\]=x-347-367988](http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-367988)
- ❖ Electronic Frontier Foundation
- ❖ Electronic Privacy Information Center
- Japan Federation of Bar Associations

- ❖ LAWSUITS
- ❖ American Civil Liberties Union et al v. National Security Agency/ Central Security Service, Complaint for Declaratory and Injunctive Relief, pdf file at <http://www.findlaw.com>

- LAW
- Japan Privacy Resource
- <http://www.privacyexchange.org/japan/main.html>



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/007

Agenda Item: 5

Presentation to APEC Privacy Symposium

Purpose: Information
Submitted by: United States



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

MAUREEN COONEY
Acting Chief Privacy Officer

PRESENTATION TO APEC
PRIVACY SYMPOSIUM

February 20, 2006



Homeland
Security

The Privacy Office

Introduction to the DHS Privacy Office

- The Setting:
 - First Statutorily Mandated CPO in the U.S. Gov't.
 - International Policy Concerns: Privacy does not end at the water's edge
- Triad of U.S. Privacy Authorities:
 - Privacy Act of 1974: Public Notice and Accountability
 - Freedom of Information Act (FOIA): Transparency and Privacy Protections
 - E-Government Act of 2002: Introduced PIAs



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 2

Overview of the DHS Privacy Office

Organization

1. Legal
 2. International
 3. Disclosure
 4. Education
 5. Compliance
 6. Technology
- + Officers in Place



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 3

International Privacy Frameworks

- APEC: 2003 Privacy Framework
- OECD: 1980 Guidelines on Transborder Flows
- EU
 - Directive 95/46/EC
 - Directives 97/66/EC and 2002/58/EC
- Various Bi-lateral Agreements, Political Commitments



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 4

Current DHS International Issues

- **APEC:** Privacy Subgroup; Lost and Stolen Passports part of RMAL
- **EU:** U.S. – EU PNR Cases before the ECJ
- **OCED:** WPISP, Enhanced Information Travel System (EITS); Biometrics
- **Various Bilateral:** Data Sharing Arrangements, e.g., Lost and Stolen Passports
- **Annual Int'l Data Protection Conference** (U.S. Observer Status)
- **“Berlin Group”** (Telecom)



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 5

STRENGTHS of APEC FRAMEWORK

- FLEXIBILITY and CONSENSUS: founded on principle of reducing barriers while maintaining privacy
- CONSISTENT WITH: 1980 OECD Guidelines
- PRIVATE and PUBLIC: flexible for both
- SELLING POINT: Privacy Awareness and Cross-border cooperation on privacy matters should be the goal for APEC Economies.



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 6

APEC Framework Compatible with Private and Government Spheres

...we are part of a global network and that in order for that network to function, people and goods have to be able to move across borders rapidly, efficiently, and safely but without sacrificing either security or privacy.

--DHS Secretary Michael Chertoff, Speech before the Woodrow Wilson School of Public and International Affairs, October 1, 2005



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 7

CONTACT INFORMATION

Maureen Cooney
Acting Chief Privacy Officer
DHS Privacy Office
U.S. Department of Homeland Security
Washington, D.C. 20528
t: 571-227-3813; f: 571-227-4171
privacy@dhs.gov



**Homeland
Security**

The DHS Privacy Office
March 26, 2006: slide 8



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/008

Agenda Item: 6

Vietnam Electronic Transaction Law 2005

Purpose: Information
Submitted by: Viet Nam



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



VIETNAM ELECTRONIC TRANSACTION LAW 2005

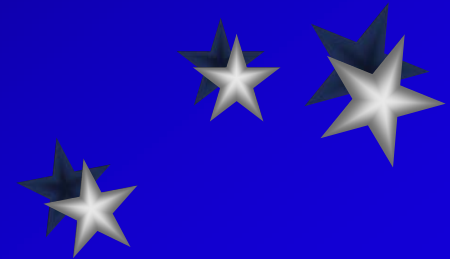
Dr. MAI ANH

Hanoi ICT Association
General Secretary



Topics

- The need to enact the E Transaction Law (ETL)
- Objectives of ETL
- Basic Principles of the ET Law
- Construction and core provisions
- Affect to society

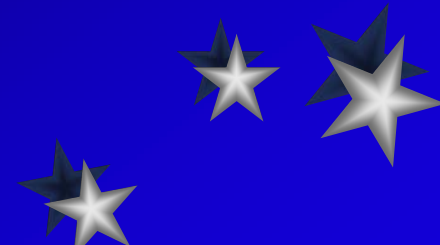


The need to enact the ETL

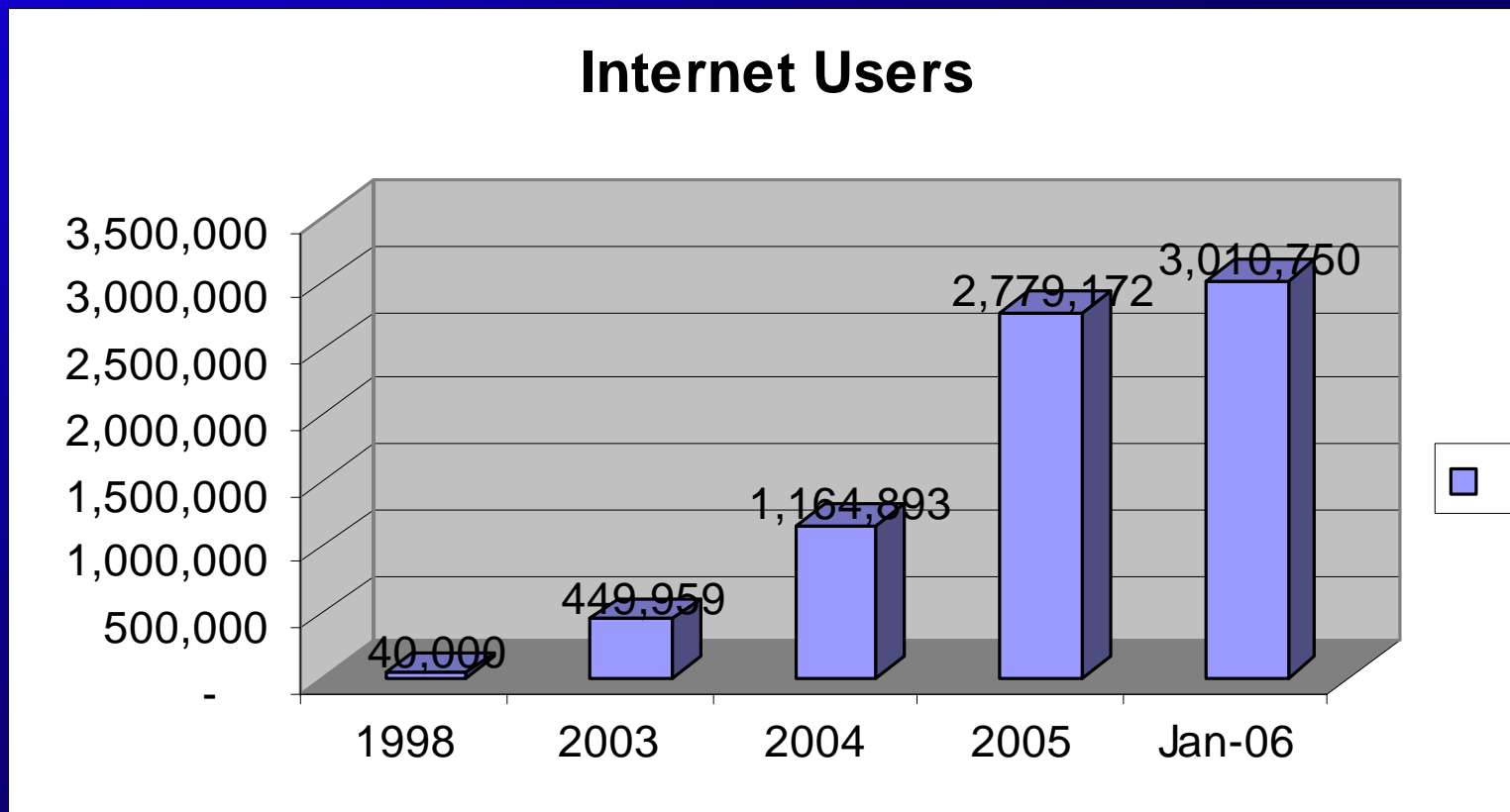
1. Requirement of ICT application in Vietnam

Vietnam has a big progress on development and application of ICT in the last 10 years

- Number of PC increase minimum 300,000 Pcs/year
- International bandwidth : increase from 2 MBps in 1997 to 3,615 Mbps 1/2006
- Internet users penetration : 12.90 %

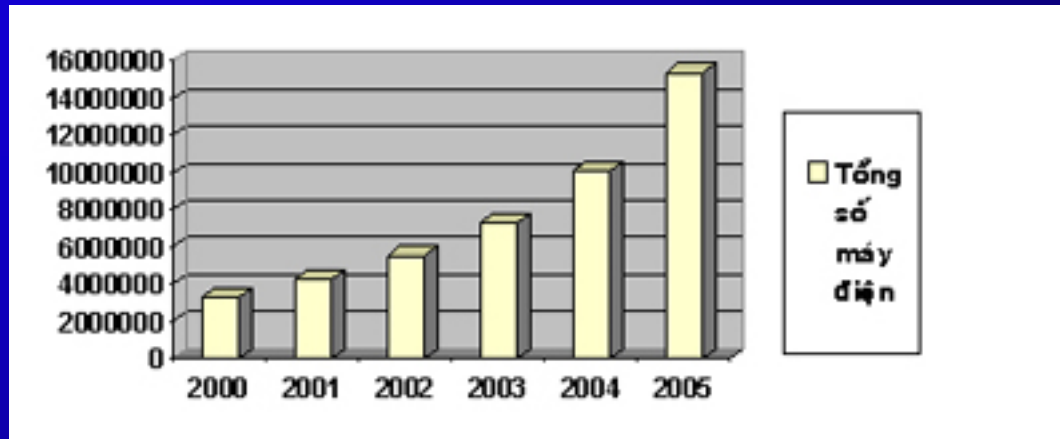


The need to enact the ETL

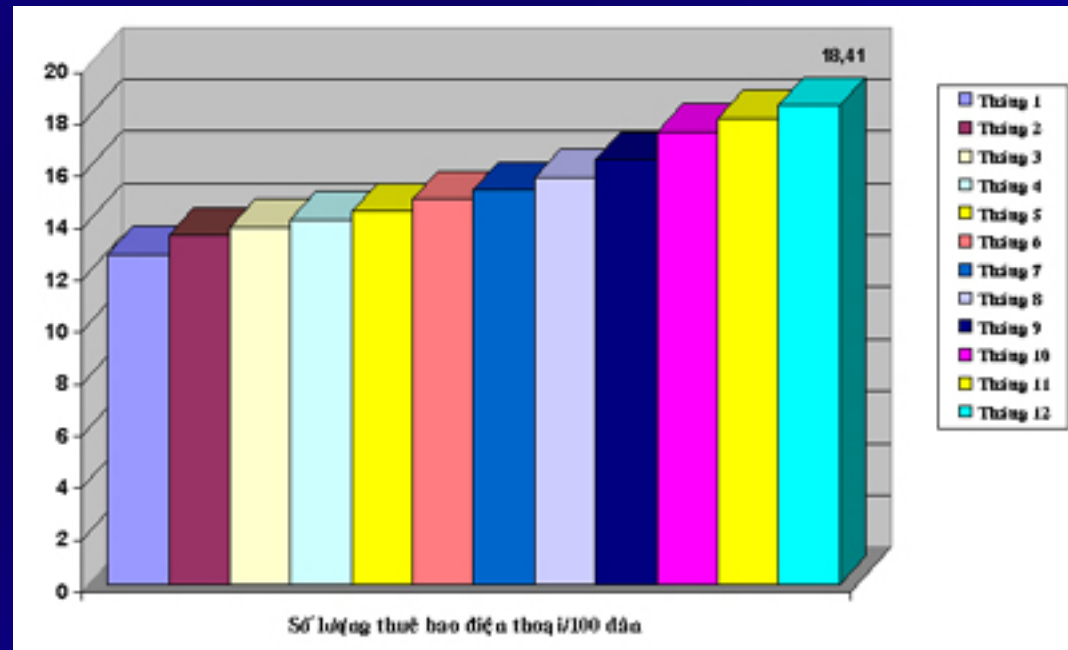


The need to enact the ETL

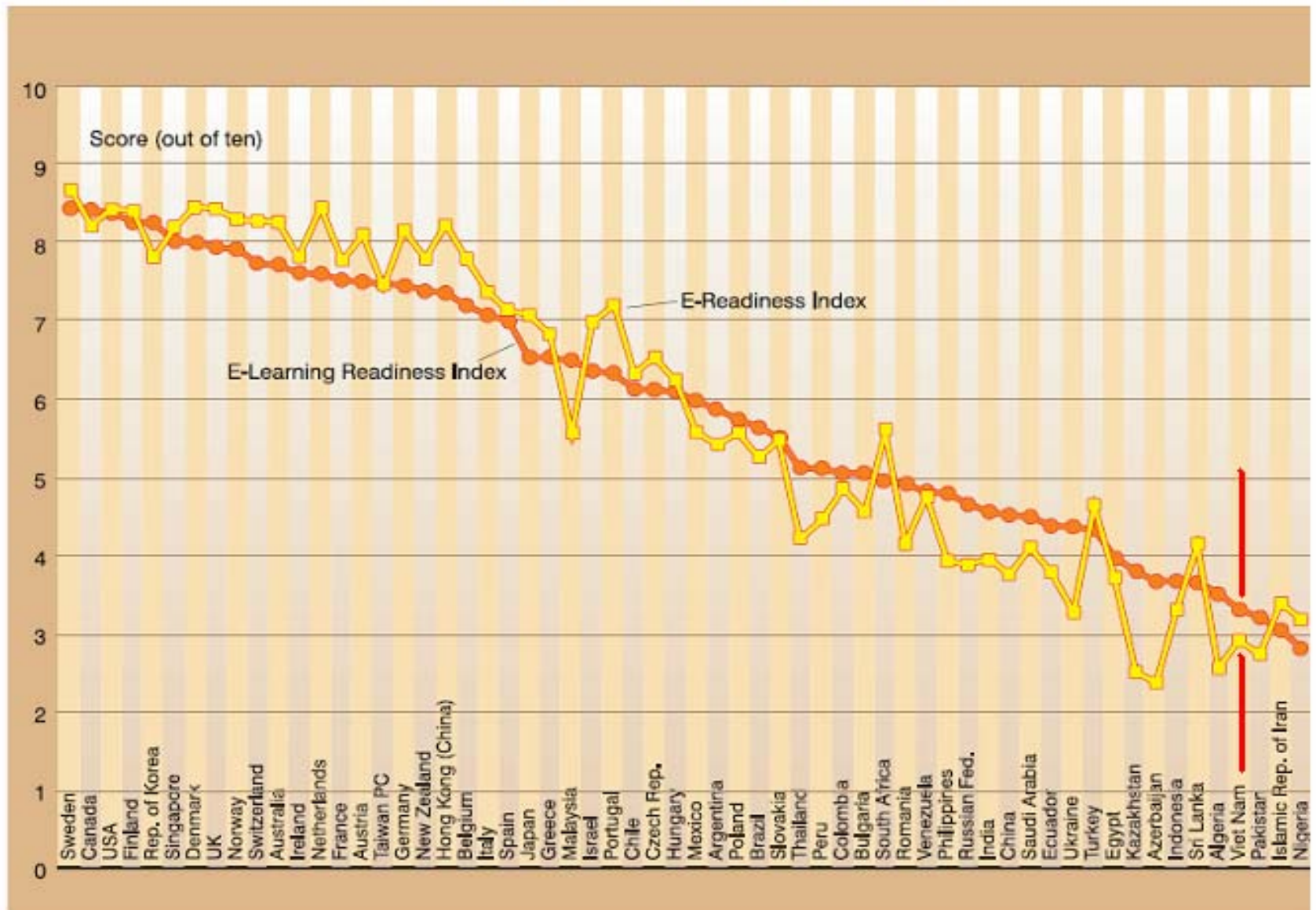
Telephone Subscribers



Telephone penetration



E-learning readiness and e-readiness



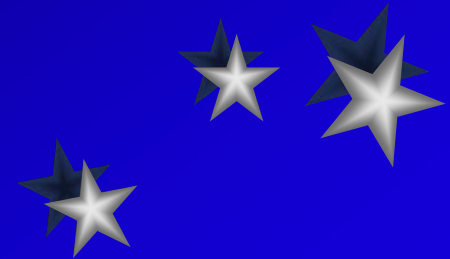
* UNCTAD based on EIU (2003a) and EIU (2003b).

The need to enact the ETL

- The governmental backbone is established since 2001
- Large activities on E. Commerce

Lack of laws and regulations to recognize the legal validity of electronic transaction

- ➔ Parallel existing 2 system : Traditional system and computerizing system
- ➔ Invest to ICT is not effectively



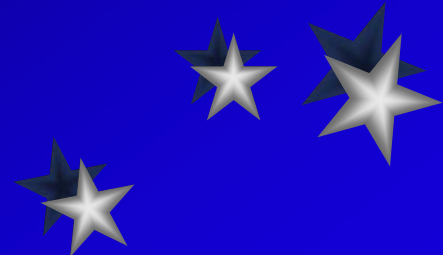
The need to enact the ETL

2. Adapt existing law system requirements

3. Requirement of the integration in the region and global



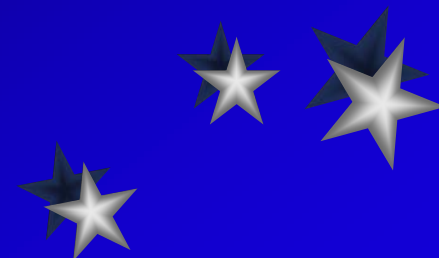
E ASEAN framework Agreement



Objectives of ETL

This law is contrued to obtain and give effects to the following purposes :

- ◆ To provide a legal environment for use and security of E transaction**
- ◆ To facilitate and promote the realizing of E Government, E Commerce**
- ◆ To spead up the administration Reform**
- ◆ To Enhance the Economy development and international Integration**



Basic principles of ETL

The E Transaction Law was contrued and developed based on these principles

- **Functional equivalence**

- Analyze traditional form of transaction in the society based on paper (“writing”, “record”, “signature”, “original”), voice .
- Analyze the provisions of existing law : Civil law, Commerce law,...according these functions
- Consider criteria necessary to replicate those functions and give data message, e- signature the same level of recognition as information on paper

- **Eliminate barriers to use E Transaction**



Basic principles of ETL

- Technology and Media neutrality

- Equal treatment of paper-based and electronic transactions
- Equal treatment of different techniques (EDI, e-mail, Internet, telegram, telex, fax); No technology shall be considered as a sole [technology] in e-transactions

- Party autonomy

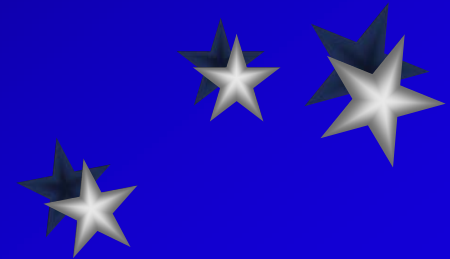
- Voluntarily select to use electronic Transaction or traditional way .
- Primacy of party agreement on whether and how to use e transaction techniques
- Parties free to choose security level appropriate for their transactions



Basic principles of ETL

- In accordance with the international laws and regulations.

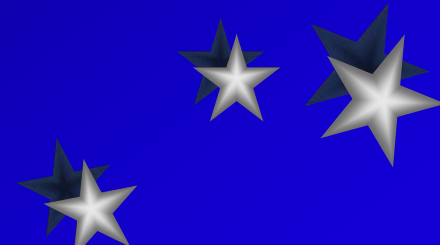
The Vietnam ETL 2005 follows closely the UNCITRAL Model Law on Electronic Commerce, which sets the framework for electronic laws in many countries.



Construction and core provisions

Construction

- **VN ETL 2005 consists of 8 Chapters and 54 Articles**
- **The Electronic Transaction Law was introduced in Parliament in May 2005, and passed on 29 November 2005. The Law will come into force on 1 March 2006.**



Core provisions :

1. General Principles in using E-Transactions :
Article 5. (**Voluntary, free choice, Party autonomy**)

2. Legal recognition of Data Message : Chapitre II

● Legal Recognition	: Article 11
● Writing	: Article 12
● Original	: Article 13
● Evidence	: Article 14
● Storage	: Article 15

Equal treatment of Paper-based and Electronic Transaction



Construction and core provisions

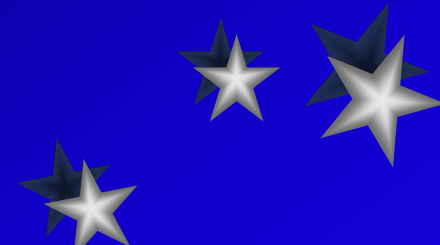
Core provisions :

3. Legal recognition of E Signature : Chapitre III

- Legal Recognition of E Signature : Article 24
Where a rule of law requires a signature, an electronic signature satisfies that rule of law.
- Principles of using E Signature : Article 23

4. E. Signature Certification (CA) and CA Service

- CA Activities : Article 28
- CA Organizations : Article 30



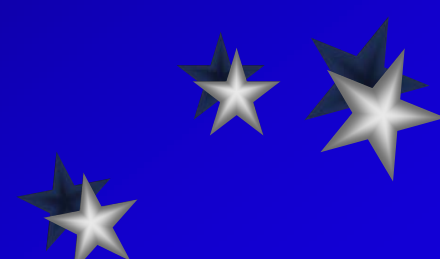
Construction and core provisions

Core provisions :

5. E Transaction in the State Agencies : CHAPTER V (G2G, G2B,G2C)

6. Confidentiality, Security and safety in E Transaction : Chapter VI

- Ensuring Security and Safety in E-transactions : Article 44.
- Protection of Data Message : Article 45.
- Information Confidentiality in E-transactions : Article 46.
- Liability of Network Service Provider : Article 47.



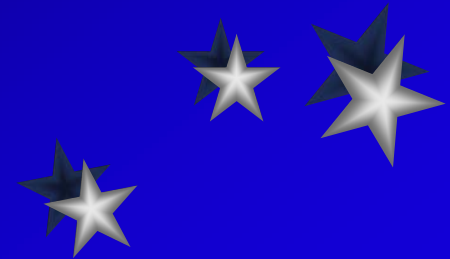
Core provisions :

Article 45. Protection of Data Message :

- *Agencies, organizations, individuals are not allowed to take any action that affects the integrity of data messages of other agencies, organizations and individuals .*

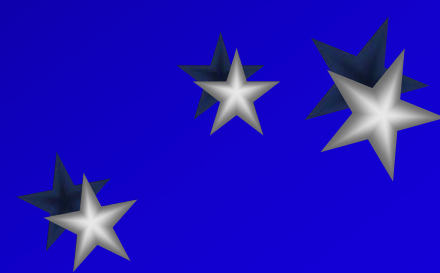
Article 46. Information Confidentiality in E-transactions :

2. *Agencies, organizations, individuals are not allowed to use, provide or disclose part or all of information related to private and personal affairs or information of other agencies, organizations, individuals which is accessible by or under the control in e-transactions*



Other provisions of VN ETL 2005

- ➡ **Prohibited activities in e-transactions** : Article 9.
- ➡ **Time and Place of dispatch Data Message** : Article 17.
- ➡ **Time and Place of receipt Data Message** : Article 19.
- ➡ **Electronic Contract** : Chapter IV
- ➡ **Dispute settlement and Handling breaches** : Chapter VII



Affect to society

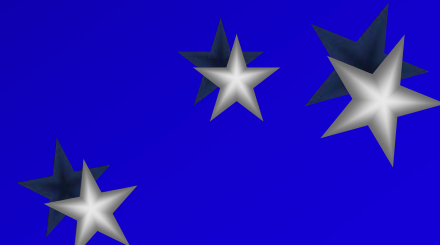
The Law has a large scope of application

➡ Article 1.

1. *This Law provides provisions on e-transactions in operations of State bodies, civil, business and other sectors as provided by the laws.*

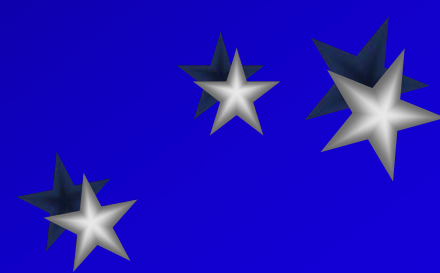
➡ Article 2. Scope of Application

- *This Law shall apply to bodies, organizations, individuals selecting to use E. transact*



Affect to society

- **ETL 2005 provides a strong legislative support to agencies, organizations and individuals to apply ICT in their activities,**
- **Speed up the realizing of : E. Commerce, E. Government, E. Learning,.....in the Country**
- **Affect to the ICT market**



Affect to society

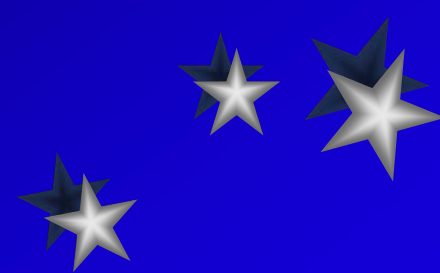
Base on this law ministries are going to draft the followings decrees :

- **E. Commerce**
- **E Transaction on the area of Finance : Tax online, E Customs, E Accounting,....**
- **E Transaction in banking : E Payement**
- **Digital Signature and CA**
- **E Transaction in State Agencies**

Several Seminars and meetings will be organized to discuss and address to the issues, how to attain the objectives of the law after the Law come into force



Thank for your attention





Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/009

Agenda Item: 7

An Art of Balance: e-Crime Investigation vs. Privacy Protection

Purpose: Information
Submitted by: Hong Kong



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

An Art of Balance - e-Crime Investigation vs. Privacy Protection

YU Yin-ching
Woman Chief Inspector of Police
Hong Kong Police Force



Agenda

- Related Privacy legislation in Hong Kong
- e-Crime Investigation
- The Need of Partnership
- Conclusions



Legislation

- Personal Data (Privacy) Ordinance, Cap 486 Laws of Hong Kong
- The Ordinance enacted since December 1996.



Objectives

- Protecting the privacy interests of living individuals in relation to personal data.
- Enabling free flow of personal data to Hong Kong from restrictions by countries that already have data protection laws.



Interpretations

“Personal data” means any data-

- (a) relating directly or indirectly to a living individual;
- (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained;
- (c) in a form in which access to or processing of the data is practicable;



Data Protection Principles

Principle 1 -- Purpose and manner of collection.

- This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.



Data Protection Principles

Principle 2 -- Accuracy and duration of retention.

- This provides that personal data should be accurate, up-to-date and kept no longer than necessary.



Data Protection Principles

Principle 3 -- Use of personal data.

- This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.



Data Protection Principles

Principle 4 -- Security of personal data.

- This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).



Data Protection Principles

Principle 5 -- Information to be generally available.

- This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.



Data Protection Principles

Principle 6 -- Access to personal data.

- This provides for data subjects to have rights of access to and correction of their personal data.



Exemption

Sec 58 Cap 486, Personal Data (Privacy Ordinance)

- (a) the prevention or detection of crime;
- (b) the apprehension, prosecution or detention of offenders;
- (c) taxation purposes;
- (d) the prevention, preclusion or remedying of unlawful or seriously improper conduct, or dishonesty or malpractice, by persons...etc.



e-Crime Investigation

- IP addresses
- Transaction Log
- Communication Log
- Account Subscriber Details
- Communication Content (e.g. email, ICQ...)



IP address / Domain name

- Open source information (Such as APNIC, ARIN, checkdomain.com...)
- DOS command (ping, netstat, tracert.....)
- Software (visual route, smartwhois....).



e-Crime Characteristics

- Absence of Physical Borders
- Time Critical
- Digital Evidence
- Multiple Stakeholders



Acquisition of Personal Data

- Exemption under Section 58 of the Personal Data (Privacy) Ordinance
- Search Warrant



Sharing of Personal Data

- Must be in compliance with the Personal Data (Privacy) Ordinance
- Sharing of “shared” Personal Data must be explicitly authorised by the original sharer or the data owner



Importance of Partners

- Local / Overseas Law Enforcement Agencies
- Industry (e.g. ISPs; Network Administrators)
- Privacy Regulators



An Art of Balance

- Identity Theft is one of biggest and Most Serious Crime over the Internet
- Enabling LEA to prevent and detect e-Crime actually help us to help you.



Our Vision

- To Ensure Hong Kong Remaining One of the Safest and Most Stable Societies in the World....and

This include the physical and cyber space



Thank You

Commercial Crime Bureau





Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/010

Agenda Item: 8

Strategies toward the Electronic Transaction Law implementation in the ICT

Purpose: Information
Submitted by: Viet Nam



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



STRATEGIES TOWARD THE ELECTRONIC TRANSACTION LAW IMPLEMENTATION IN THE ICT APPLICATIONS

DR. NGUYEN AI VIET
STANDING OFFICE
NATIONAL STEERING COMMITTEE FOR ICT
HANOI – February 2006



CONTENTS

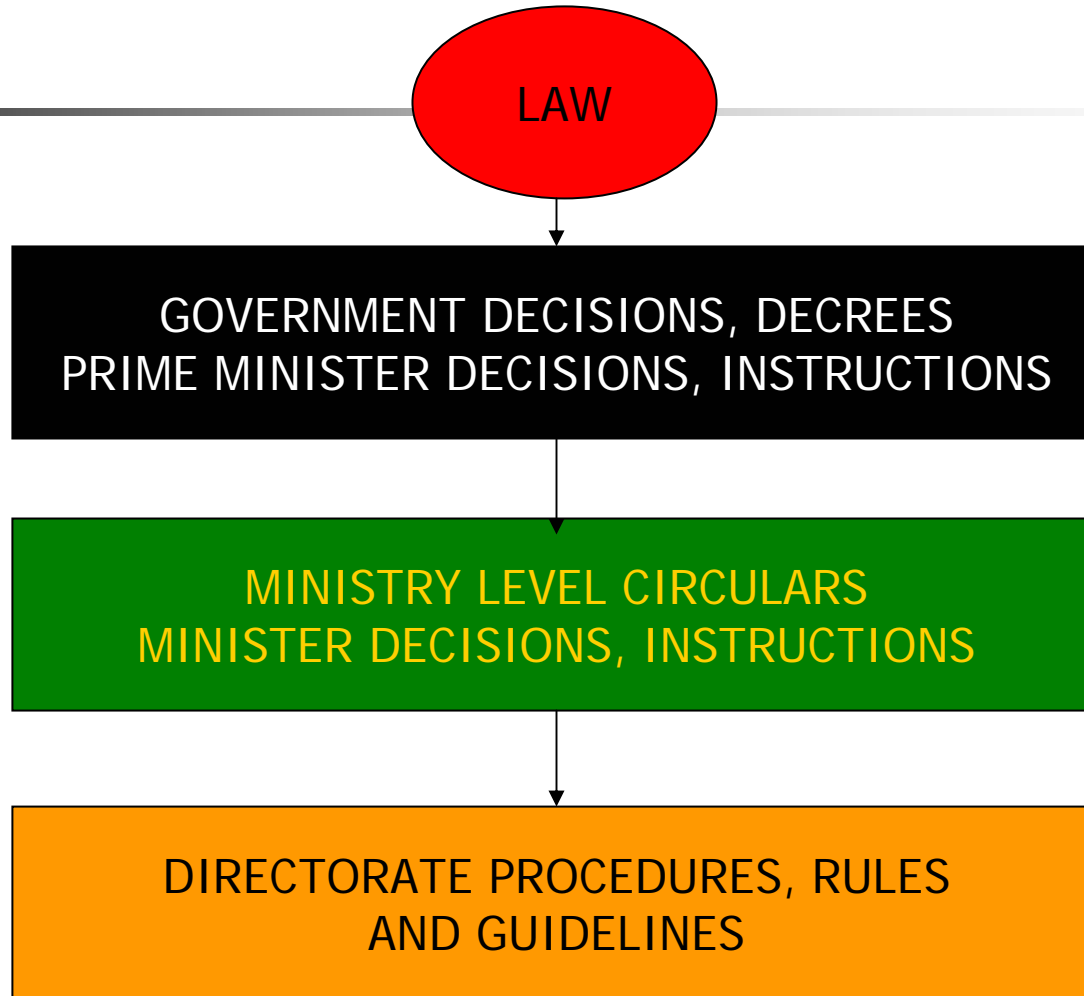
- THE LEGAL REGULATORY BACKGROUND
- STRATEGIES TOWARD THE SOLUTIONS
- THE PRACTICAL ISSUES RELATED TO THE INFORMATION PRIVACY IN THE ELECTRONIC ENVIRONMENT

THE LEGAL REGULATORY BACKGROUND



- The electronic transaction law (approved in November 2006)
- The first foundations for electronic information privacy.
- However, it focuses mainly on technical aspects.
- There is still a long way to practical implementation of the electronic information privacy.
- Information and Privacy Acts (???)

THE IMPLEMENTATION STEPS



STRATEGIES



- Solid legal foundations
- Consistency, especially in the overlapping areas.
- Priority order
- Under one law, there can be a lot of decrees. However, large number of decrees can cause inconsistencies.
- One decree can guideline different items in the Law.

THE CONTEXT TO BE GUIDELINED



- Digital key management and use in public agencies (24.3)
- Accepting the digital keys of foreign partners (27.2)
- The content of electronic certificate (29.9)
- Registration, operation and cross certification of CA service providers (30.4)
- Rights and duties of the CA service providers (31.2)
- Public Administration of the electronic signature certification service (32.2)

THE DECREE OF DIGITAL SIGNATURE

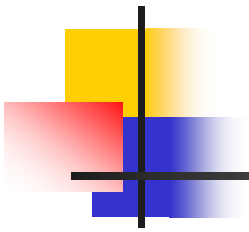
- 
- Objective: Guidelines for digital signature use and digital signature certification service.
 - MPT.



THE DECREES TO BE ISSUED

- Decree of guidelines for electronic transactions (Who will be in charge ?)
- Decree of guidelines for electronic contracts (Is it necessary at all ? The Ministry of Trade already drafted the Decree of E-commerce)
- Decrees of guidelines for crypt ions, for network security, cyber crimes, disputes,...

THE MINISTRY LEVEL REGULATIONS

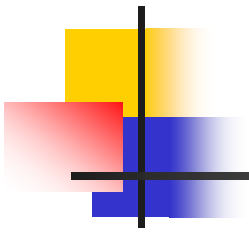
- 
- After the government decrees are issued, the ministry level circulars, regulations, decisions and instructions will be needed for further implementation of the law.
 - To guideline the decree of digital signatures, the details of the related regulations will be needed.



DIAP

- Directorate of IT Application Promotion represents MPT in IT Application Administration.
- It is in charge of CA service registration. The detailed guidelines will be issued.

FURTHER WAY TO THE PERSONAL INFORMATION PRIVACY

- 
-
- Necessary legal foundations
 - World wide trends: National security versus the information privacy protection
 - The information sharing, freedom versus the privacy.
 - The social awareness of privacy.



Necessary legal foundations

- There is still a long way from the electronic transaction law to the personal information privacy (even just in the cyber context).
- The Information Law, the Privacy Law, the Information Privacy Act must be in place.
- In practice, the branches exist before the frames. The trial-error process would take very long time.



National security versus the information privacy protection

- This is quite a newly emerging issue in the developed countries.
- Discouraging influence for the nations on the way to the information privacy.
- Revival of the old belief: the privacy must give priority to the national security.
- Experience in the US and recent participation of the American IT companies in the information censorship in China.



The information sharing, freedom versus the privacy.

- In the different cultures, the information privacy can have different meaning.
- Under the same slogan, the objective can be misunderstood.
- Information sharing and freedom is the most basic element of the E-government toward an information society can be distorted and abused against the information privacy.



The social awareness of privacy

- The privacy is a new concept to the oriental traditions (For instance, the Chinese post man found it quite natural to give away the business information).
- Information is not valued in normal people perception



CONCLUSIONS

- The personal information privacy is a benefit of an advanced society not a merely imposed will.
- There are some cultural barriers to that in oriental societies.
- A lot of practical activities must be done to progress toward the personal information privacy. In Vietnam, IT is also a pioneering area.
- Actions will bring foundations for the conceptual establishments.



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/011

Agenda Item: 9

Legal & Regulatory Environment for Protecting Individuals

Purpose: Information
Submitted by: Hunton & Williams LLP



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



Legal & Regulatory Environment for Protecting Individuals

Martin Abrams

Center for Information Policy Leadership

Mabrams@hunton.com

www.informationpolicycenter.com

The Problem

- ◆ Modern business and governmental processes are driven by data
- ◆ Data about people can both drive economic value, but may also be used to harm individuals
- ◆ The harm isn't always easy to measure
 - Inhibiting participation may be a harm



Three Traditional Theories of Privacy

- ◆ Right to be left alone
- ◆ The ability to control others' knowledge of me
- ◆ An environment where I am free of information caused harm
- ◆ The common denominator is protecting individuals from the inappropriate use of information (harm broadly defined)



A Privacy Regulatory Environment Should

- ◆ Create a environment where information may be confidently used to create value for society and the individual
- ◆ While protecting the individual from harm
- ◆ And protecting society from the effects of individuals not participating



How Does APEC Help?



**Information
Fed
E-Commerce**



Apec Privacy Framework



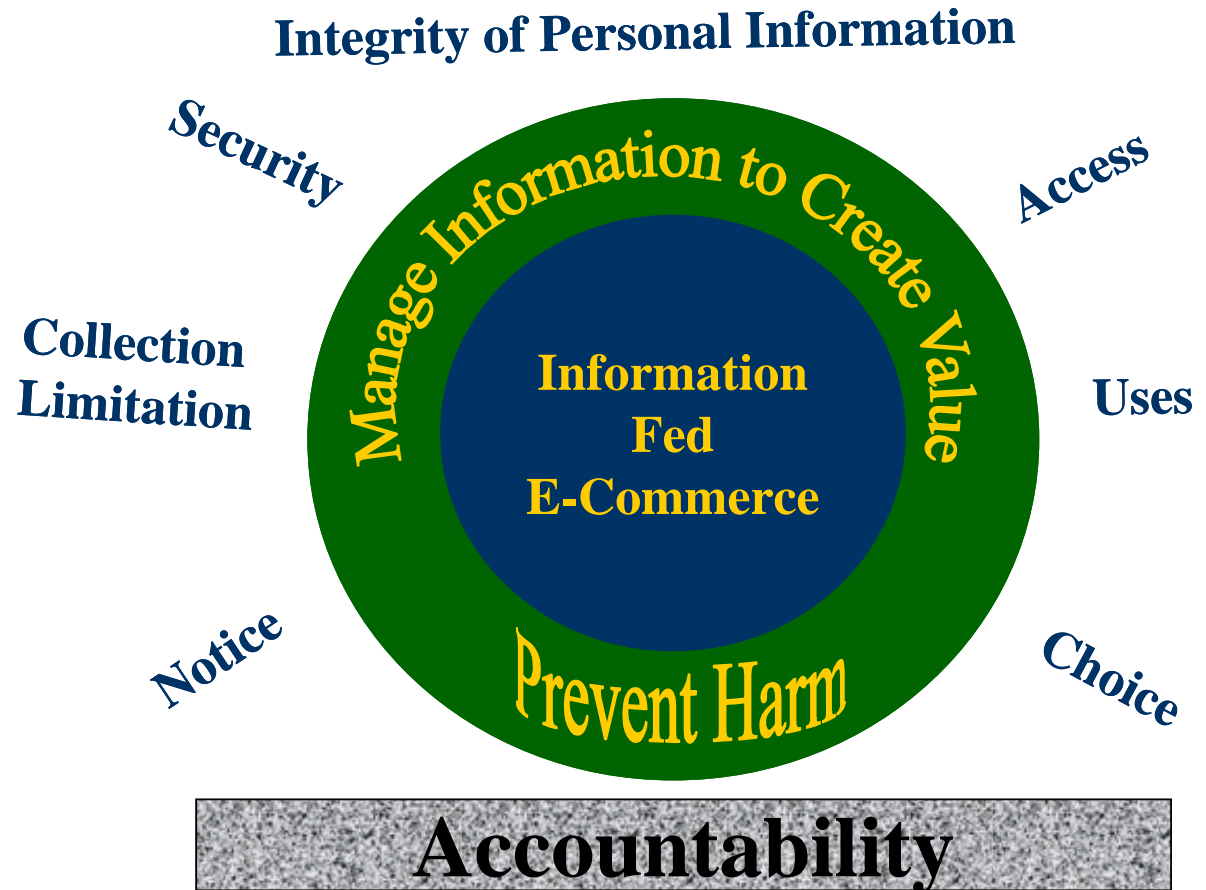
Principles Give Us Discipline



Integrity of Personal Information



Accountability Assures Protection



Linkage to Traditional Data Protection

- ◆ Focused on individual control
 - Principles defined process to assure control
- ◆ Purpose of control is protection
- ◆ APEC Framework and Data Protection have common objectives and values



Concepts to Guide New Laws

- ◆ Place the priority on preventing harm broadly defined while creating consistent goals for data users
- ◆ Define principles that assist organizations and enforcers in implementing law's objectives
- ◆ Require Accountability
- ◆ Recognize global nature of data flows
 - Create a means for transfer that is flexible but protects individuals



New Laws Should Contain

- ◆ Preamble that defines purpose
- ◆ Focus attention on preventing harm
- ◆ Discipline from key principles
 - Transparency (notice & appropriate access)
 - Defines purpose and collection limitations
 - Access where appropriate
 - Security safeguards
 - Choice appropriate to the data and use
 - Accuracy appropriate to the use
 - Redress
- ◆ Accountability



Globalization

- ◆ Must be based on accountability – obligations travel with the data
- ◆ Culturally neutral
 - Avoid concepts of equivalent law
- ◆ Create means for cooperation





Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/012

Agenda Item: 9

A Business Guide: Meeting Your Legal and Business Obligations to Safeguard Personal Information

Purpose: Information
Submitted by: Hunton & Williams LLP



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

THE CENTER
FOR INFORMATION
POLICY LEADERSHIP
HUNTON & WILLIAMS LLP

**A BUSINESS GUIDE:
MEETING YOUR LEGAL AND BUSINESS OBLIGATIONS
TO SAFEGUARD PERSONAL INFORMATION**

by
Ellen Finn

February 2006

The Center for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. The Center is a member-driven organization that operates within the Privacy and Information Management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Center provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal interests. Visit us at www.informationpolicycenter.com.

Introduction

Identity fraud and financial account fraud are not new and many of the tried and true methods for committing these crimes are decidedly low-tech; dumpster-diving and stealing mail have long been the primary methods by which criminals gain access to individual's sensitive personal information. But the methods used by criminals to gain access to the personal information that makes these crimes possible are changing with our times. Increasingly, criminals are turning to more technologically sophisticated methods of gathering and exploiting personal information along with their traditional tricks of the trade.

Willie Sutton is frequently quoted as saying that he robbed banks, "because that's where the money is."¹ Today, criminals are discovering that personal data can be as good as money and they are increasingly targeting businesses to get it. Why? Because that's where the data is collected. Criminals are also increasingly using technology to gather and use personal information. For example, law enforcement officials have begun to see local drug dealers, who used to rely on street addicts to supply them with credit cards, checks, or account statements stolen from mailboxes and dumpsters, now engaging in complex joint ventures with organized crime rings around the world by using the Internet to communicate, buy and sell personal data, and transfer money.² In addition, "phishing" schemes that use deceptive email messages to trick individuals into disclosing credit card numbers, Social Security numbers, passwords, and other information, are an increasingly common way of obtaining information for fraudulent purposes.³

Businesses that collect, use, and store individuals' personal information need to be aware of these threats — both old and new — and take steps to protect the security of individuals' information. First and foremost, it is the right thing to do as a matter of human decency and respect, as well as being a good business practice. But, in addition, and, perhaps surprisingly given the variety of laws have been proposed recently to address information security

¹ Ironically, it appears that Sutton did not utter this famous line, although he later appropriated it for the title of his autobiography, "Where the Money Was: The Memoirs of a Bank Robber." See reporter Steve Cocheo's March 1997 article, "The bank robber, THE QUOTE, and the final irony," in the ABA's Banking Journal, available at http://www.banking.com/aba/profile_0397.htm.

² See, for example, USA Today articles, "Meth addicts use Internet to cash in on identity theft" and "Meth addicts' other habit: Online theft" both by Byron Acohido and Jon Swartz, published on December 24, 2005; and the Seattle Post-Intelligencer article "Many meth users turn to identity theft" by Greg Risling, published on December 28, 2005.

³ "Phishing" messages typically purport to be from legitimate businesses with which large numbers of consumers may have accounts. They generally tell the consumer that there is some kind of problem with their account and provide a link to a website where the consumer is requested to sign in and provide various personal details. These websites look legitimate, but they are set up by criminals to gather user names, passwords, and other information that is then used to defraud consumers. Statistics on the increasing number of unique phishing attacks are available from the Anti-Phishing Working Group at <http://www.antiphishing.org/index.html>.

and identity theft,⁴ the safeguarding of personal information is already required by law of companies doing business in the United States.

Legal Requirements to Protect Personal Information

Legal requirements to protect individuals' personal information have existed for some years now for companies in particular industries. Financial institutions⁵ have been subject to the Gramm-Leach-Bliley Act⁶ and its implementing regulations, which require them to protect the privacy and security of their customers' nonpublic personal information.⁷ In particular, financial institutions must implement a comprehensive information security program that includes administrative, technical, and physical safeguards designed to:

- ensure the security and confidentiality of customer information;
- protect against any anticipated threats or hazards to the security or integrity of the information; and
- protect against unauthorized access to or use of the information that could result in substantial harm or inconvenience to the customer.

The security program must contain safeguards that are appropriate to the institution's size and complexity, the nature and scope of the institution's activities, and the sensitivity of the customer information at issue.⁸

Similarly, companies in the health care industry have had to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")⁹ and its implementing Security

⁴ Proposed identity theft legislation includes the Identity Theft Protection Act, S. 1408 (Smith); Comprehensive Identity Theft Prevention Act, S. 768 (Schumer); and the Personal Data Privacy and Security Act of 2005, S. 1789 (Specter). Proposals to limit the use and display of Social Security numbers include the Social Security Number Protection Act, HR. 1078 (Markey); and the Social Security Number Privacy and Identity Theft Prevention Act, HR. 1745 (Shaw). Proposals targeted at the regulation of data brokers include the Consumer Data Security and Notification Act, HR. 3140 (Bean); and the Information Protection and Security Act, S. 500 (Nelson).

⁵ The term "financial institution" is extremely broadly defined, and includes companies that are "significantly engaged" in any of a variety of specified "financial activities" such as transferring money, extending credit, or providing certain financial data processing and transmission services. 16 C.F.R. § 313.3(k)(1) (2005).

⁶ 15 U.S.C. §§ 6801-6827 (2004).

⁷ "Nonpublic personal information" is defined as personally identifiable information (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution in connection with its provision of a financial product or service. It does not include most publicly available information. 15 U.S.C. § 6809 (2005).

⁸ 16 C.F.R. § 314.3(a) (2005).

⁹ Pub. L. No. 104-191, 110 Stat. 1936 (1996).

Rule.¹⁰ Covered entities¹¹ are required to ensure the confidentiality, integrity, and availability of all electronic protected health information that they create, receive, maintain, or transmit. Pursuant to the Security Rule, each covered entity must:

- conduct a risk assessment of potential threats to the confidentiality of protected health information and implement a risk management program to reduce the identified risks to a reasonable and appropriate level;
- have in place specified administrative, physical, and technical safeguards to protect information and adopt written policies and procedures regarding how these safeguards will be implemented; and
- enter into “business associate agreements” with unrelated persons or entities that contractually obligate them to abide by the legal standards in the Security Rule.

In addition, companies with privacy policies — which have generally been online companies or the online operations of offline companies — have faced liability for deceptive trade practices under Section 5 of the Federal Trade Commission Act¹² when statements in their privacy policies, including statements about the confidentiality and security of consumers’ personal information, were false or misleading. Since 2002, the Federal Trade Commission has brought five cases against companies for deceptive security claims.¹³ State Attorneys General have also enforced their mini-FTC acts in privacy and security cases where companies did not live up to their promises.¹⁴

But, until this past year, the vast majority of companies — those outside the financial services and health care industries and without published privacy policies — believed that they were not subject to a legal requirement that they safeguard individuals’ personal information. Then, in June 2005, the FTC announced a settlement agreement with BJ’s Wholesale Club resolving charges that BJ’s failure to implement appropriate security measures to protect

¹⁰ 45 C.F.R. §§ 160, 162, 164 (2004).

¹¹ The Health Insurance Portability and Accountability Act applies to health plans, health care clearinghouses or health care providers that transmit health information in electronic form in connection with certain specified transactions.

¹² 15 U.S.C. § 45(a) (2005).

¹³ The five FTC cases are: Petco Animal Supplies, Inc. (Docket No. C-4133); MTS Inc., doing business as Tower Records, Tower Books, or Tower Video (Docket No. C-4110); Guess?, Inc. (Docket No. C-4091); Microsoft Corp. (Docket No. C-4069); and Eli Lilly (Docket No. C-4047). Complaints, consent agreements, and additional related information are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

¹⁴ Companies signing settlement agreements with individual states regarding information compromises have included the ACLU (http://www.oag.state.ny.us/press/2003/jan/ jan14a_03.html); Barnes and Noble (http://www.oag.state.ny.us/press/2004/apr/ apr29a_04.html); Eli Lilly (<http://caag.state.ca.us/newsalerts/2002/02-084.htm> and <http://www.epic.org/privacy/medical/lillyagreement.pdf>); Victoria’s Secret (http://www.oag.state.ny.us/press/2003/oct/oct21b_03.html); and Ziff Davis Media (http://www.oag.state.ny.us/press/2002/aug/aug28a_02.html).

the sensitive information of thousands of its customers was an unfair practice that violated federal law.¹⁵

Specifically, the FTC charged that BJ's failed to encrypt consumer information when it was transmitted or stored on computers in BJ's stores; created unnecessary risks to the information by storing it for up to thirty days, in violation of bank security rules, even when it no longer needed the information; stored the information in files that could be accessed using commonly known default user IDs and passwords; failed to use readily available security measures to prevent unauthorized wireless connections to its networks; and failed to use measures sufficient to detect unauthorized access to the networks or to conduct security investigations. Millions of dollars worth of fraudulent purchases were made using counterfeit copies of credit and debit cards used at BJ's stores, causing banks to cancel and re-issue thousands of credit and debit cards and causing consumers inconvenience, worry, and time loss dealing with the affected cards. The FTC alleged that BJ's failure to secure customers' sensitive information was an unfair practice because it caused substantial injury that was not reasonably avoidable by consumers and not outweighed by offsetting benefits to consumers or competition. The settlement required BJ's to establish and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards and requires BJ's to obtain audits from a qualified, independent, third-party professional every two years for the next twenty years, certifying that BJ's security program meets the standards of the order.

The BJ's case was not a fluke. On December 1, 2005, the FTC announced that DSW Inc., an Ohio-based footwear retailer, had agreed to a nearly identical settlement of similar FTC allegations that it engaged in "unfair" business practices by failing to properly secure customer data.¹⁶ The FTC's requirements in these cases, as well as the earlier deception cases based on security promises to consumers, closely resemble the requirements imposed on financial institutions by the Commission's Safeguards Rule. The result is, in essence, a de facto requirement that any business that collects, uses, or maintains consumers' sensitive personal information implement a safeguards program.

The practical significance of the FTC's enforcement actions would not be nearly as great, however, in the absence of the security breach notification laws enacted first by California and now by 22 other states.¹⁷ In the absence of these breach notification laws, companies that suffered an information compromise could generally keep the incident quiet and, as a result, were unlikely to face an investigation from the FTC or State Attorneys General. Consumers were generally not notified of breaches and therefore companies were unlikely to face class action lawsuits. In the absence of consumer notice, security incidents rarely hit

¹⁵ Case materials for BJ's Wholesale Club, Inc. (FTC Docket No. C-4148) are available at <http://www.ftc.gov/os/caselist/0423160/0423160.htm>.

¹⁶ See <http://www.ftc.gov/os/caselist/0523096/0523096.htm>.

¹⁷ The states and related laws include: Arkansas (SB 1167); California (SB 1386); Connecticut (SB 650); Delaware (HB 116); Florida (HB 481); Georgia (SB 230); Illinois (HB 1633); Indiana (SB 503); Louisiana (SB 205); Maine (LD 1671); Minnesota (HF 2121); Montana (HB 732); Nevada (SB 347); New Jersey (AB 4001); New York (AB 4254); North Carolina (SB 1048); North Dakota (SB 2251); Ohio (HB 104); Pennsylvania (SB 712); Rhode Island (HB 6191); Tennessee (HB 2170); Texas (SB 122); and Washington (SB 6043).

the press, so there was little damage inflicted to a company's reputation or stock price.¹⁸ By contrast, consumer notification laws now all but guarantee private class action lawsuits, bad publicity that damages company brands and reputation, FTC and State Attorney General investigations, and a drop in stock price. In severe cases, the breach may raise questions under Sarbanes-Oxley with respect to a company's internal controls. Because notification laws create such significant costs for companies that suffer a data breach, they provide a powerful incentive to safeguard data in the first instance.

So what exactly is it that you are required to do?

Safeguards

Every business should develop a written information security plan that describes its program to protect individuals' personal information. The plan should be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it handles. While there are a handful of basic elements listed below that every safeguards plan should address, businesses have the flexibility to implement policies, procedures, and technologies that are appropriate to their unique circumstances.

1. Designate one or more employees to coordinate your safeguards program.

Whether you decide to task a single employee with coordinating safeguards or you spread the responsibility among a team of employees, someone in your organization needs to be accountable for information security. In deciding who it should be, you should recognize that information security is fundamentally a management issue, not a technology issue. While information technology can play a significant role in protecting data, effective information security requires a broader focus and should include physical security, employee training and management, and business processes. Even with respect to information technology, the focus should be on managing your technology, not the technology itself. Buying a firewall, for example, does little to improve your security unless you configure and monitor it properly.

In addition, your safeguards program will almost certainly require the coordination of legal, human resources, information technology, audit, and business functions. The person or team that you choose to coordinate your program should have the ability to communicate and work effectively with all of these different groups.

2. Identify and assess the risks to individuals' personal information in each relevant area of your company's operations, and evaluate the effectiveness of your current safeguards for controlling these risks.

To conduct a risk assessment, you will need to understand what you are protecting and what you are protecting it from. In particular, in this context, you should focus on protecting individuals' personal information in addition to your company's business information and operations. To begin, therefore, you should identify what personal information you are actu-

¹⁸ The exceptions generally are cases where a "security researcher" publicized an incident claiming that going to the press was an attempt to fix the problem after efforts to contact the company directly had failed.

ally collecting, how your company uses it, where it is stored, to whom it is disclosed, who has access to it for what purposes, and how it will ultimately be disposed. You should map these data flows and classify data by sensitivity so you can prioritize your security measures.

Next, you need to think about all the ways that this personal information could be compromised. While you obviously need to consider intrusions by computer hackers, you should also think about ways that employees, service providers, business partners, or vendors could compromise the security of your personal information either intentionally or through carelessness. You should think about risks beyond those associated with information technology and consider business processes as well. It is a good idea to have the risk assessment process conducted by a team that includes both technical and business personnel because their perspectives on the likelihood and impact of threats may differ.

Once you have identified the risks you face, you will need to conduct a gap analysis to see where your current safeguards are inadequate. Where current safeguards are inadequate to address the risks you have identified, you will need to analyze your options. You should consider the likelihood a given risk will occur and the severity of the consequences if it does. You should also consider the effectiveness of the various available security measures and their cost relative to the harm caused by a compromise.

When thinking about the costs of a compromise you should consider the full range of potential costs you could face: the cost of investigating a security breach; mitigating and remediating damage to your systems and securing the systems after the breach; lost sales or productivity caused by the unavailability of systems or data; notifying affected individuals and government agencies, as appropriate; responding to regulator inquiries and enforcement actions; legal fees and costs for the defense of private lawsuits; lost customers; reputational damage; and a possible drop in stock price. The harm caused by a compromise, however, should be defined more broadly than just the resulting financial costs. Traditional risk assessment has systematically undervalued the protection of individuals' personal information because it has focused on the costs of compromise to the company rather than including costs to individuals. Moreover, it has focused only on financial costs rather than including less quantifiable harms such as anxiety, intrusion, individual reputation, and privacy. Despite the difficulty in quantifying these broader harms, they should be included in your analysis of the cost of available security measures relative to the harm caused by a compromise. Your calculation of the cost of a particular security measure should include not only the cost of any technology, but also the human resources and training needed to configure and monitor the technology properly.

3. Design and implement a safeguards program, and regularly monitor and test it.

In designing your safeguards program, you should consider all areas of your operations. In particular, you should be sure to address employee management and training; information systems; and managing system failures, which includes prevention, detection and response to attacks, intrusions, or other system failures. Believe it or not, despite the scope of issues that your program should address, designing a safeguards program may actually be the easier part of this process; implementing the program is often the harder part.

Your goal is to be sure that your security policies and procedures are more than mere paper and that they are actually followed in the day-to-day operation of your business. You also

want to be sure that any technology you deploy is properly configured and maintained and that any reports or alerts it provides are regularly reviewed and investigated. How can you tell whether these things are happening? By monitoring and testing each of the elements of your program. Your testing should reveal whether your safeguards program is being followed consistently and whether it is operating effectively to manage the risks to personal information that it was designed to address.

4. Select appropriate service providers and contract with them to implement safeguards.

When service providers or other third parties have access to your data or information systems, you should take steps to determine whether they can be trusted not to compromise your information security and to ensure that they are contractually required to meet your safeguards standards. Although the FTC's Safeguards Rule explicitly addresses only service providers, you should consider whether contractual provisions regarding safeguards are warranted in other relationships, for example, with vendors, business partners, or customers whose activities may affect your information security.

Your due diligence on service providers and other third parties should include some or all of the following measures: reviewing an independent audit of the third party's operations; obtaining information about the third party from several references or other reliable sources; requiring that the third party be certified by a recognized trade association or similar authority; reviewing and evaluating the service provider's information security policies or procedures; or taking other appropriate measures to determine the competency and integrity of the party.

Your contracts with third parties should specifically address safeguards obligations; a general confidentiality provision is really not sufficient. You should also require third parties to notify you of significant security incidents (so you can determine whether you have any legal obligations to provide notice to individuals of a possible data compromise) and to cooperate in responding to security incidents and investigating data breaches. In addition, you may want to ask for the right to audit a third party's safeguards program for compliance with legal and contractual requirements.

5. Evaluate and adjust your safeguards program in light of relevant circumstances, including changes in your business arrangements or operations, or the results of testing and monitoring.

Security is an ongoing process, not a static condition. You will need to evaluate and adjust your safeguards program at regular intervals and make appropriate changes in light of the results of your testing and monitoring. In addition, you need to consider whether changes to your safeguards program are needed in connection with changes in technology, business practice, and personnel. You should also keep up to date on new or emerging threats to information security and changes in the legal and regulatory environment. If you have an institutionalized change management process, it should include a security and risk management component.

* * *

We live in a world of unprecedented dependence on information and technology. The networked nature of our information systems means that we also live in a world of unprecedented dependence on the actions of others to ensure our own security. Safeguarding individuals' personal information is an important part of our collective responsibility to secure and sustain the viability of our information economy and our technological infrastructure. Compliance with legal requirements regarding the safeguarding of individuals' personal data should be understood within this broader context.

© 2006 The Center for Information Policy Leadership at Hunton & Williams LLP. The content of this paper is strictly the view of the Center for Information Policy Leadership and does not represent the opinion of either its individual members or Hunton & Williams LLP. The Center does not provide legal advice. These materials have been prepared for informational purposes only and are not legal advice, nor is this information intended to create an attorney-client or similar relationship. Whether you need legal services and which lawyer you select are important decisions that should not be based solely upon these materials. Please do not send us confidential information. Contact: Martin E. Abrams, Executive Director, The Center for Information Policy Leadership, 1900 K Street, NW, Washington, DC 20006-1109, (202) 955-1627, mabrams@hunton.com.



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/013

Agenda Item: 10

Personal Information Protection in Korea

Purpose: Information

Submitted by: Korea



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Personal Information Protection in Korea

With Reference to Korea Integrated Criminal Justice System(KICS)



Seong-Jin Choi

Director of KICS/Prosecutor

Contents



Overview of KICS initiative



Legal regime of P.I.P. in Korea



P.I.P. framework of KICS



Guidelines of P.I.P. in KICS

P.I.P. in Korea

. Overview of KICS initiatives 1. Backgrounds and Vision

Backgrounds

Request for Effectiveness

- Increasing use of IT but
- there are redundant data entries, difficulties in information sharing within & between government agencies

Request for Fairness

- Demands for fairness and transparency in criminal justice services
- Increase in citizens' participation through the internet

Paradigm Shift of Public Service

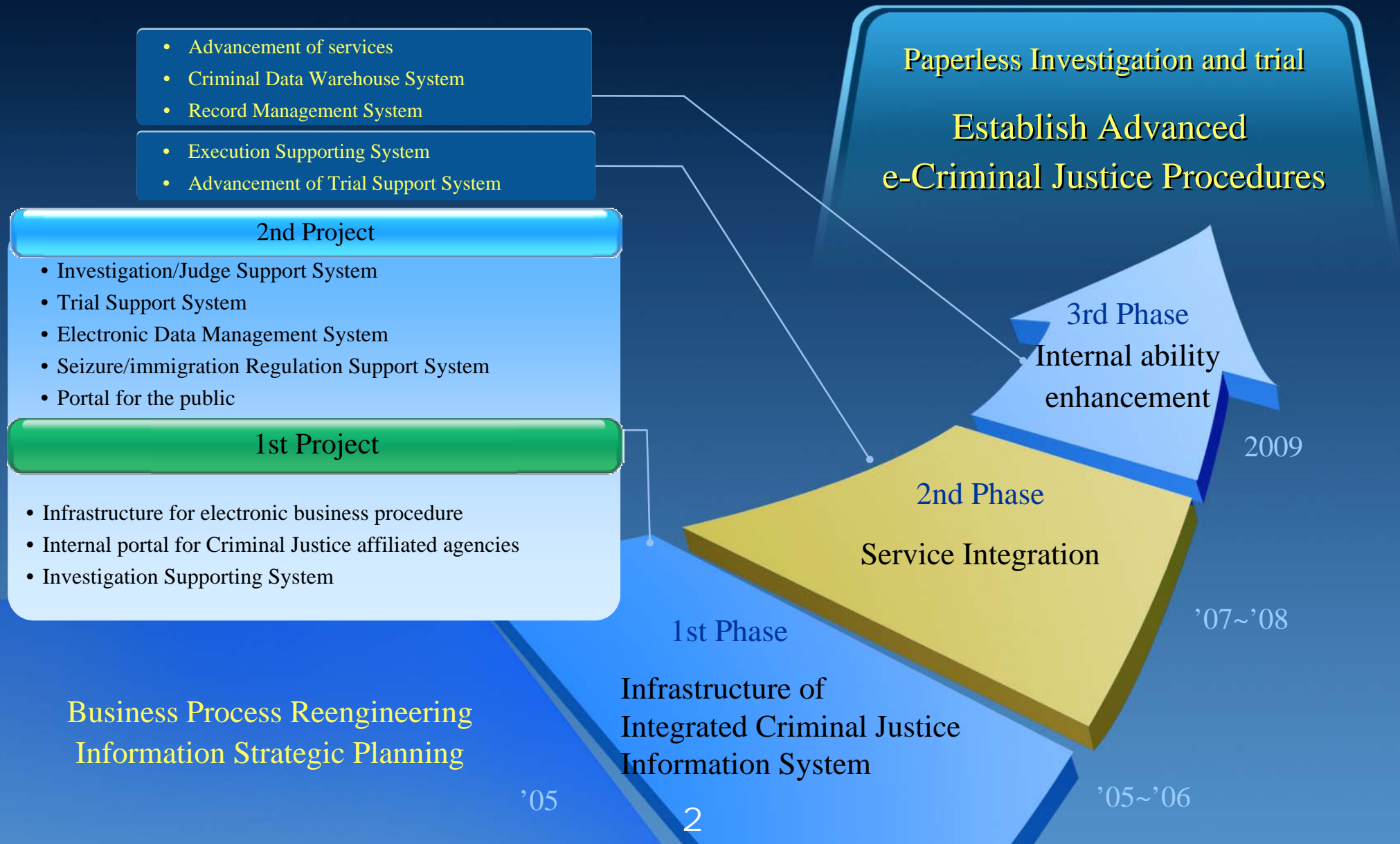
- From government-centered to citizen- centered
- Citizen as client

Vision
Implementation of
efficient and fair E-Justice System



P.I.P. in Korea

. Overview of KICS initiatives 2. Roadmap



P.I.P. in Korea

*. Overview of KICS initiatives
3. Why P.I.P is so important?*

■ The Public's Anxiety over Big Brother

- ❑ Centralization of Criminal Justice Information
- ❑ Public belief on digitization of information

■ Major incidents about P.I.P in Korea

- ❑ Electronic Personal Identification Card(2005)
- ❑ NEIS(National Education Information System)(2003)

■ President's concerns of privacy protection in KICS

- The most important things while developing the KICS is protecting the infringement of the human rights.

P.I.P. in Korea

. Legal Regime of P.I.P. in Korea

Protection Model	Jurisdiction	Rules & Regulations
Comprehensive Laws	Public Sector	• Act on the Protection of Personal Information Maintained by Public Agency
	Private Sector	• The Act on Promotion of Information and Communication Network Utilization and Data Protection
Sectoral Laws	Public & Private Sector	<ul style="list-style-type: none"> • Protection of Communications Secrets Act • Telecommunication Business Act • Medical Service Act • Use and Protection of Credit Information Act • Framework Act on Electronic Commerce • Digital Signature Act
Self-Regulation	Private Sector	• The Guidelines on the Private Information Protection

“Private information” means the information concerning a living person including the full name and resident registration number, etc., by which the individual concerned can be identified (including information by which the individual concerned cannot be identified but can be identified by simple combination with other information)

P.I.P. in Korea

. P.I.P. framework of KICS 1. Legal Compliance

Act on the Protection of Personal Information Maintained by Public Agencies

- Limitation on collecting information
- Relations to other guidance and regulations
- Obligation of data user
- R&R of head of criminal justice information sharing public agency
- Limitation on using and sharing information etc.

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

- R&R of personal information controller
- Definitions
- Limitation on collecting information
- Right of the user and personal information subject etc.

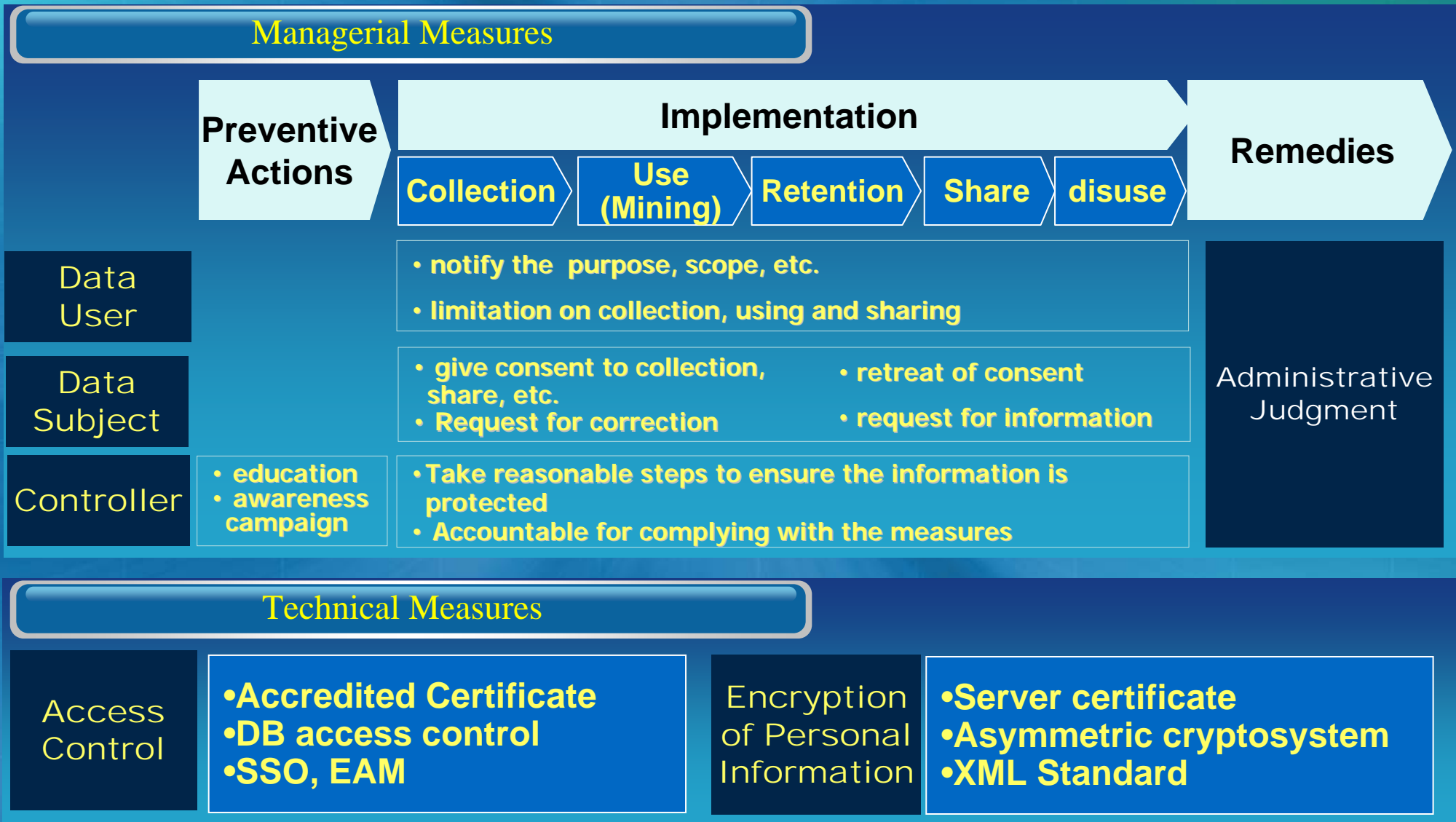
The Guidelines on the Private Information Protection

- Access Control of DB and data users
- Intrusion Protection System(IPS) and Intrusion Detection System (IDS)

Exemption : Recorded private information files on matters pertaining to the investigation of crimes, introduction and maintenance of prosecution, the execution of a sentence, handling of a rectification, handling of public security, or immigration control

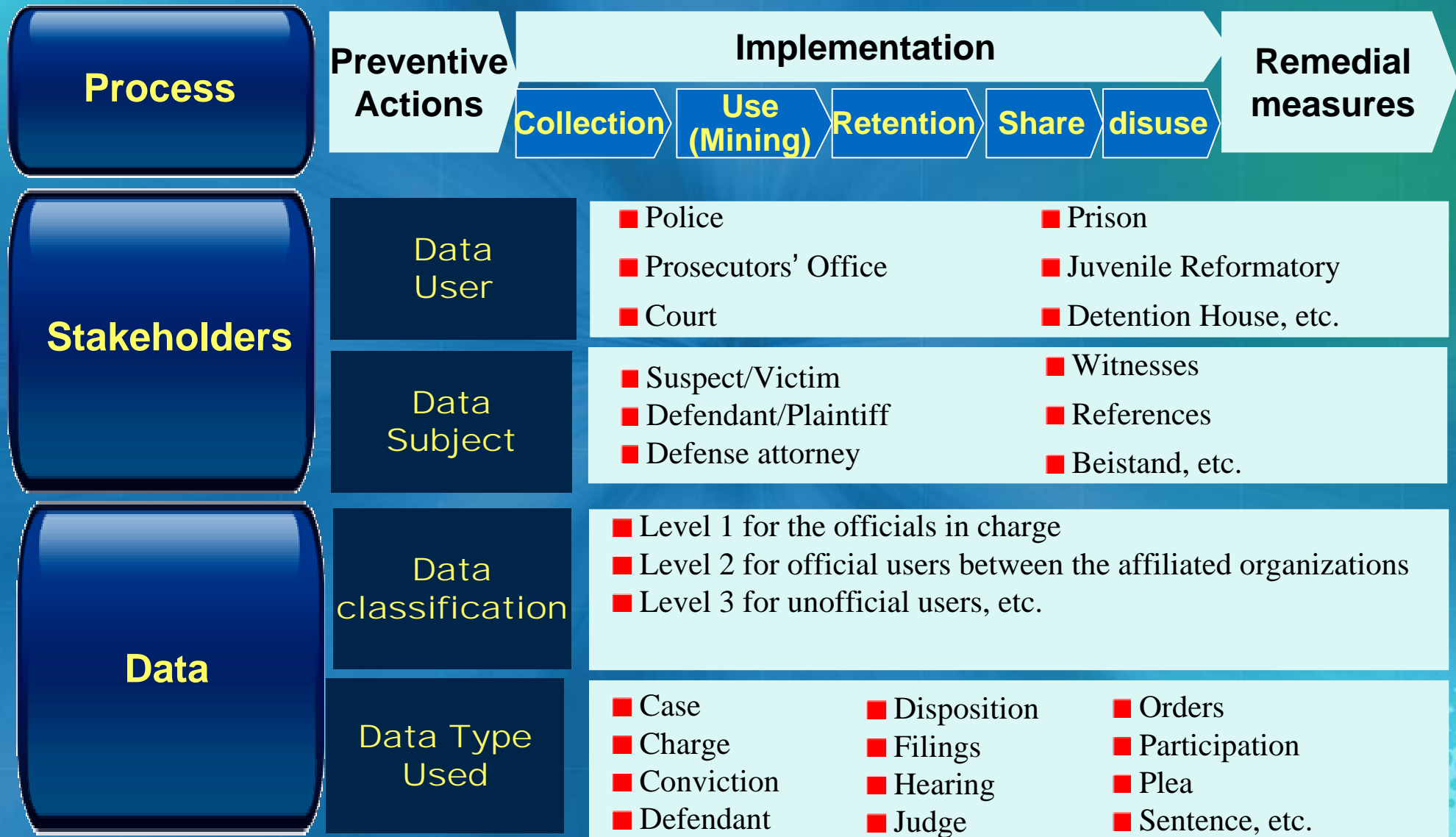
P.I.P. in Korea

. P.I.P. framework of KICS 2. Concept of the Framework



P.I.P. in Korea

Guideline of P.I.P. in KICS
1. Key Features(draft)



■ Things to be done to institutionalize the guideline

- ☐ The guidelines is still rough draft
- ☐ Coordination is needed within the 4 agencies
- ☐ Which agency is in charge of institutionalizing the guideline
- ☐ Which agency will manage(install, maintain) the information assets(the data)

■ Human Resources(staffing)

- ☐ Personal Information Controller
- ☐ Personal information protection roles should be integrated to the those of Information Security Manager
- ☐ More workload to the practitioner

■ Performance vs. level of security

- DRM(Data Right Management) solution is too heavy and it declines computer/network performance(speed)
- Internet issuance of certificate(ex copy of written judgment) can be hacked

■ Protection vs. Convenience

- ID/Password is convenient but weak in security
- Accredited Certificate vice versa



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/014

Agenda Item: 11

Information Privacy Protection – The Role of Technology

Purpose: Information
Submitted by: Microsoft



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Information Privacy Protection

The Role of Technology

*Meng-Chow Kang, CISSP, CISA
Chief Security & Privacy Advisor
Asia Pacific Region, Microsoft*

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
February 20-22, 2006
Horison Hotel, Hanoi, Vietnam

Microsoft
Trustworthy Computing

Privacy Invading Technology

- There are often legitimate needs for identifying, tracking, and monitoring capabilities, e.g., safety, security audit, automation, management, which can be misused or abused
- PIT is becoming pervasive
 - Exploiting technology capability
 - "Knowledge is Power"
 - Financial opportunities
 - Exploiting vulnerabilities
 - Financial gains
 - Business/individuals laxes
 - Ignorance or over-enthusiasm (CRM, safety/security concerns)
 - Simply bad practices
- Many forms of PIT
 - User devices (installed software, active contents, browser extensions, toolbars)
 - On the Internet (Internet gateways, email servers, proxies, web sites)

- Some recent cases:

DoubleClick **Click**

- Tracked behavior across sites
- Stored personal information and sold it to various third parties

real

- RealJukebox unique identifier
- Info on every track ripped or played was returned to RealNetworks along with the ID

a Alexa

- Toolbar purports to enhance searching and purchasing experiences
- Tracks sites, full URLs, IP addresses, emails, search results, products explored



Re@dNotify



Welcome to ReadNotify.com !

ReadNotify lets you know when email
you've sent gets read

Length of Reading

Find out how long they read your email for

[Start here!](#) New: [Get the optional Plugin](#)

Member Sign-in

email:

password:

Sign-in

Sign up now - Free!

Your existing email address:

GO!

home

about Re@dNotify

business solutions

member utilities

About ReadNotify.com

What is ReadNotify?

ReadNotify is the most powerful and reliable email tracking service that exists today. In short - ReadNotify tells you when email you sent gets read / re-opened / forwarded and so much more!

How does ReadNotify work?

Sending tracked emails via ReadNotify is incredibly easy: simply add **.readnotify.com** to the end of your recipients email address (they won't see this) - or install one of our [Active Tracker plug-ins](#) to add the tracking for you. The email is then directed to pass through our server, where we assign it a tracking code, "strip off" the .readnotify.com part and send it on to your recipient. When your recipient opens the email, the assigned tracking code sends our server a message, which allows us to report the details to you.

ReadNotify.com does not use any kind of spyware, nor do we install anything onto your recipients computer in order to track emails.

Can you read my emails?

No. We do not cache or copy the body of your emails. The only time that emails are stored on our server is to enable our 'ensured' or 'self-destructing' features. (Although once an ensured or self-destructing email expires, no record of it is retained by us)

Is my email address safe with you - will I get spammed?

Your email address is completely safe with us - we never send, allow or support 'spam' or unsolicited email of any kind - nor do we publish anything on lists.

How can I contact you?

If you cannot find answers to your queries in our FAQ's, please email the appropriate department:

- accounts@readnotify.com - for anything relating to accounts and payments
- pr@readnotify.com - for affiliate, reseller or publicity-related assistance

Deceptive Software - Spyware

	<u>Function</u>	<u>Description</u>	<u>Examples</u>
None	Innocuous	• No potential harm	+ Notepad
Potential for harm	Advertising	<i>Spyware and other Potentially Unwanted Software: Programs that perform certain functions without appropriate user consent and control</i>	
	Data Collection		
	Configuration Changes		
	Monitoring		
	Dialing		
	Remote Resource Use		
Extreme	Malicious Activity	• Clearly malicious (virus, worm, trojan)	— Sasser

Strider HoneyMonkey (MSR)

- Exploit Data Analysis – Suspicious List (May~June 2005)
 - Gathered 16,190 suspicious URLs through Web search and exploit neighborhood crawling
 - Identified 288 of them as exploit URLs → 1.28%
 - Expanded into 752 exploit URLs after auto-visit URL analysis → 263% expansion

	# Exploit URLs	# Exploit Sites
Total	752	288
WinXP SP1-UP	688	268
WinXP SP2-UP	204	115
WinXP SP2-PP	17	10
WinXP SP2-FP	0	0

Evolving Landscape

Past

Broadcast attacks

- Networks worms
- Denial of Service

Present

Financially motivated attacks

- Phishing / Social Engineering
- Botnets
- Rootkits

Future









Specific target attacks

- Technically-oriented social engineering attacks
- Cross-device attacks



- Identity Theft
- Data Leakage/Theft
- DDoS Extortion
- Frauds
- Software Piracy
- Illegal Downloads
- Child Exploitations
- Others

Recent losses of data

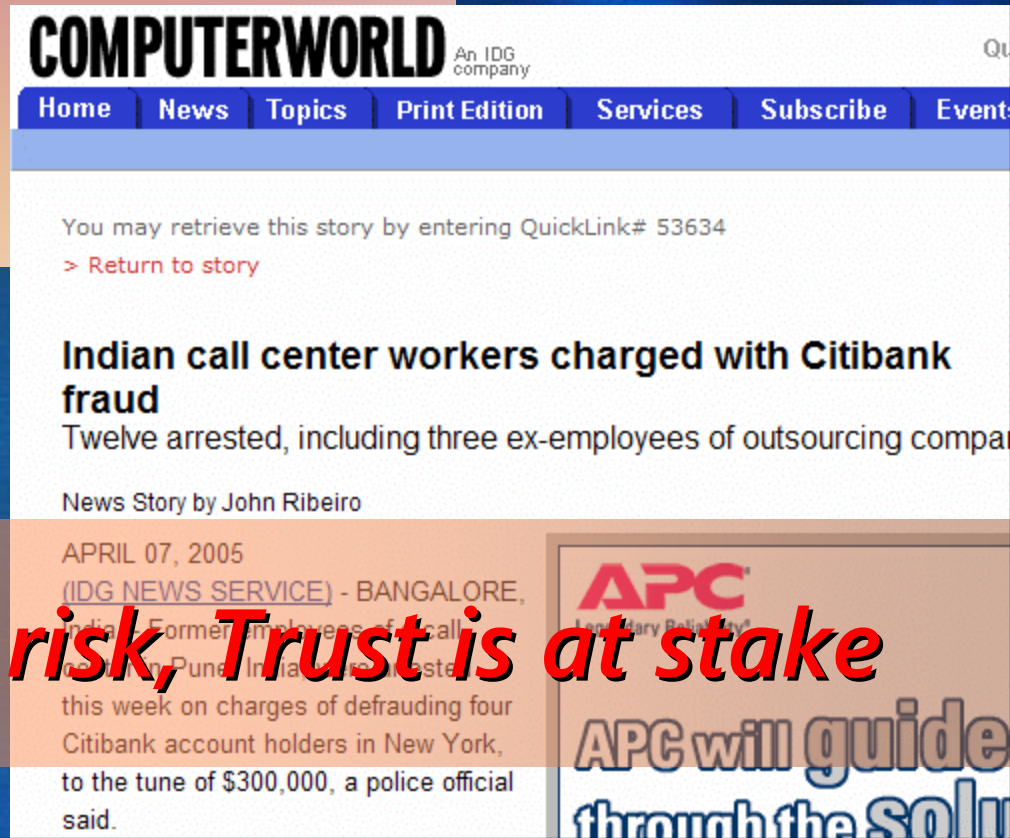
	When	What	How
	2/15/2005	145,000 addresses and SSNs	Bought data posing as legitimate customers
	2/25/2005	1,200,000 SSNs	Computer backup tapes were lost.
	3/8/2005	1,400,000 credit and debit cards	Hackers stole data from a database from 108 stores
	3/9/2005	310,000 SSNs and driver's licenses	Unauthorized use of customer logins
	3/17/2005	120,000 addresses and SSNs	Intruder hacked into a school computer
	4/14/2005	180,000 credit cards	Employees
	4/19/2005	200,000 items	Backup computer tape was lost in shipping
	5/2/2005	600,000 SSNs	Backup computer tape was lost in shipping

When Security slacks, Privacy is at Risk

Expanding threat boundary

- Mphasis Call Center (India)
 - Four bank accounts, defrauding up to US\$300,000/- by three BPO's employees
 - Implication extended beyond security and privacy of outsourcing providers
 - Cost and challenges of restoring trust (many entities)

When Privacy is risk, Trust is at stake



The screenshot shows a news article from Computerworld, an IDG company. The article is titled "Indian call center workers charged with Citibank fraud" and is dated April 07, 2005. It reports that twelve people, including three ex-employees of an outsourcing company, were arrested for defrauding four Citibank account holders in New York for a total of \$300,000. The article is by John Ribeiro. In the bottom right corner, there is a partial view of an APC advertisement with the text "APC will guide through the Solu".

COMPUTERWORLD An IDG company

Home | News | Topics | Print Edition | Services | Subscribe | Events

You may retrieve this story by entering QuickLink# 53634
> [Return to story](#)

Indian call center workers charged with Citibank fraud
Twelve arrested, including three ex-employees of outsourcing company

News Story by John Ribeiro

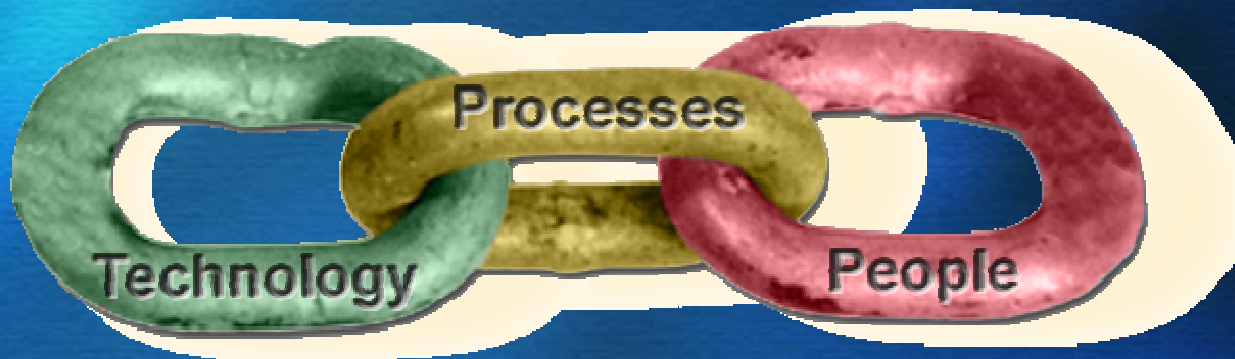
APRIL 07, 2005
(IDG NEWS SERVICE) - BANGALORE, India - Former employees of a call center in Pune, India, were arrested this week on charges of defrauding four Citibank account holders in New York, to the tune of \$300,000, a police official said.

APC
Let's Make Your Business a Reality!

APC will guide through the Solu

Privacy Is Only As Strong As The Weakest Link

- Technology is neither the whole problem nor the whole solution
- Privacy enhanced systems depend upon Technology, Processes (including Policies) and People (including Organization)



Privacy enhancing technologies and features

- Privacy statement (short notices)
- Platform for Privacy Protection (P3P) integration
- Privacy settings and centralized management
- Ability to see what's being transmitted
- Ability to clear tracks and stored information
- Documentation of privacy-related data
- Unsubscribe feature
- Access control
- Encryption
- Anonymizer - proxy
- Mix
 - Anonymous communications
 - Unlink, or remove correspondences between in incoming and outgoing messages
 - Mix unrelated messages to remove linkages
- ... see www.petworshop.org and www.cfp.org

Privacy enhancing technologies

- History-clearing tools

<http://www.historykill.com>

- Popup blockers

- Anti-spam, anti-phishing

- Anti-spyware

www.spychecker.com/software/antispay.html

www.microsoft.com/antispayware

- Cookie managers

- Secure file deletion

`cipher.exe /w:directory`

- Online privacy protection suites

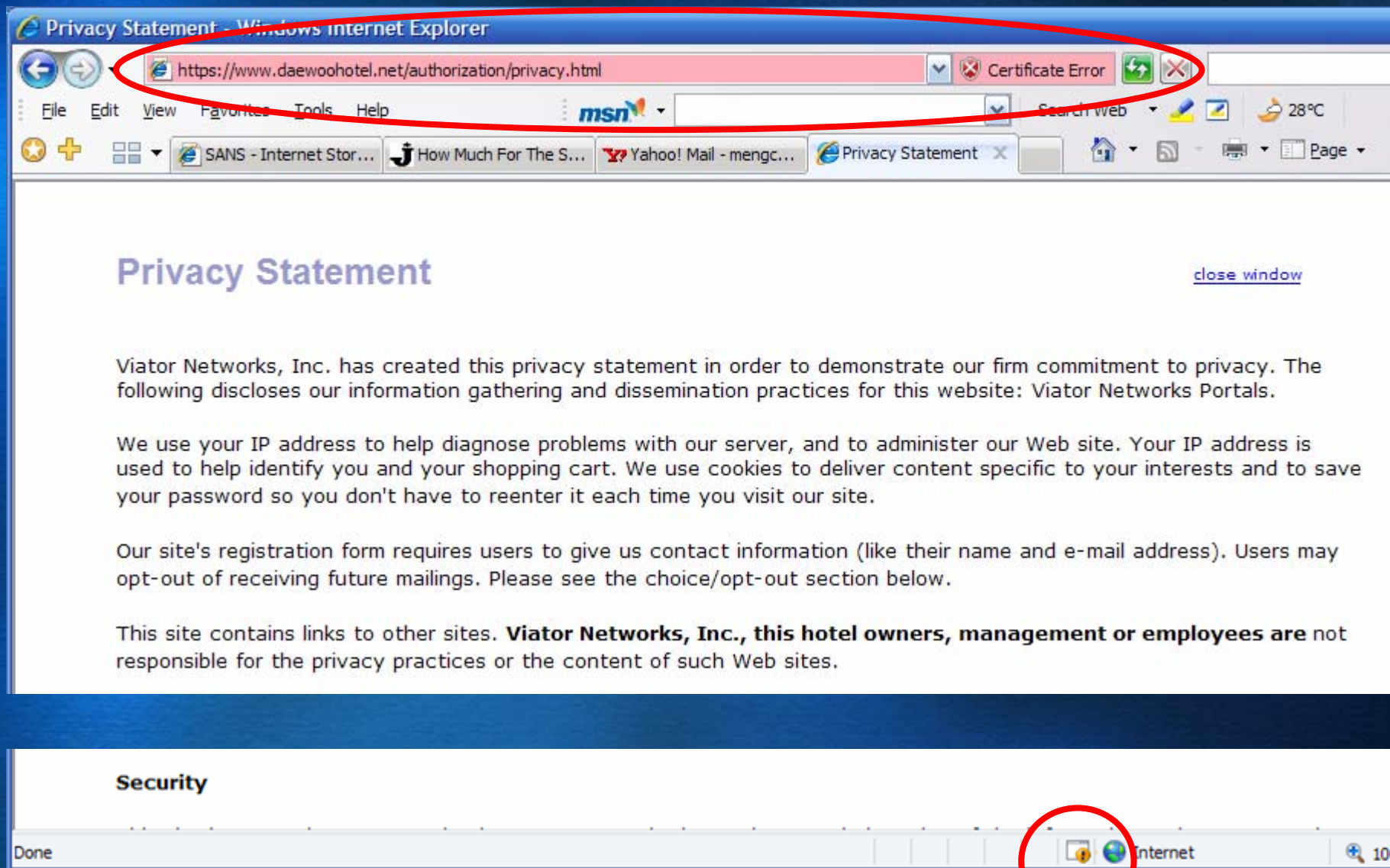
<http://www.junkbusters.com>

<http://www.synomos.com> (enterprise)

Microsoft PETs

<i>BizTalk HIPPA Accelerator</i>	Permits BizTalk users to protect medical information included in transactions
<i>CryptoAPI</i>	Data encryption APIs in VisualStudio.NET
<i>EFS</i>	Protects confidential files at the operating system level
<i>Internet Explorer popup blocker</i>	Blocks ads and other privacy-invading devices on web sites Anti-Phishing Toolbar & integration (IE7)
<i>RMS and IRM</i>	Protect and restrict documents (Office 2003)
<i>Internet Explorer</i>	P3P integration helps for managing cookies
<i>MS-CRM</i>	Email privacy settings
<i>MSN</i>	Parental controls; spam protection; email certification and sealing (beta); popup "pusher"; anti-spyware (MSN Premium); Sender-ID
<i>Outlook</i>	Anti-spam; support for IRM; Secure remote access
<i>Office hidden data removal tool</i>	Removes metadata from Word, Excel, and PowerPoint documents
<i>Windows Messenger</i>	Control visibility of state and who can send you messages

Anti-Phishing in IE7



Key Trends in Digital Identity...

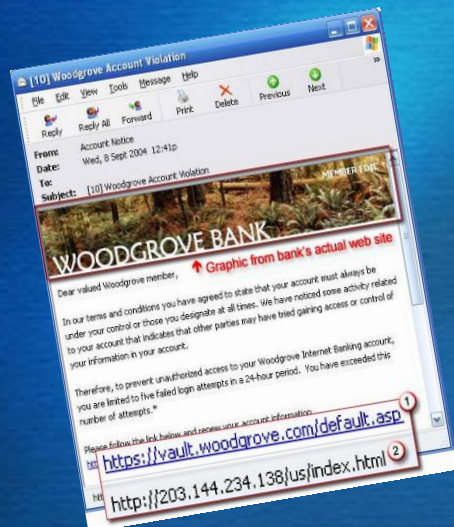
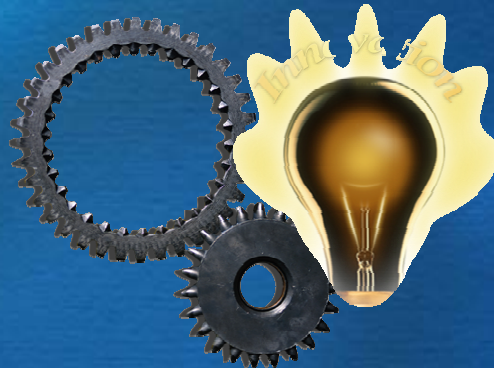
Number of Passwords Growing

Company	User Name	Password
eBay	john658739	football
MSDN	john@home.com	gohawks
WSJ	john@wsj.com	gohawks
My Bank	My Account #	gohawks1
My Broker	My SS#	Go#Hawks1
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.
.	.	.

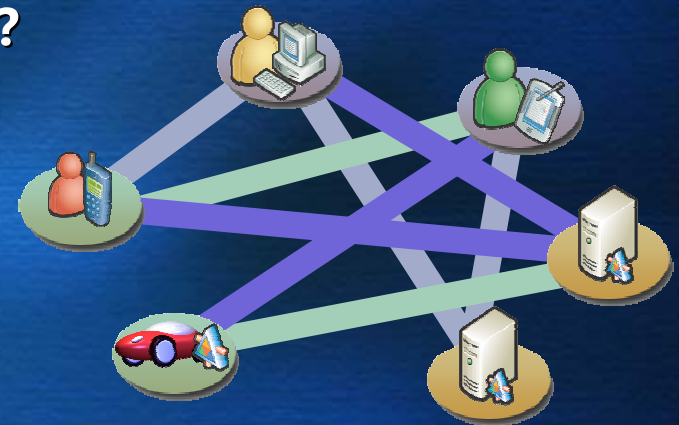
Mobile Identities On the Rise



Is the Industry Finished Innovating?



New Threats Emerging



Applications Increasingly Connected

Lessons from Passport & others



- Passport designed to solve two problems
 - Identity provider for MSN
 - 250M+ users, 1 billion logons per day
 - Identity provider for the Internet
 - Unsuccessful
- Identity efforts succeed and fail for reasons both technological and sociological
- Solution must move beyond single technology and single provider
- Solution must withstand the tests of a set of fundamental principles or propositions, i.e., the Laws of Identity.

The Laws of Identity

Established Through Industry Dialogue

1. User control and consent
2. Minimal disclosure for a defined use
3. Justifiable parties
4. Directional identity (public versus private identity)
5. Pluralism of operators and technologies
6. Human integration
7. Consistent experience across contexts

Join the discussion at www.identityblog.com

Identity Metasystem whitepaper -

<http://msdn.microsoft.com/webservices/webservices/understanding/advancedwebservices/default.aspx?pull=/library/en-us/dnwebsrv/html/identitymetasystem.asp>



Trustworthy Computing



Security

- Resilient to attack
- Protects confidentiality, integrity, availability of data and systems



Privacy

- Individual control of personal data
- Products, online services adhere to fair information principles
- Protects right to be left alone



Reliability

- Engineering Excellence
- Dependable, performs at expected levels
- Available when needed



Business Integrity

- Open, transparent interaction with customers
- Address issues with products and services
- Help customers find appropriate solutions

Aspirations for the Industry



Support the **Trust Ecosystem** through accountable identities

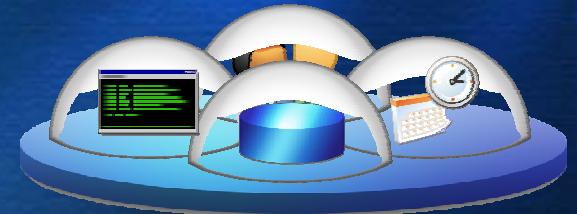


Engineering for Security

Embrace secure coding practices
incorporating TwC
D3+C



Drive for **Simplicity**



Fundamentally Secure Platforms

Develop products, services,
and platforms using standards
and best practices

The Microsoft logo is displayed in a bold, black, sans-serif font. Below it, the tagline "Your potential. Our passion." is written in a smaller, italicized, black, sans-serif font. The text is centered on a white, cloud-like shape that has a soft, glowing blue gradient around it. The background of the entire slide is a dark blue gradient.

Microsoft®

Your potential. Our passion.™

© 2006 Microsoft Corporation. All rights reserved.

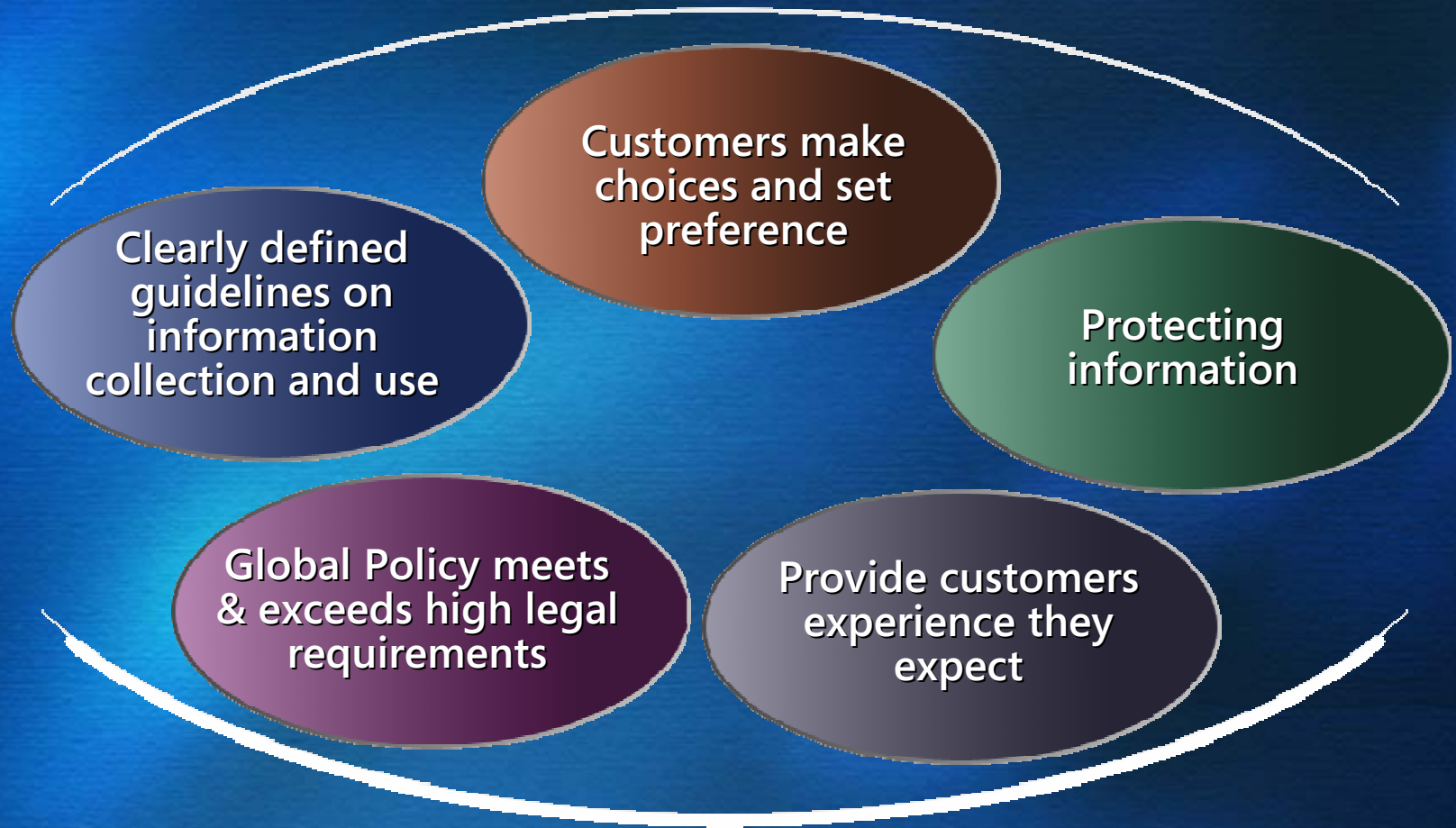
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

Customer Trust



Help realize the potential of Technology

Microsoft's Approach to Privacy



Putting Customers in Control of their Information

PD3+C Privacy Framework

PD³ + Communications

Privacy in Design

- Put users in charge of their information
- Address needs of enterprises and parents
- Comply with corporate policies

Privacy by Default

- Collect only data that is required
- Get appropriate consent
- Protect the storage and transfer of data

Privacy in Deployment

- Privacy deployment guidelines for users
- Offer comprehensive privacy options
- Privacy response team for all products

Communications

- Analyst reviews and white papers
- Content on MS.com, MSN.com privacy sites
- Participation in privacy & tech conferences



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/015

Agenda Item: 12

Privacy-Preserving Data Mining and E-commerce & E-government

Purpose: Information

Submitted by: Japan



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Privacy-Preserving Data Mining and E-commerce & E- government

Tu Bao Ho

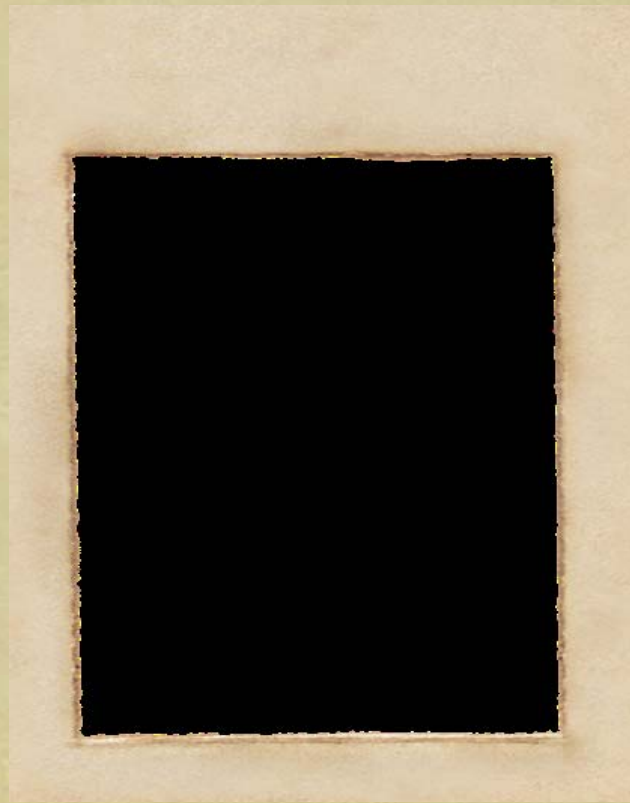
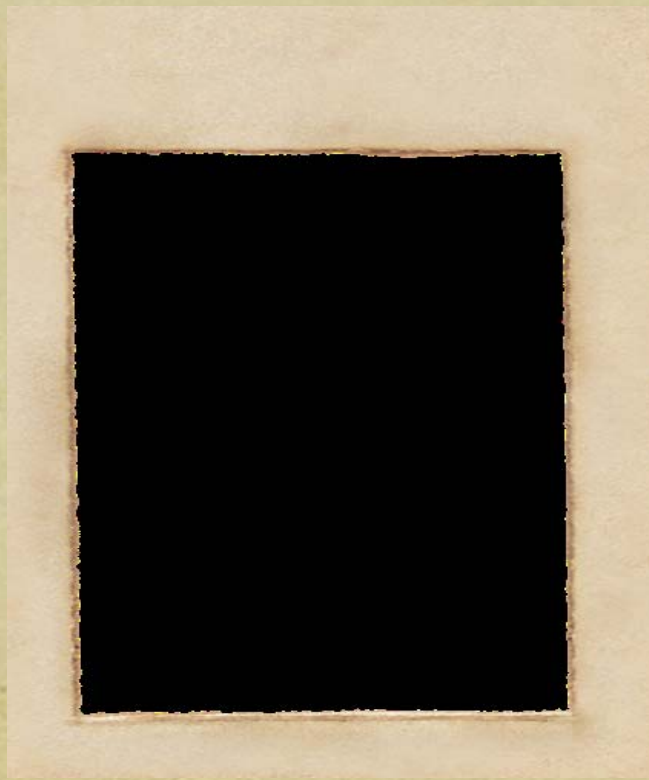
School of Knowledge Science

Japan Advanced Institute of Science and Technology

and

IOIT, Vietnamese Academy of Science and Technology

Outline

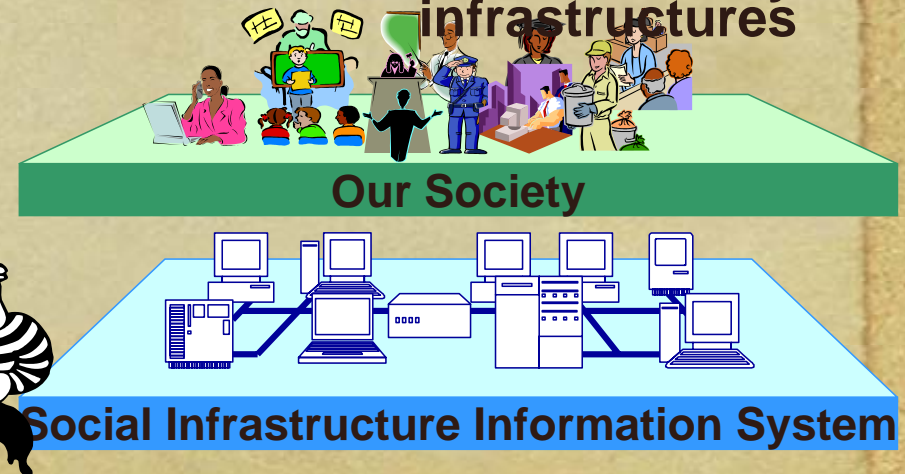


Requirements for trustworthy e-society

- ♦ E-government: networked and digitalized administration.
- ♦ E-commerce: Online business
- ♦ Can you trust e-society infrastructure information system and leave your life to it?
- ♦ Is your private data illegally accessed or altered?

COE program on
“Verifiable and
Evolvable
E-Society” (2004-2009)

1. Correctness
2. Accountability
3. Security
4. Fault Tolerance
5. Evolvability
6. Trustworthy infrastructures



Just the tip of the iceberg for consumers and for enterprises...

Data on individuals and enterprises are widely available from electronic databases

Business Intelligence

A Corp. ordering \$35,000,000
of our product

Password Files

Financial Data

ABC corp. will be reporting a
loss of \$1.20 per share

Intellectual Property

Secret beverage recipe: Sugar,
water, and a hint of CO₂



Data mining: An interdisciplinary field

- Data collection
- Data access
- Data analysis

Machine Learning

Build computer systems that learn as well as humans do (learning from data).

Discovery of new and useful knowledge (patterns/models) in databases

Statistics

Infer information from data (deduction and induction, mainly numeric data)

Database

Store, access, search, update data (deduction)



What does data mining do?

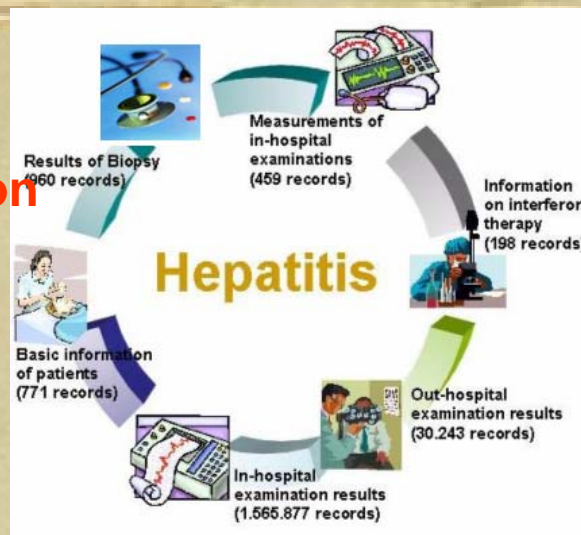
Tasks and methods

• Classification and Prediction

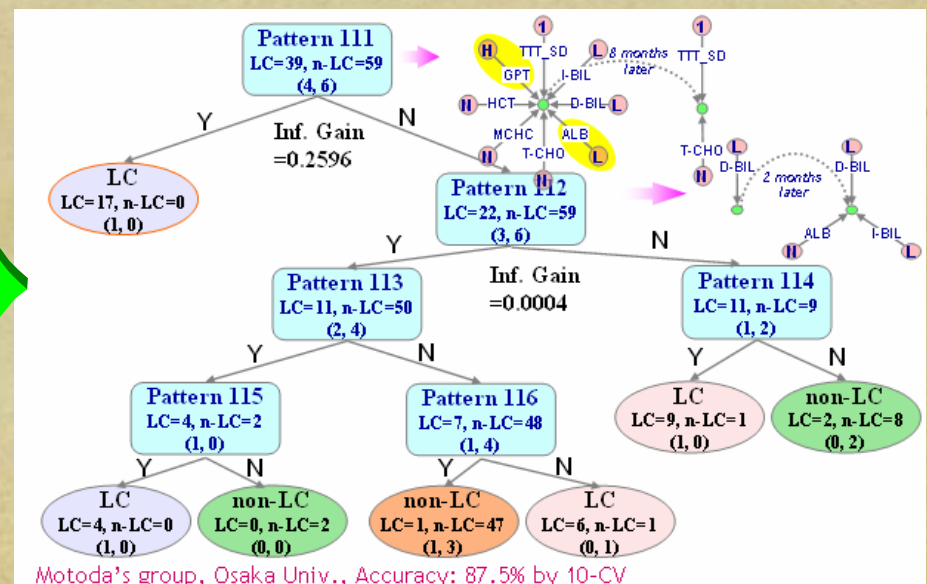
- Decision trees
- Neural network
- Rule induction
- Support vector machines
- Hidden Markov Model
- etc.

• Description

- Association analysis
- Clustering
- Summarization
- etc.



IF ALB = NormalToLow
AFTER
TP = high & peaks
THEN Liver cirrhosis (LC)



Motoda's group, Osaka Univ., Accuracy: 87.5% by 10-CV

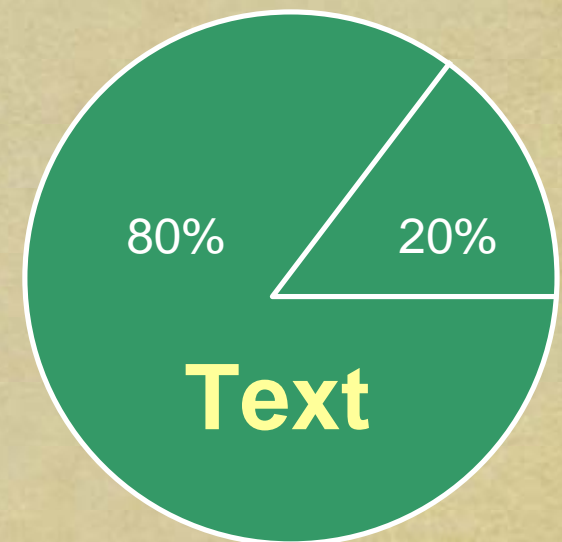
Text mining: A typical example

- Extract pieces of evidence from article titles in the biomedical literature (Swanson and Smalheiser, 1997)
 - "stress is associated with migraines"
 - "stress can lead to loss of magnesium"
 - "calcium channel blockers prevent some migraines"
 - "magnesium is a natural calcium channel blocker"



Induce a **new hypothesis not in the literature** by combining culled text fragments with human medical expertise

- Magnesium deficiency may play a role in some kinds of migraine headache

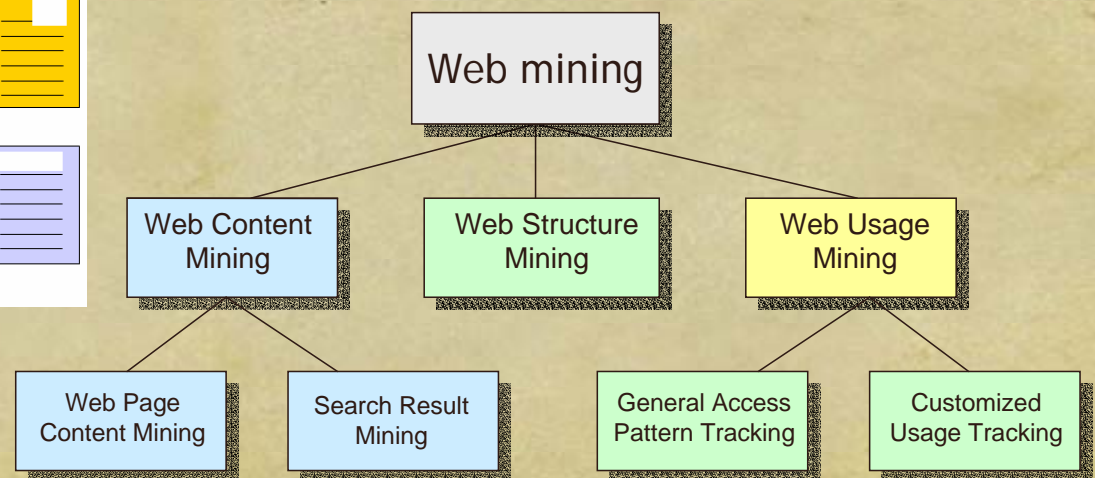
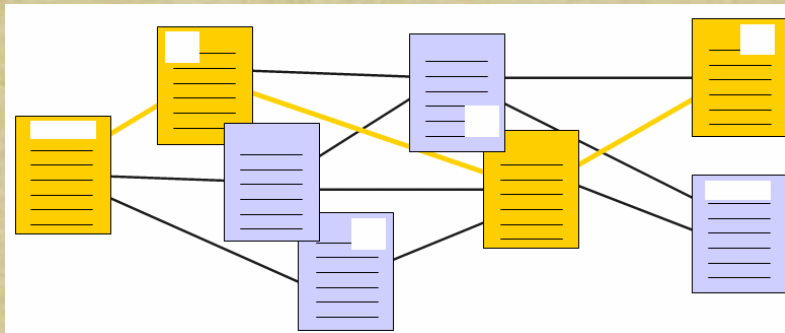


Web mining

Typical data in a server access

log

```
looney.cs.umn.edu han - [09/Aug/1996:09:53:52 -0500] "GET mobasher/courses/cs5106/cs5106l1.html HTTP/1.0" 200
mega.cs.umn.edu njain - [09/Aug/1996:09:53:52 -0500] "GET / HTTP/1.0" 200 3291
mega.cs.umn.edu njain - [09/Aug/1996:09:53:53 -0500] "GET /images/backgnds/paper.gif HTTP/1.0" 200 3014
mega.cs.umn.edu njain - [09/Aug/1996:09:54:12 -0500] "GET /cgi-bin/Count.cgi?df=CS home.dat&dd=C\&ft=1 HTTP
mega.cs.umn.edu njain - [09/Aug/1996:09:54:18 -0500] "GET advisor HTTP/1.0" 302
mega.cs.umn.edu njain - [09/Aug/1996:09:54:19 -0500] "GET advisor/ HTTP/1.0" 200 487
looney.cs.umn.edu han - [09/Aug/1996:09:54:28 -0500] "GET mobasher/courses/cs5106/cs5106l2.html HTTP/1.0" 200
... ..
```



KDD: New and fast growing area



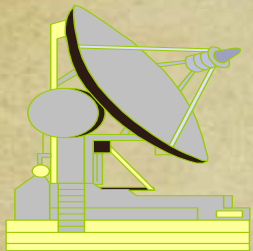
KDD'95, 96, 97, 98, ..., 04, 05 (ACM, America)

PAKDD'97, 98, 99, 00, ..., 04, 05 (Pacific & Asia)

<http://www.jaist.ac.jp/PAKDD-05> (Hanoi)

PKDD'97, 98, 99, 00, ..., 04, 2005 (Europe)

ICDM'01, 02,..., 04, 05 (IEEE), SDM'01, ..., 04, 05 (SIAM)



Industrial Interest: IBM, Microsoft, Silicon Graphics, Sun, Boeing, NASA, SAS, SPSS, ...



Japan: FGCS Project focus on logic programming and reasoning; attention has been paid on knowledge acquisition and machine learning. Projects “Knowledge Science”, “Discovery Science”, and “Active Mining Project” (2001-2004)

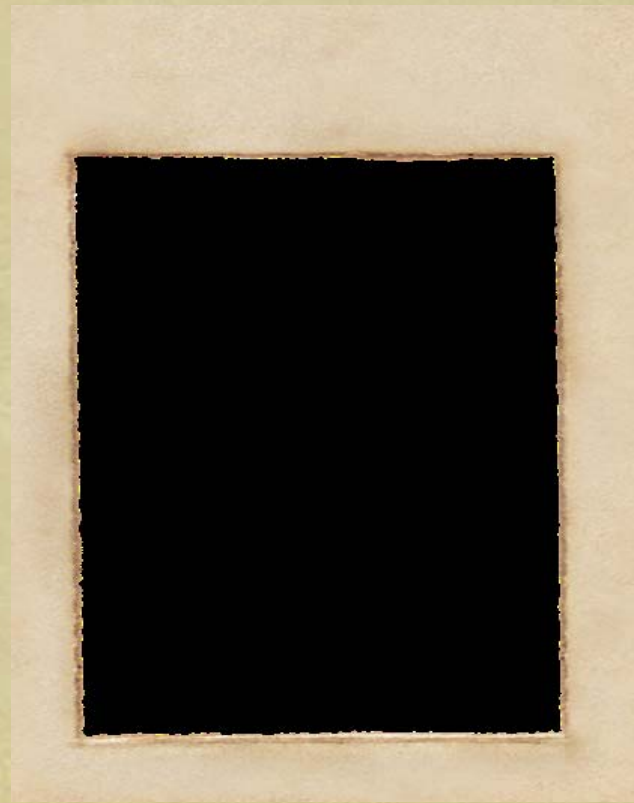
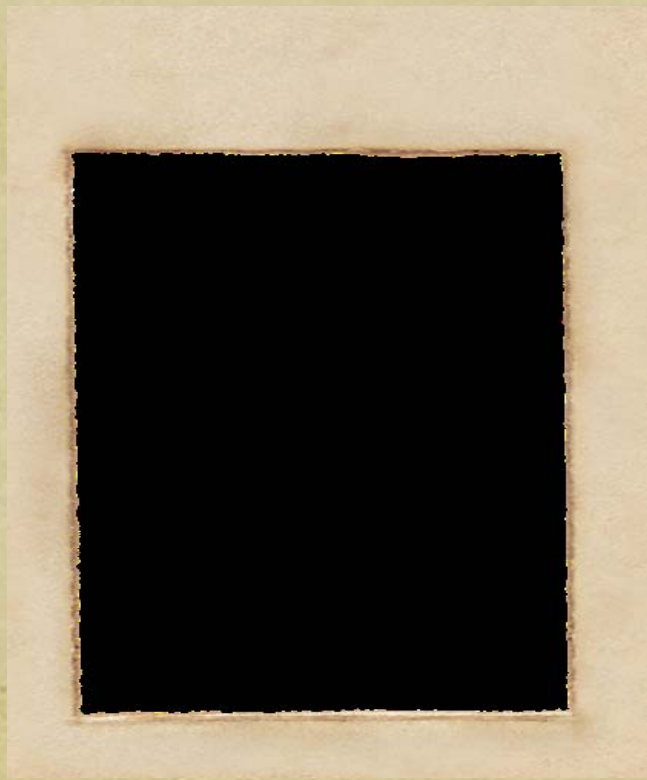
E-commerce and Data Mining

- ♦ A person buys a book (product) at Amazon.com.
- ♦ Task: Recommend other books (products) this person is likely to buy
- ♦ Amazon does clustering based on books bought:
 - ♦ customers who bought “E-Commerce Security and Privacy”, also bought “E-commerce & privacy: What net users want”
- ♦ Recommendation program is quite

E-government and Data Mining

- ♦ Hospital data contains
 - ♦ Identifying information: name, id, address
 - ♦ General information: age, marital status
 - ♦ Medical information
 - ♦ Billing information
- ♦ Database access issues:
 - ♦ **Your doctor** should get every information that is required to take care of you
 - ♦ **Emergency rooms** should get all medical information that is required to take care of whoever comes there
 - ♦ **Billing** department should only get information relevant to billing
- ♦ Data usage issue: “**who** is doing **what** to **which** and **how much** critical information, **when** and from **where**”

Outline



Data Mining and Privacy

- ◆ There is a growing concern among citizens in protecting their privacy
- ◆ Government and business have strong motivations for data mining
- ◆ Can we satisfy both the data mining goal **and** the privacy goal?

Protests over a National Registry



Privacy-Preserving Data Mining

- ◆ Allow multiple data holders to collaborate to compute important (e.g., security-related) information while protecting the privacy of other information.
- ◆ Particularly relevant now, with increasing focus on security even at the expense of some privacy.

Advantages of privacy protection

- ◆ **Protection of personal information**
- ◆ **Protection of proprietary or sensitive information**
- ◆ **Fosters collaboration between different data owners (since they may be more willing to collaborate if they need not reveal their information)**

10 challenging problems in data mining

(ICDM'05)

1. Developing

2. Scaling
streams

3. Mini

4. Min

5. Data

6. Dist

7. Da

8. Mining

9. Security, privacy and data integrity

10. Dealing with non-static, unbalanced and cost-sensitive data

The trade-off between sharing information for analysis and keeping it secret to corporate trade secrets and customer privacy is a growing challenge.

data

problems

ms

Three approaches to PPDM

- ◆ **Distribute limited subset of data**
 - ◆ E.g., Census bureau releases only some fields
 - ◆ Theory tells which subsets can be safely released
- ◆ **Distribute purposely distorted data records**
 - ◆ Nobody see the real data
 - ◆ Tell recipients the probabilistic distortion function
 - ◆ They can compute original data distribution, but not original data records
- ◆ **Distribute the computation instead of data**
 - ◆ Use cryptographic methods to assure privacy of intermediate computations

Distribute limited subset of data

- A naïve solution to the problem is **de-identification** — removing all identifying information from the data and then releasing it—but pinpointing exactly what constitutes identification information is difficult.
- Latanya Sweeney (2001)
 - Date of birth uniquely identifies 12% of the population of Cambridge, MA.
 - Date of birth + gender: 29%
 - Date of birth + gender + (9 digit) zip code: 95%
 - Sweeney was therefore able to get her medical information from an “annonymized” database

Distribute purposely distorted data records

- ♦ **Goal:** Hide the protected information
- ♦ **Approaches:** Data perturbation
 - ♦ **Swap values between records:** exchanging data values between records in ways that preserve certain statistics but destroy real values
 - ♦ **Randomly modify data:** adding noise to data to prevent discovery of the real values.
- ♦ **Problems**
 - ♦ Does it really protect the data?
 - ♦ Can we learn from the results?

Distribute purposely distorted data records

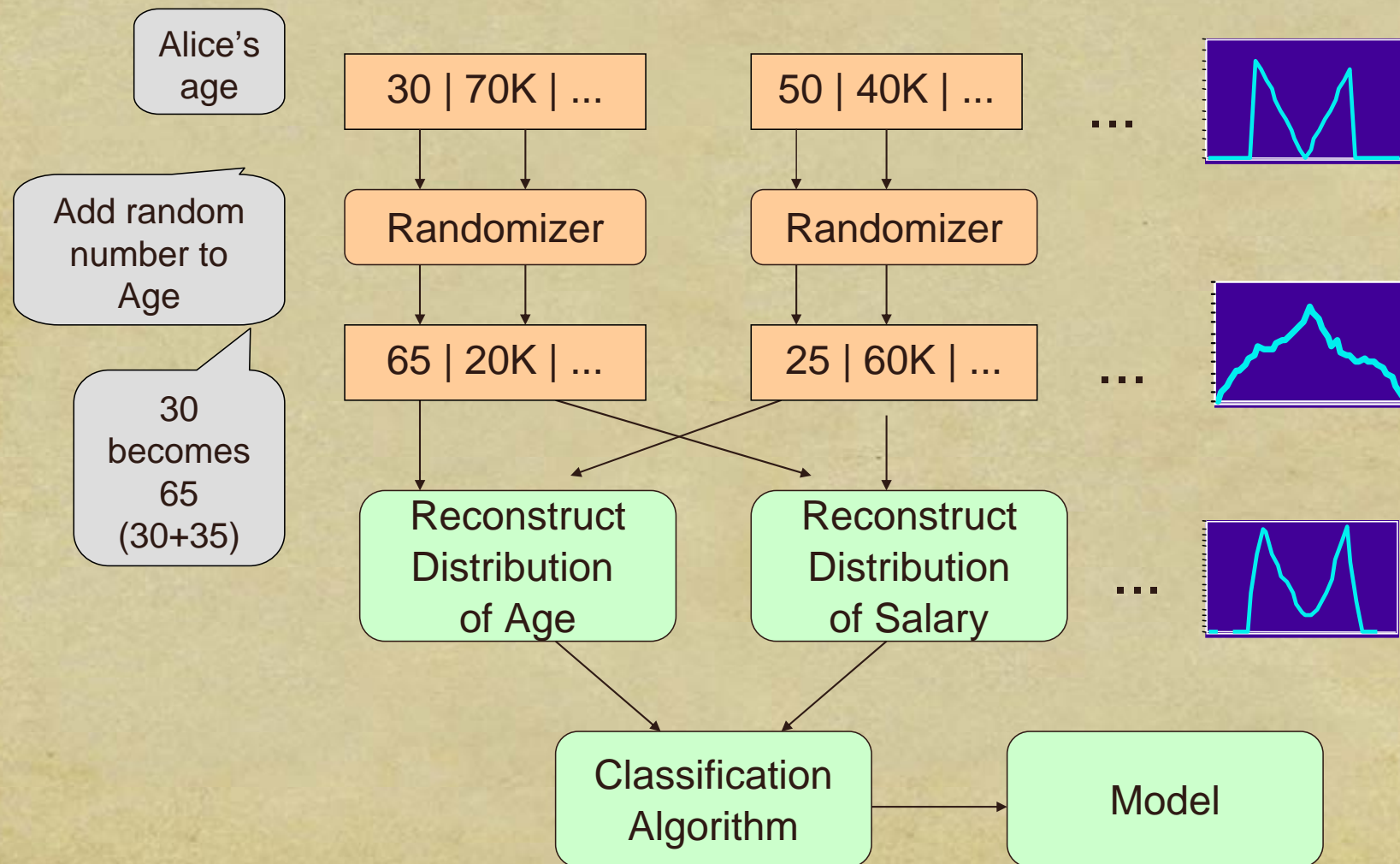
- ♦ Miner doesn't see the real data
 - ♦ Some knowledge of how data obscured
 - ♦ Can't reconstruct real values
- ♦ Results still valid
 - ♦ **Can** reconstruct enough information to identify patterns
 - ♦ But not entities
- ♦ Example: Work of Agrawal & Srikant (2000)

Decision trees

Agrawal and Srikant '00

- Assume users are willing to
 - Give true values of certain fields
 - Give modified values of certain fields
- Practicality
 - 17% refuse to provide data at all
 - 56% are willing, as long as privacy is maintained
 - 27% are willing, with mild concern about privacy
- Perturb data with value distortion
 - User provides $x_i + r$ instead of x_i
 - r is a random value
 - Uniform, uniform distribution between $[-\alpha, \alpha]$
 - Gaussian, normal distribution with $\mu = 0, \sigma$

Randomization approach overview



Reconstruction problem

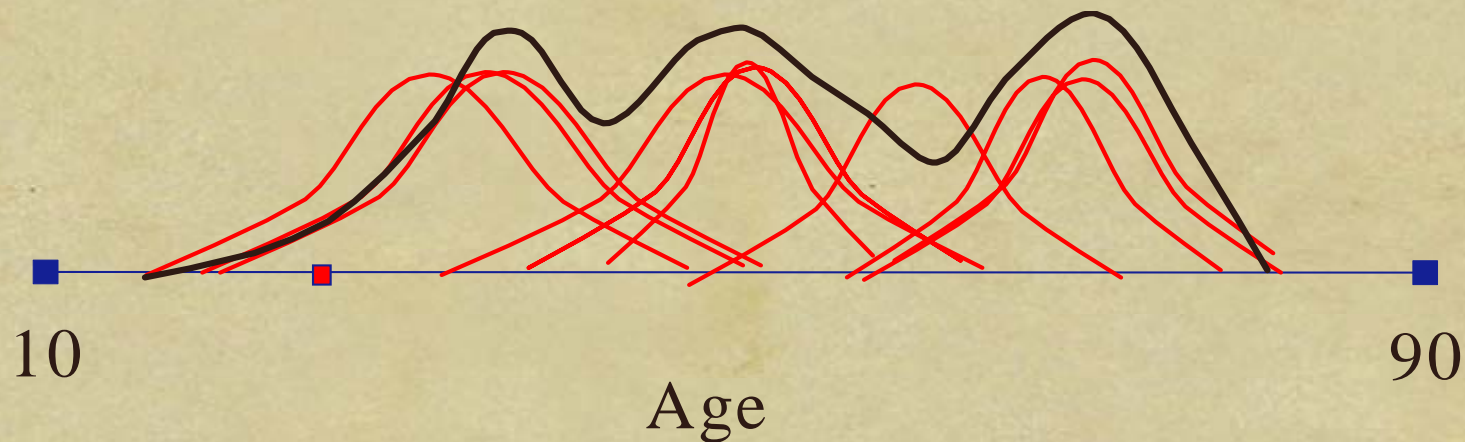
- ♦ Original values x_1, x_2, \dots, x_n
 - ♦ from probability distribution X (unknown)
- ♦ To hide these values, we use y_1, y_2, \dots, y_n
 - ♦ from probability distribution Y
- ♦ Given
 - ♦ $x_1+y_1, x_2+y_2, \dots, x_n+y_n$
 - ♦ the probability distribution of Y

Estimate the probability distribution of X .

Reconstructing the distribution

Combine estimates of where point came from for all the points:

Gives estimate of original distribution.



$$f_X = \frac{1}{n} \sum_{i=1}^n \frac{f_Y((x_i + y_i) - a) f_X^j(a)}{\int_{-\infty}^{\infty} f_Y((x_i + y_i) - a) f_X^j(a)}$$

Reconstruction: Bootstrapping

$f_X^0 :=$ Uniform distribution

$j := 0$ // Iteration number

repeat

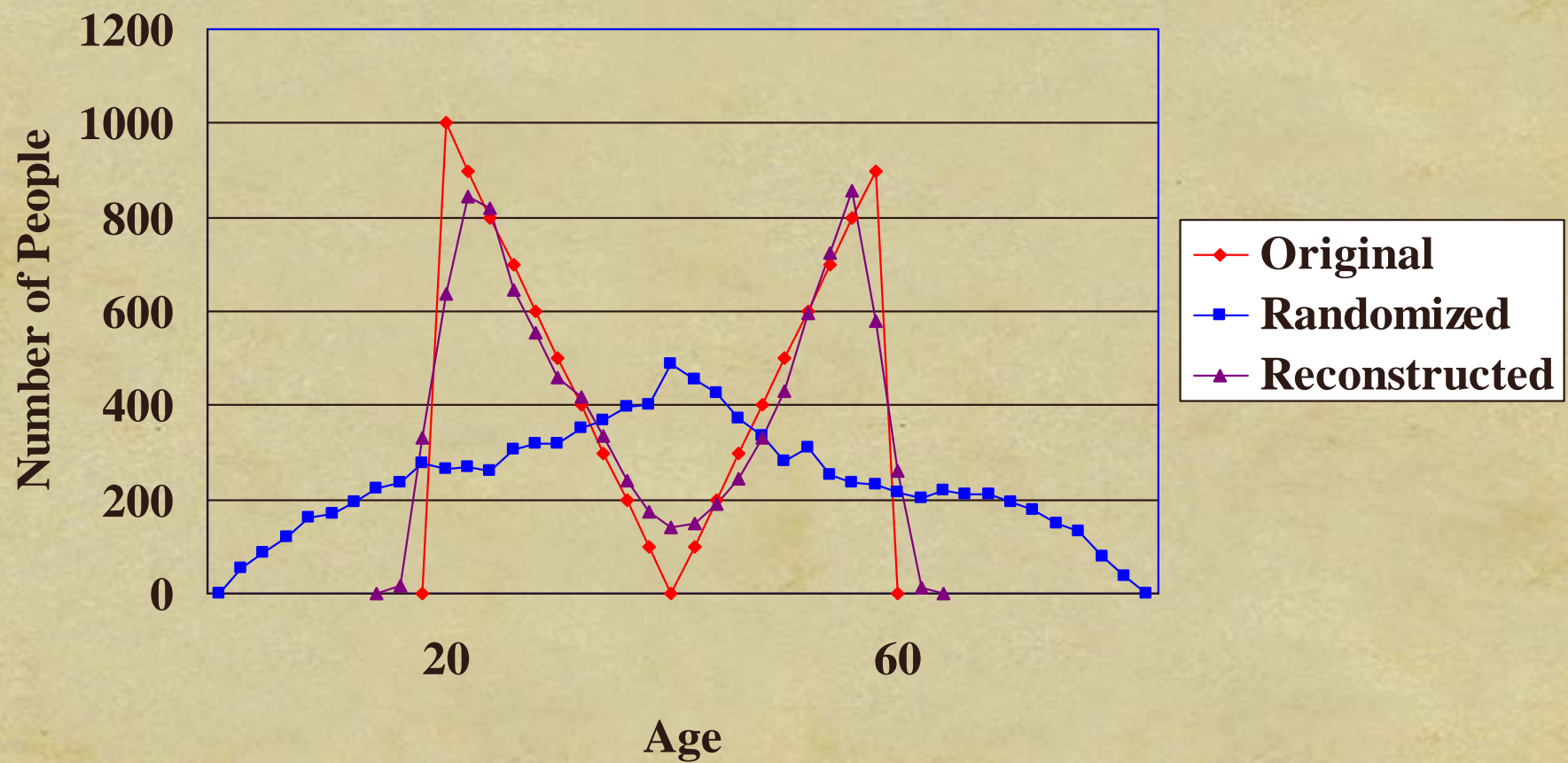
$$f_X^{j+1}(a) := \frac{1}{n} \sum_{i=1}^n \frac{f_Y((x_i + y_i) - a) f_X^j(a)}{\int_{-\infty}^{\infty} f_Y((x_i + y_i) - a) f_X^j(a)} \quad \text{(Bayes' rule)}$$

$j := j+1$

until (stopping criterion met)

- Converges to maximum likelihood estimate.
 - D. Agrawal & C.C. Aggarwal, PODS 2001.

Works well



Distribute the computation instead of data

- ◆ **Suppose**

- ◆ Multiple hospitals hold private patient data,
- ◆ They wish to learn rules for SARS treatment effectiveness
- ◆ But will not share details patient records

- ◆ **Idea**

- ◆ Allow them to retain their data, and their individual privacy policies
- ◆ Distribute computation
- ◆ Use cryptographic techniques to maintain privacy of distributed computation

Scenario

- ♦ **Multi database scenarios:** Two or more parties with private data want to cooperate.
- ♦ **Horizontally split:** Each party has a large database. Databases have same attributes but are about different subjects. For example, the parties are banks which each have information about their customers.



- ♦ **Vertically split:** Each party has some information about the same set of subjects, e.g., the participating parties are government agencies; each with some data about every citizen.

Secure multiparty computation (SMC)

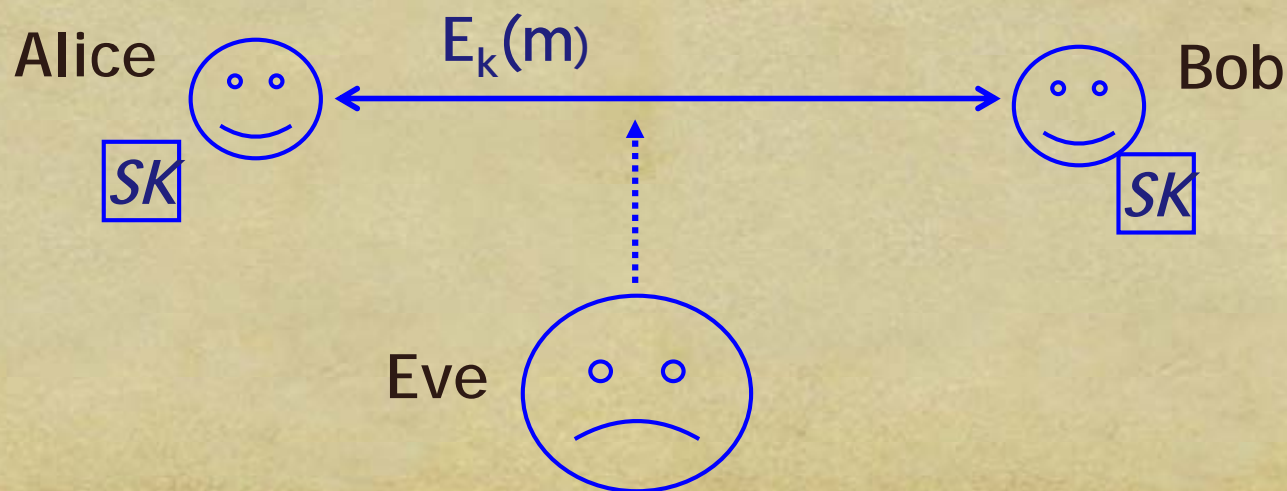
- ◆ A specialized form of privacy-preserving, **distributed data mining**.
- ◆ Parties that each know some of the private data participate in a protocol that generates the data mining results, yet that can be proven not to reveal data items to parties that don't already know them.
- ◆ **The basic idea is that parties hold their own data, but cooperate to get the final result.**

The methodology

- Because all interaction occurs through the messages sent and received, we simulate the views of all the parties by simulating the corresponding messages.
- If we can simulate these messages, then we can easily simulate the entire protocol just by running it.
- Instead, we use a notion from **cryptography**—the same message can be encrypted with different keys to look different, even though they represent the same message.

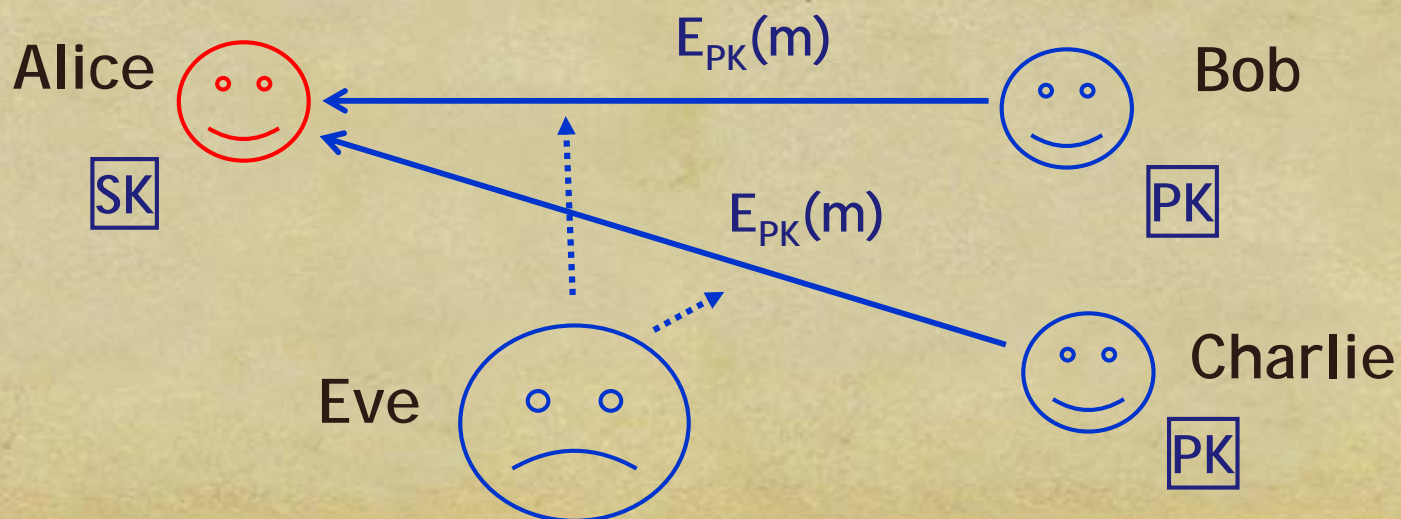
Encryption

- Alice wants to send a message $m \in \{0,1\}^n$ to Bob
 - Set-up phase is **secret**
 - Symmetric encryption: Alice and Bob share a secret key SK
- They want to prevent Eve from **learning** anything about the message.



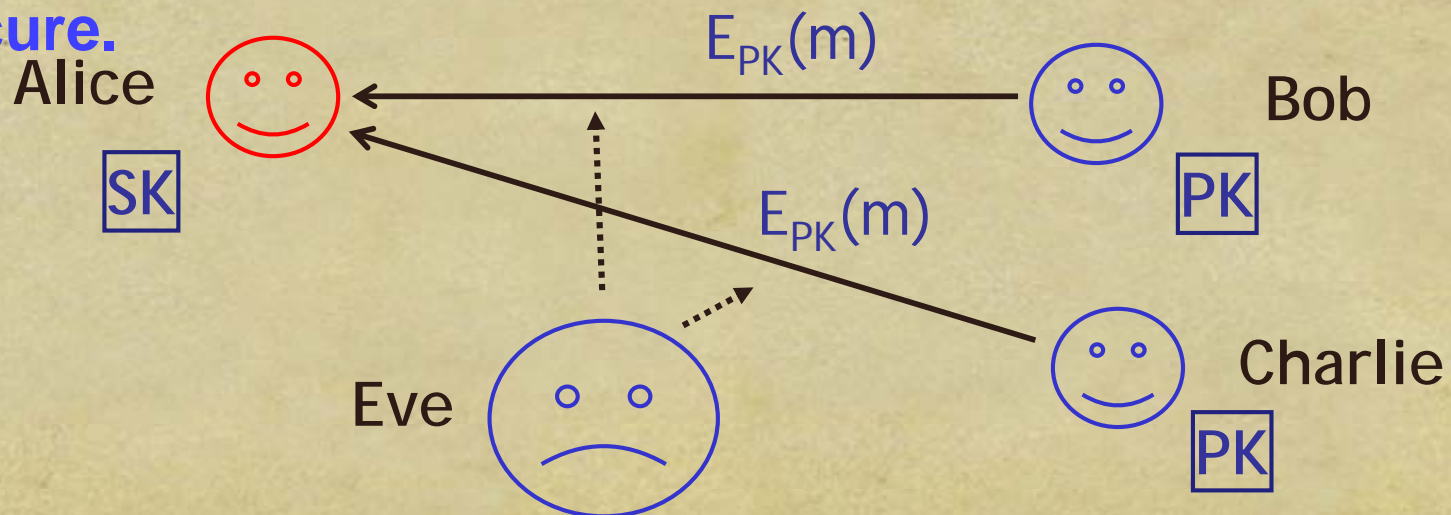
Public key encryption

- Alice generates a private/public key pair (SK,PK)
- Only Alice knows the secret key SK
- Everyone (even Eve) knows the public key PK, and can encrypt messages to Alice.
- Only Alice can decrypt (using SK)



Secure multiparty computation (SMC)

- A distribution of numbers is said to be **computationally indistinguishable** from another distribution of numbers if no polynomial time program can distinguish between the two distributions.
- As long as the sequence of numbers revealed during a protocol is computationally indistinguishable from numbers drawn from a random distribution, the protocol is assumed to be **secure**.



Progress has been made

- ◆ **Secure two party-computation (Yao, 1986)**
- ◆ **Secure multiparty-computation (secure distributed computation) (Goldreich et al., 1987)**
- ◆ **SMC techniques for data mining: ID3 (Lindell and Pinkas, 2002), association rule mining (Clifton, 2003, 2004), etc.**

Conclusion

- Privacy-preserving data mining is of growing importance, and some important progress has been made.
- Three ideas here:
 - Distribute only subset of data features
 - Distribute perturbed data records
 - Distribute computation rather than data
- Technical solutions can help (more work needed), but technology, policy, and education must work together.

References

- R. Agrawal, R. Srikant, “Privacy-Preserving Data Mining”, ACM SIGKDD, 2000.
- C. Clifton, “Privacy-Preserving Distributed Data Mining”, Tutorial ACM SIGKDD, 2003.
- T.B. Ho, Lecture on Knowledge Discovery and Data Mining, JAIST, 2005.
- Y. Lindell, B. Pinkas, “Privacy-Preserving Data Mining”, J. Cryptology, Vol. 15, No. 3, 2002.
- T. Mitchell, “Privacy-Preserving Data Mining”, CALD Summer School, June 2003.
- R. Srikant, “Privacy Preserving Data Mining: Challenges & Opportunities”, Invited talk, PAKDD 2002.
- J. Vaidya, C. Clifton, “Privacy-Preserving Data Mining: Why, How and When”, IEEE Security & Privacy, 2004.



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/016

Agenda Item: 14

Privacy Protection in the APEC Framework: The Potential of Technological Tools

Purpose: Information

Submitted by: Oracle



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Privacy Protection in the APEC Framework : The Potential of Technological Tools

Joseph Alhadeff
Vice President for Global Public Policy and
Chief Privacy Officer
Oracle

joseph.alhadeff@oracle.com

The Role of Technology Generally

- Technology is a tool that works in conjunction with, and support of, appropriate policies, practices and procedures
- First develop a privacy policy consistent with the applicable framework, establish the operational practices and determine the procedures.
- Understand the technology tools/functions available
- Optimize for the needs of the organization

Technology In Support Of Multiple Organization Needs

- Too often technology implementations do not support privacy because the “needs” are traded off against each other.
- There is a need to accomplish organization objectives, to secure information and also to protect privacy rights – ALL can be optimized.
- Many of the same functions that enable security and other organization functions also enable privacy

The Myth of Privacy Enhancing Technologies

- Too often people only focus on those technologies that are designed to support privacy as the only technology tools that support privacy
- The vast majority of software that is used by an enterprise of any size may be able to support privacy requirements.
- It can only do so, however, if its configured with privacy as one of the objectives

Privacy Supported in Technology

- Authentication: Who is the end user, who are the users accessing the system on the inside
 - Identity Management
- Authorization: What rights to authenticated users have?
 - Tied to HR system allows for updated management upon change of roles
- Access control: Based on user identity and rights, what content can user access
- Audit: Has user behavior contravened policy
 - Selective audit, fine grain audit, investigatory functions
- Encryption: stored and in transit

Database Technology and the APEC Framework

Framework Concept

Specify Uses of PII

Choice

Integrity

Security

Access and Correction

Accountability

Tool

Meta data and permissions

Role based access
controls

Application based controls

Recovery to previous state

Defense in depth

Label Security, VPD

Encryption

Security alerts

Audit controls

http://www.oracle.com/technology/deploy/security/db_security/index.html

ORACLE

Supporting Today's Information Flows: Policy and Tech

Commercial/E- government

Privacy Policy

Privacy Notice

Internal controls/PIA

Training

Accountable sharing

Compliance and
governance

Complaint handling

Enforcement

Implementation

Practices and procedures

Short form

Technology tools

E-learning

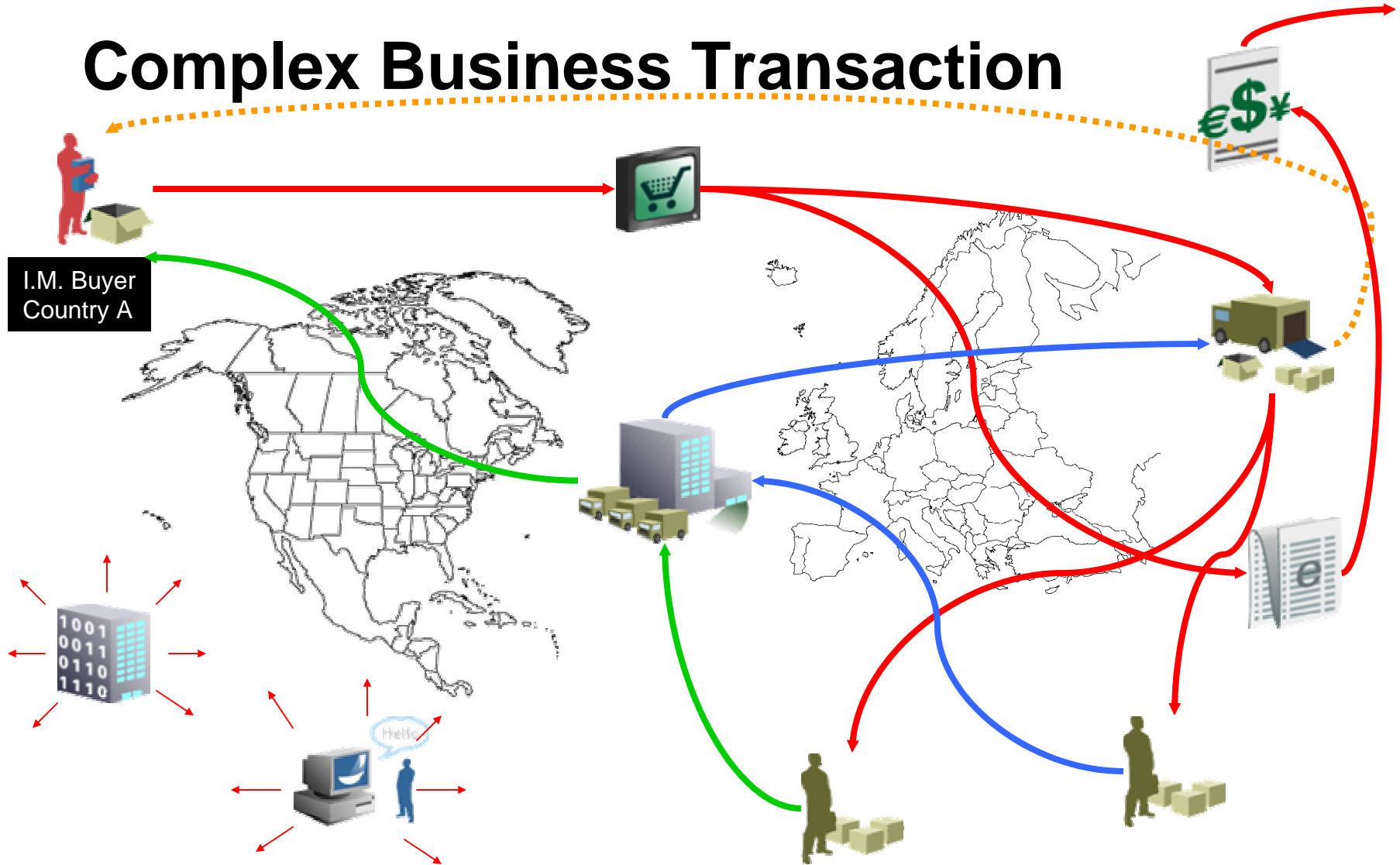
Agreements, MOU, Bridge...

Policies and Rules

Customer service training

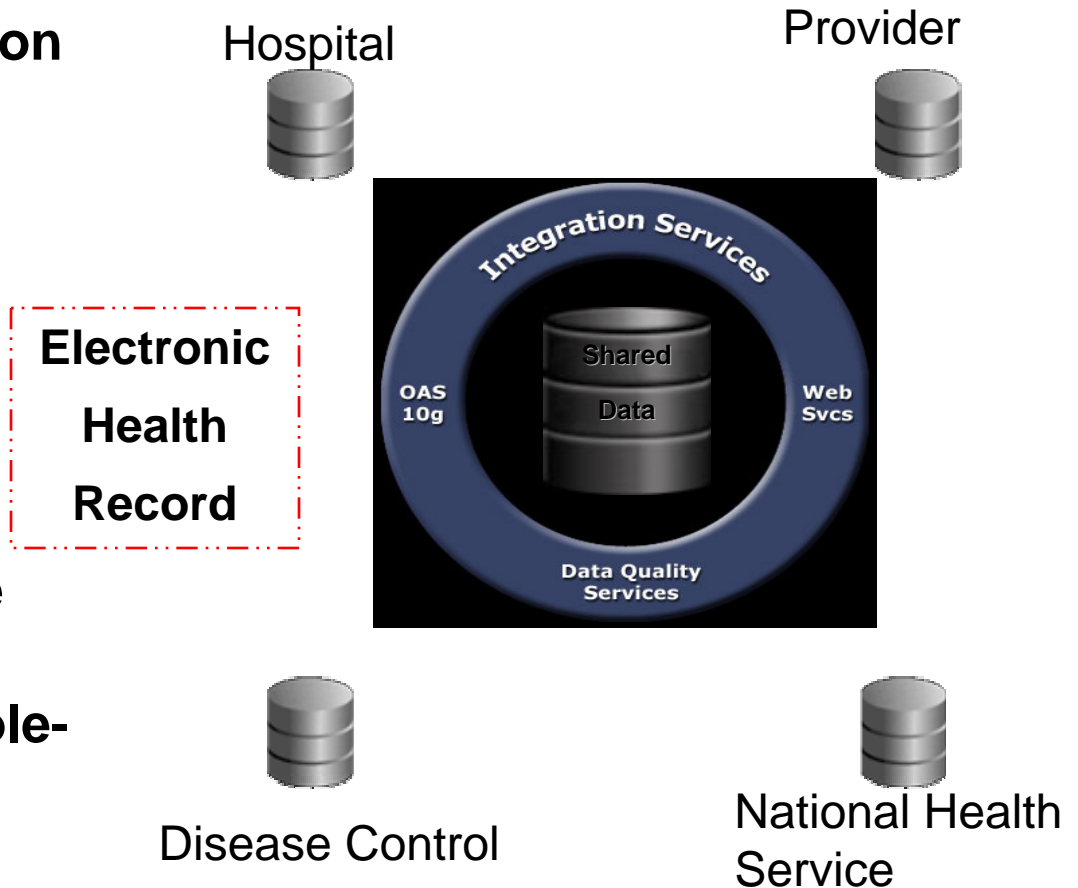
Internal procedures and
cooperation with
authorities

Complex Business Transaction



E-government Citizen Services Hub

- **Single source of truth for customer/event definition**
- **Near real-time data synchronization**
- **Data cleansing**
- **Key interactions**
- **360 degree view of data with pre-built analytics**
- **Local control of source info**
- **Appropriate rule and role-based sharing**
- **Supports compliance**



ORACLE®

Centralization and Compliance

Centralization of information may actually increase privacy

- Fault tolerant grid infrastructure
- Single Sign On - Password confusion limited
- Bastion security approach – both moat and security guard models
- Single view of user aids in compliance
- Compliance choke points
 - Privilege management
 - Accountability framework

In Conclusion

- Technology is a facilitating tool, not an end
- You must consider the needs of the organization, including privacy and then optimize the configuration
- Most software has privacy functionality
- Consider the overall information flows and the legal, technology and policy frameworks as well as your overall customer/citizen relationship



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/017

Agenda Item: 16

The SAMCOM project and information privacy protection

Purpose: Information
Submitted by: Viet Nam



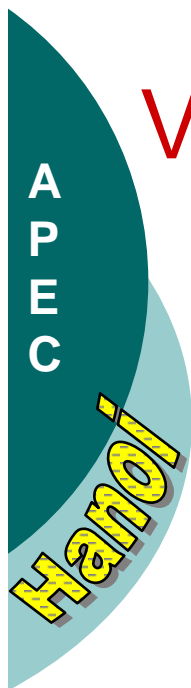
**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

VIETNAM PROGRAMME OF ADMINISTRATIVE REFORM

THE SAMCOM PROJECT AND INFORMATION PRIVACY PROTECTION

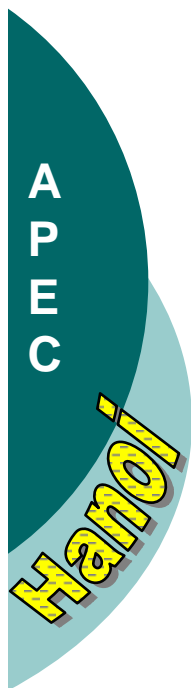
Nguyen Chi Cong
Project Consultant

APEC Symposium on Information Privacy Protection in E-government & E-commerce\
Hanoi, 20-22 February 2006



VIETNAM ADMINISTRATIVE REFORM

- **By his Decision No. 136/2001/QD-TTg of 17 September 2001 the Vietnam PM Phan Van Khai approved an Overall Programme on State Administrative Reform for the period of 2001-2010.**
- **By his Decision No. 169/2003/QD-TTg of 12 August 2003 the PM approved a Project on Restructuration and Modernization of Public Administrative System.**



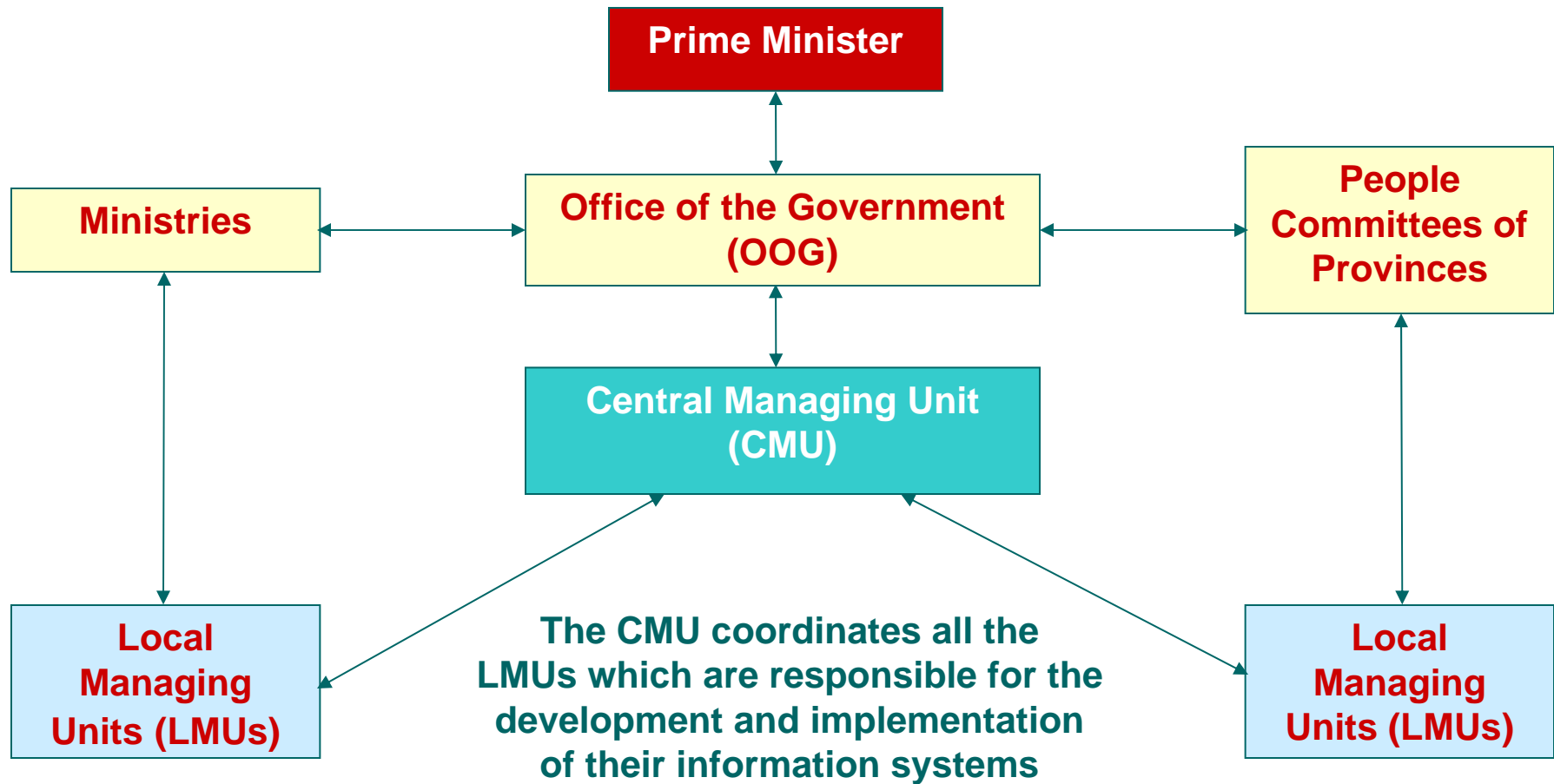
PROJECT ORIGINE

- On November 2000, in Singapore, the Vietnam PM signed the “e-ASEAN” Framework Agreement.
- By his Decision No. 112/2001/QD-TTg of 25 July 2001 the PM approved the Project of State Administrative Management Computerization (SAMcom) to start building the Vietnam digital administrations.
- By two Decisions No. 137/2001/QD-TTg and 27/2002/QD-TTg the PM established then the Project Central Managing Unit and assigned responsibilities to its members.

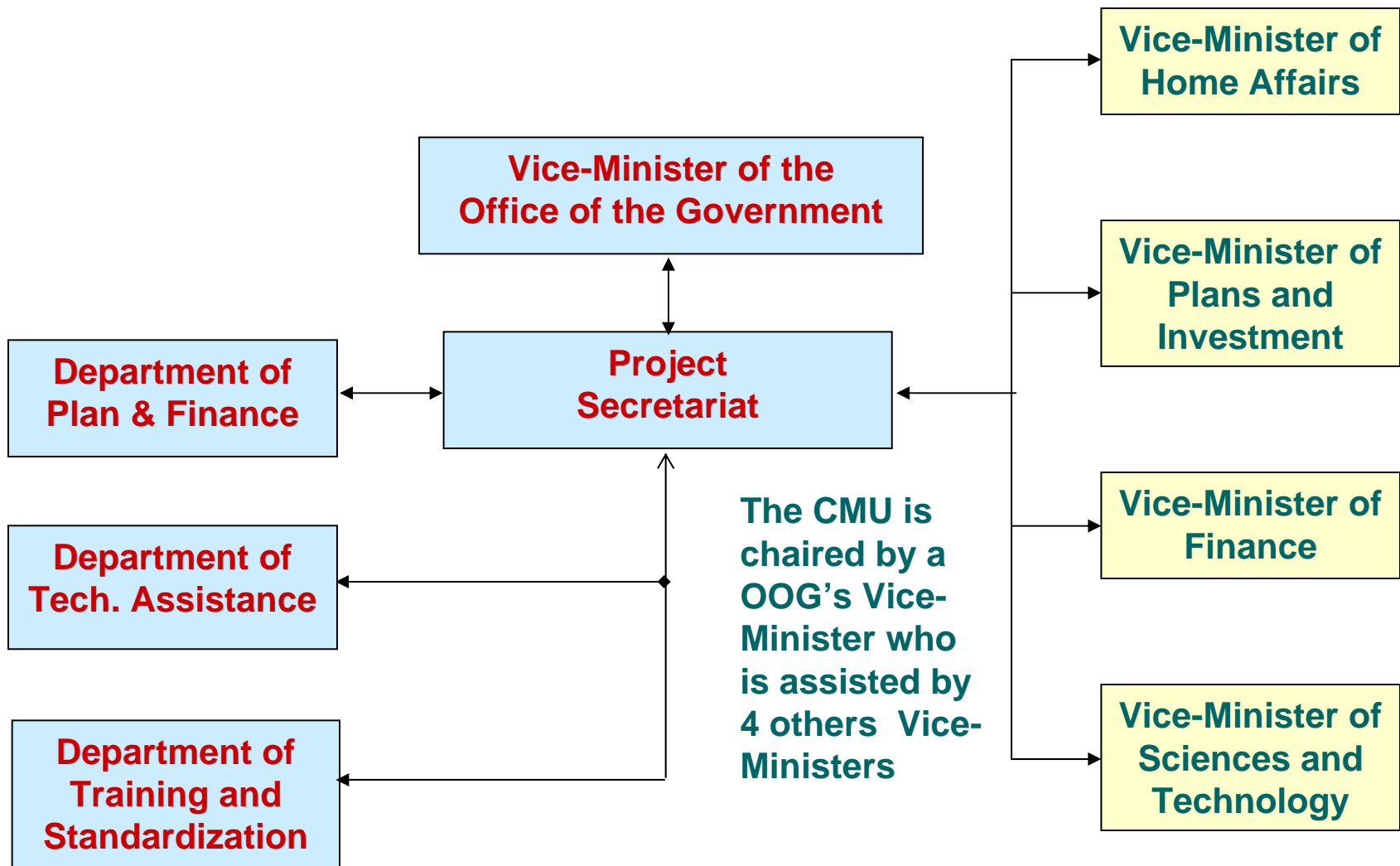
PROJECT TARGET

- **Computerize Ministries & People Committees**
- **Link their intranets by a backbone government network (CPnet)**
- **Standardize digital administrative information and processing formalities**
- **Build necessary information systems of the state administrative management for internal use and public services**
- **Train all public employees to use the systems**
- **Protect user privacy of the government information systems.**

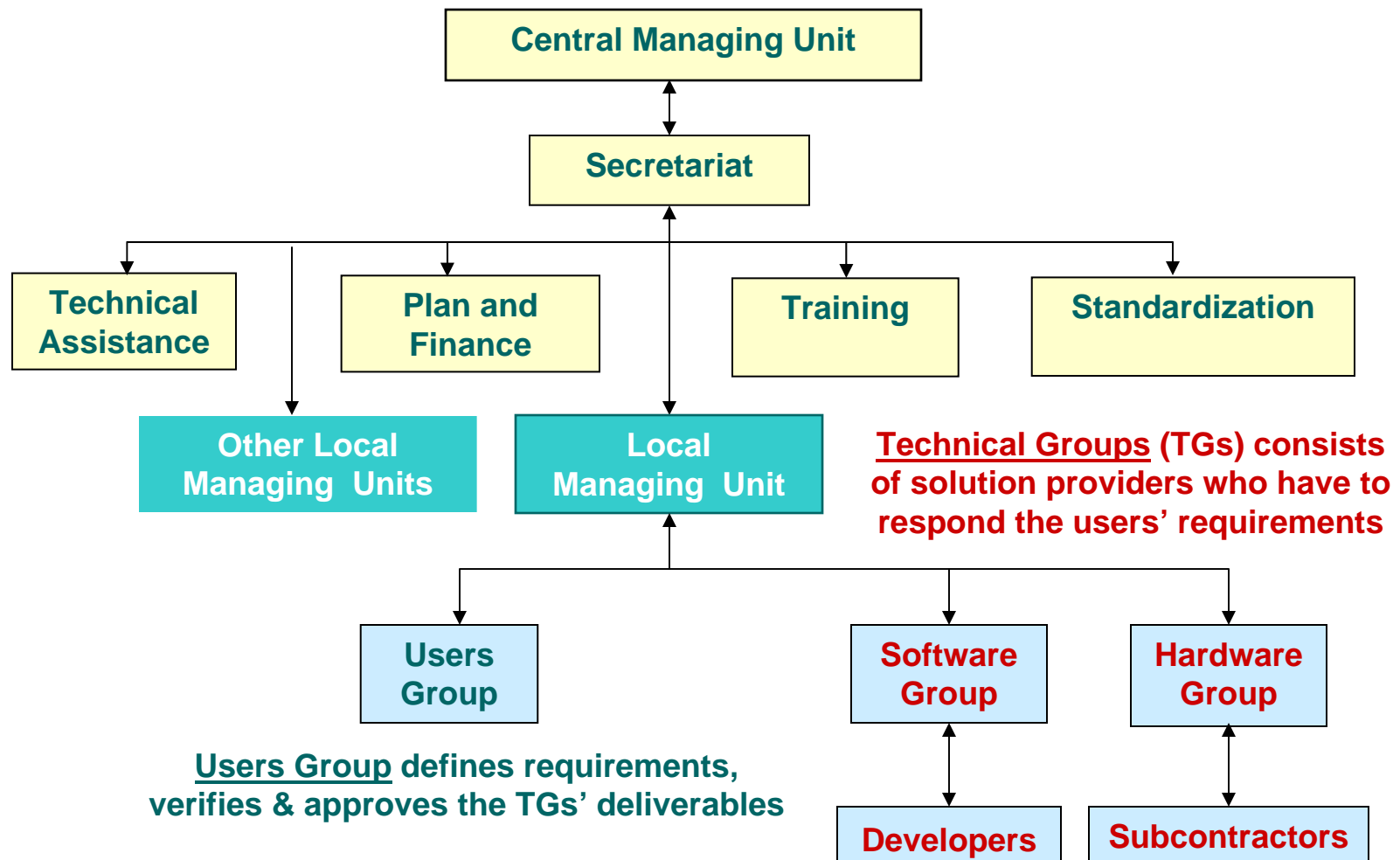
PROJECT ORGANISATION



CENTRAL MANAGING UNIT (CMU)



LOCAL MANAGING UNITS



RELATED LEGISLATION WORK

- In 2005, the Vietnam National Assembly has approved the Electronic Transaction Act and adjusted the Act on Customs.
- There are several proposals of a Decree on Digital Signature, a Decree on e-Commerce and a Bill on Using Information Technology.
- But there is neither law on information nor law on e-government.

PRINCIPLES OF PRIVACY

- **Citizens and businesses should have notice both of the fact that some information is being collected about them and of the purpose for which this information is being collected.**
- **Any governmental information system should give its users some control over the use of data about themselves and to manage the consequences of others' use of this data.**
- **Governmental agencies have to publish their privacy policy and update their list of secrecy.**

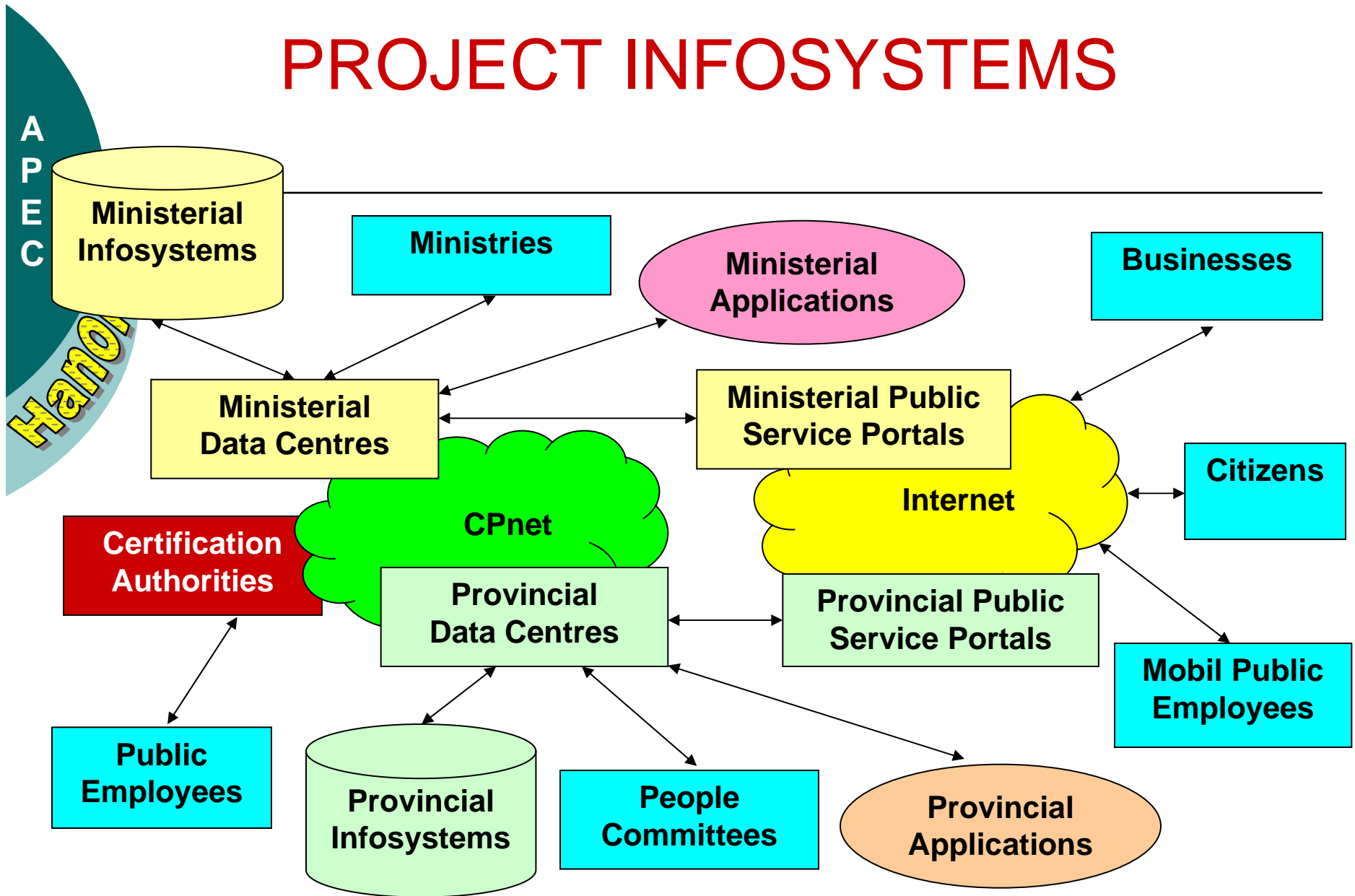
PROJECT PRACTICES

- **The Project Central Managing Unit (CMU) defines and recommends its standards on sharing and using the governmental data.**
- **All CMU's public databases are designed with constraints on information privacy.**
- **Information privacy is about control, fairness and consequences, rather than simply keeping it secret.**

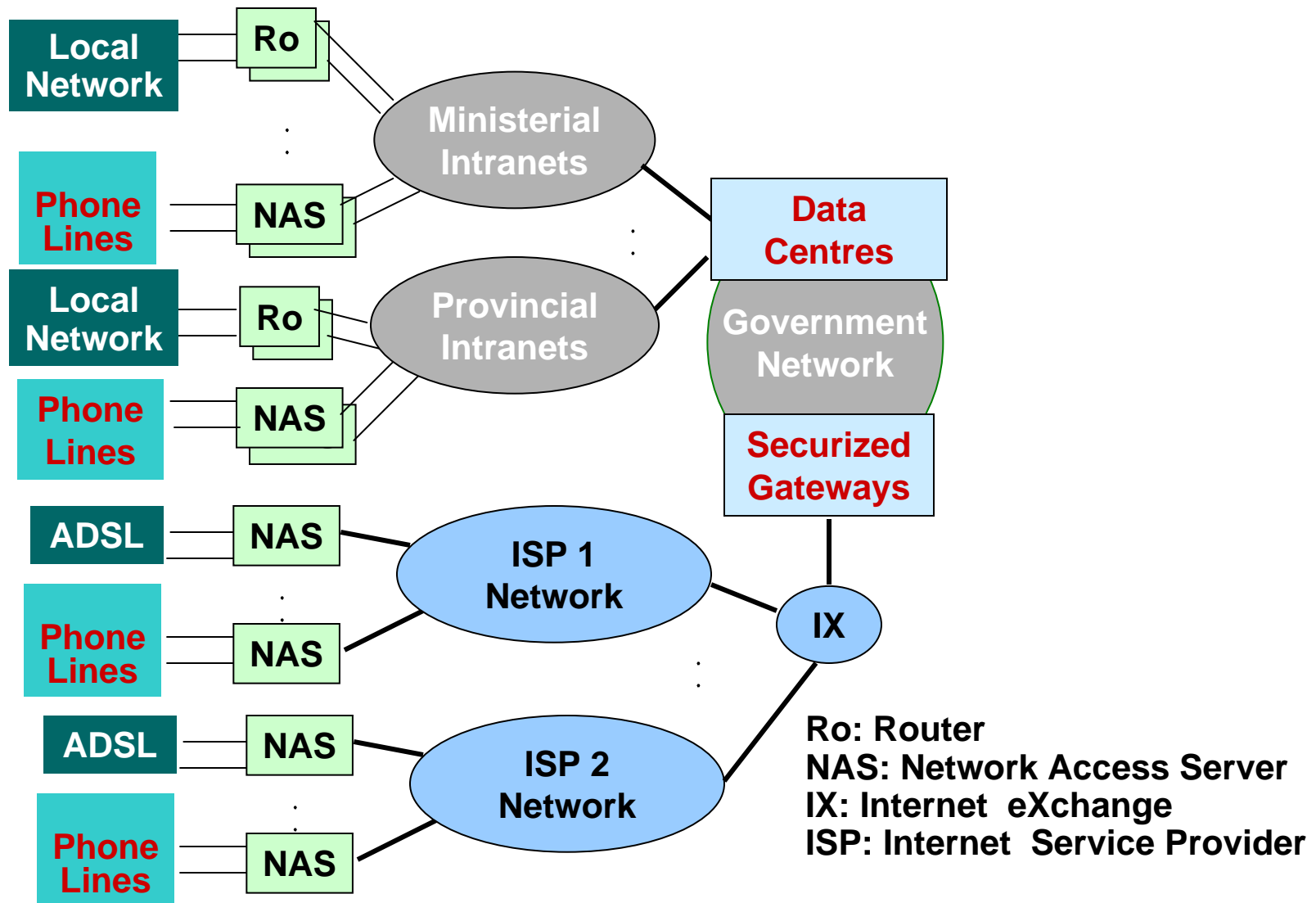
USER PROTECTION

- Each sensible data interchange should be based on a prealable aggrement between its direct participants.
- Information privacy should be protected by separated data acquisition, secure archiving and hierachical access in any governmental databases.
- Information subject-based searches should be used in priority to pattern-based searches.

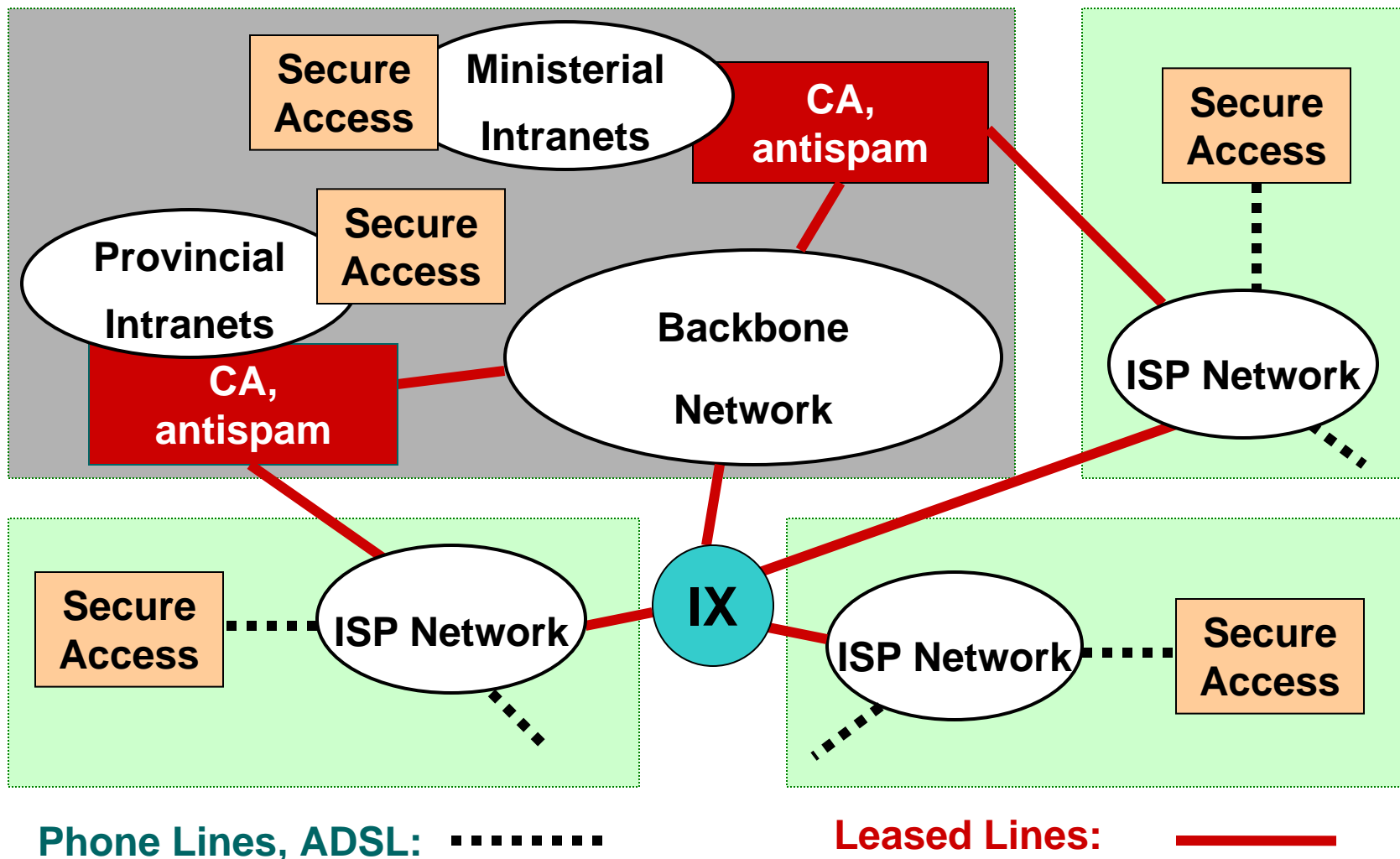
PROJECT INFOSYSTEMS

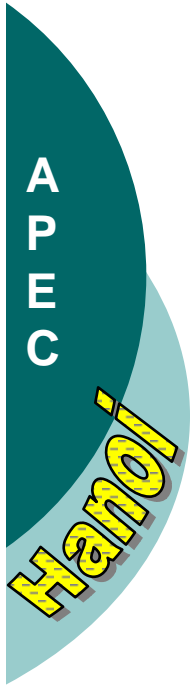


ACCESS TO DATA CENTRES



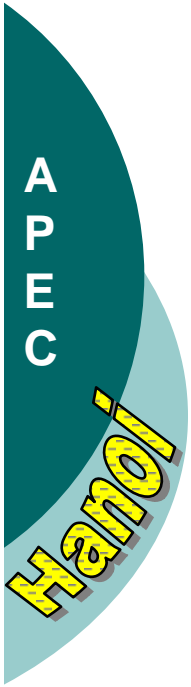
PROJECT NETWORK SECURITY





PHASE 1 OF THE PROJECT

- **Period of Phase 1: 2001-2005**
- **Central Budget: 800 Billion VND**
- **Provincial Budget: 200 Billion VND**
- **Published Documents & Manuals: 23**
- **Trained Public Employees: 67,000**
- **Deployed Infosystems: >500**
- **Portals and Websites: >100**
- **Defined Standards: > 200**
- **Data Centres: 115**



PHASE 2 OF THE PROJECT

- **Period of Phase 2: 2006-2010**
- **Adaptation of the APEC Framework**
- **Plan: to be approved soon**



THANK YOU

Nguyen Chi Cong
Project Consultant
nccong@ifi.edu.vn



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/018

Agenda Item: 17

Experience of Chile in the frame of APEC Privacy Framework

Purpose: Information

Submitted by: Chile



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



Experience of Chile in the frame of APEC Privacy Framework

Alberto Cerda Silva
Legal Advisory of Ministry of Economy of Chile
acerda@economia.cl



right decisions

omnibus law

protect natural person

automated & non-automated data process

public and private sector

principles of personal data protection



right decisions

rights of personal data subject

information - access

rectification - elimination - block

obtain free copies of the registry



good initiatives

decree that establishes practical
standards for the development of
web sites for the Government

good practices code on e-commerce
Chamber of Commerce of Santiago



self-regulation problems

legality
representative
publicity
enforcement



our mistakes

exceptions

some ambiguity

registration system just public organisms

sensible data

any control mechanisms



our mistakes

no automatized decisions about a persona

dispositions to the trans-border
flows of personal data

control authority



work

Government`s Program of
Mrs. Michelle Bachelet



"There is no document of civilization
which is not at the same time a document of barbarism"

Walter Benjamín,
Theses on the Philosophy of History



Experience of Chile in the frame of APEC Privacy Framework

Alberto Cerda Silva
Legal Advisory of Ministry of Economy of Chile
acerda@economia.cl



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/019

Agenda Item: 18

Lesson Learned from APEC Framework Implementation: Indonesia

Purpose: Information
Submitted by: Indonesia



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



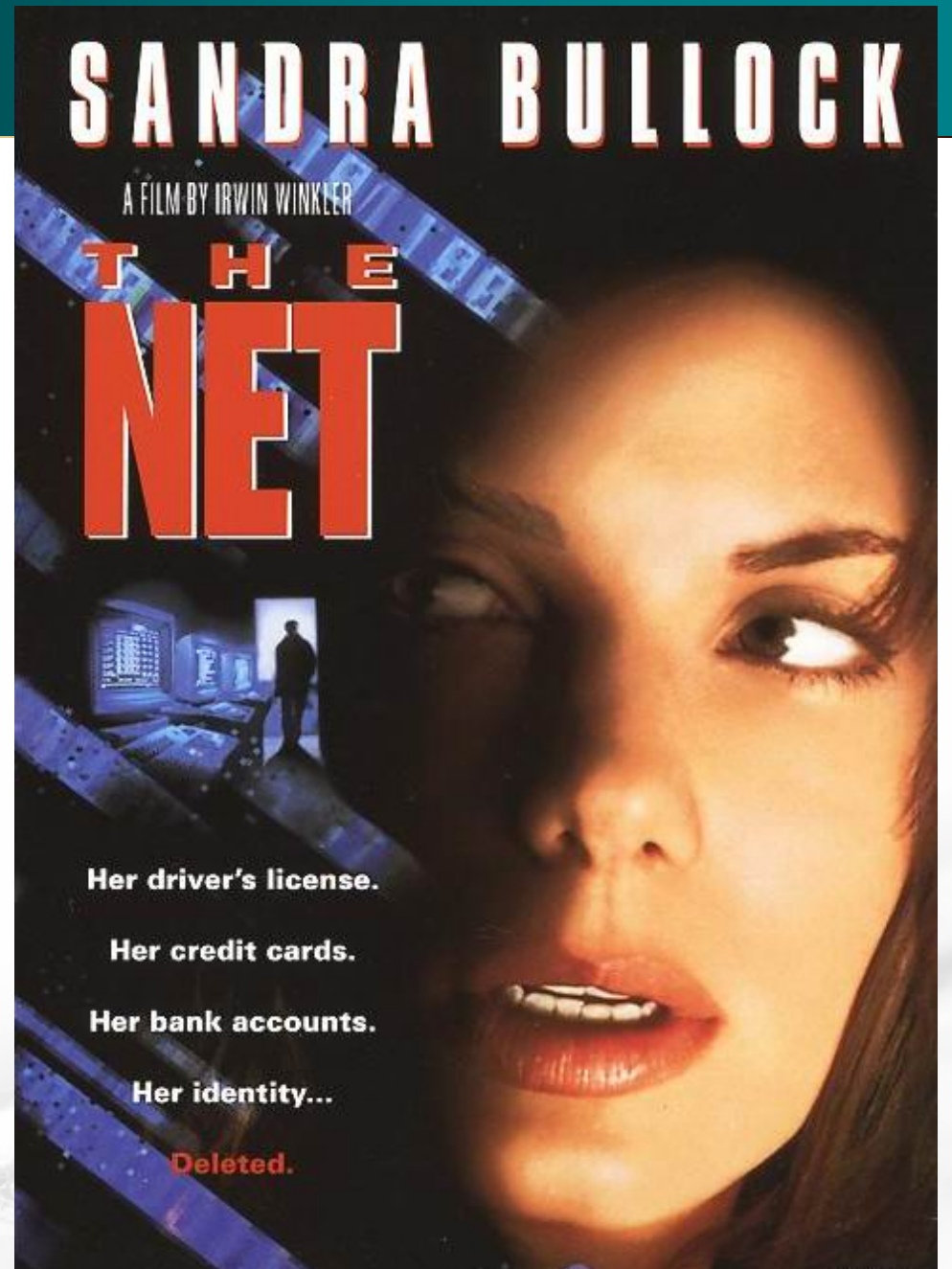
Lesson Learned from APEC Framework Implementation: Indonesia

**APEC Symposium on Information Privacy Protection in
E-Government and E-Commerce**

Horison Hotel, Hanoi, 20-22 February 2006

*Her driver's license.
Her credit cards.
Her bank accounts.
Her identity.*

DELETED





nagging question

- How is it possible?
(a very naive question)
- How are we going to overcome the problem?
- What measures should be taken by individual/organization/economy?
- What initiative has been taken by economies?
- How Indonesia coop with the issue?

Indonesia's Great Challenges

- **The unique characteristics compared to other countries in particular:**

- ❑ Geographically consisting of more than 17,000 islands
- ❑ Uneven distribution of population with more than 224 millions people
- ❑ Diversified cultures with more than 520 ethnic groups and around 300 local languages
- ❑ Newly democracy with current multi-dimensional problems

- **Today Infrastructures (2005):**

- ❑ Telephone line : 9.4 millions (fixed) and 27.9 millions (mobile)
- ❑ Public phone : 382,000 units
- ❑ Internet Penetration : 1,5 millions subscriber and more than 16 millions users
- ❑ Internet Kiosks : 261,000
- ❑ Internet Exchanges (IX) : 3
- ❑ ISP : 140 licensees, 35 operational
- ❑ Radio Broadcasting : 1,400 stations (nation-wide and local)
- ❑ TV Broadcasting : 10 nation-wide networks
- ❑ Pay TV : 4 TV cables, 2 DBS TV



Indonesian National ICT Vision

- *“to bring into reality a modern information society, prosperous and highly competitive, with strong support from ICT*
- *This vision has thoughtful meaning, that is: to bring into reality an Indonesian information society with ethics, morals, and cultural identity that respects traditional aspects of the community; and acting as a force to drive the Indonesian nation towards self-sustainability, a nation that owns her integrity and has the capability to effectively execute each aspect of nation building, democracy, and prosperity*

OVERALL CONDITION

- TELEDENSITY

Major City (11 – 25 %).

Rural (0.2 %).

± 43.022 villages without telephone access
(64.4 % out of 66.778 villages).

Infrastructure :

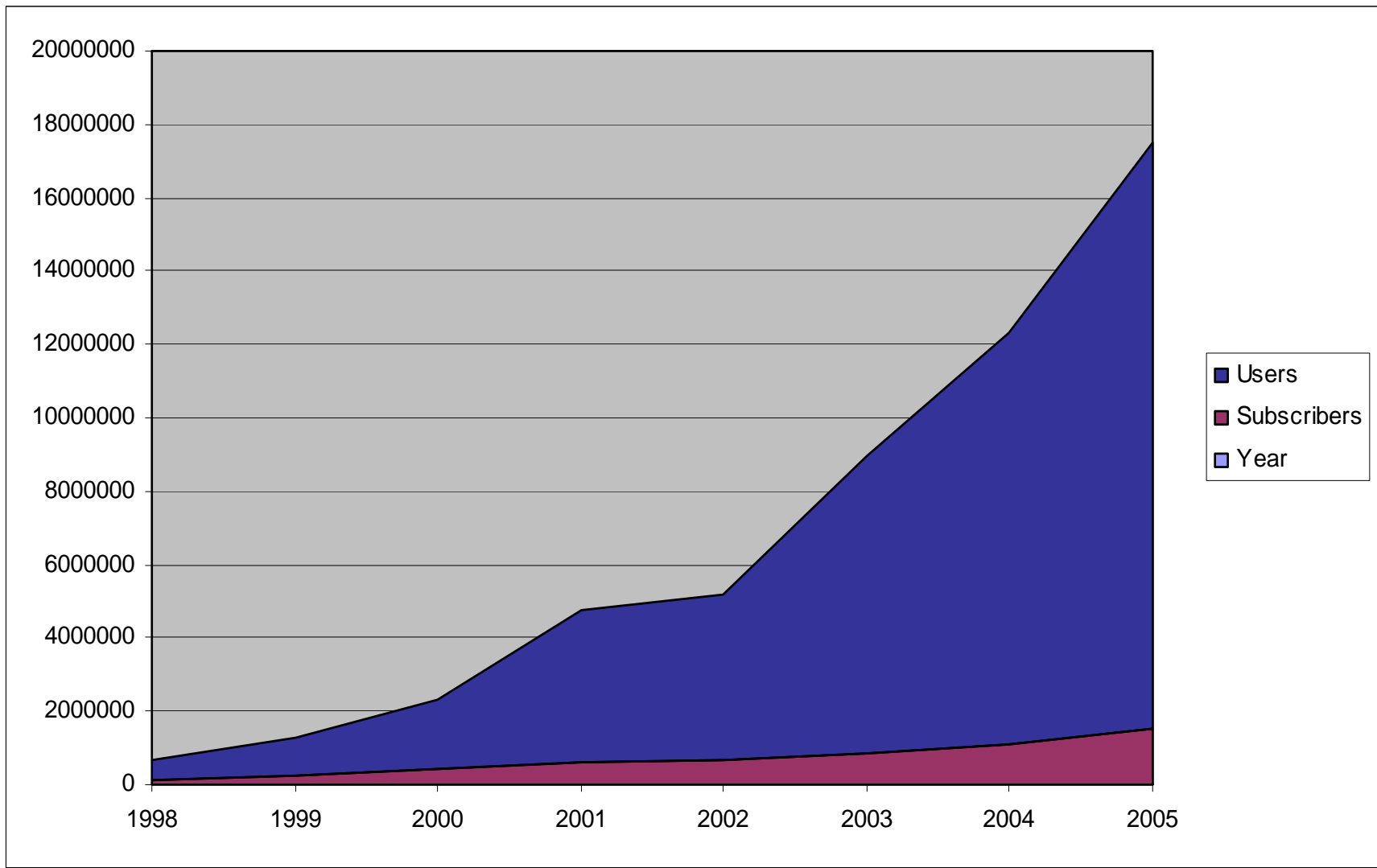
9.4 million fixed line (4.2 %)

27.9 million cell phone (11 %)

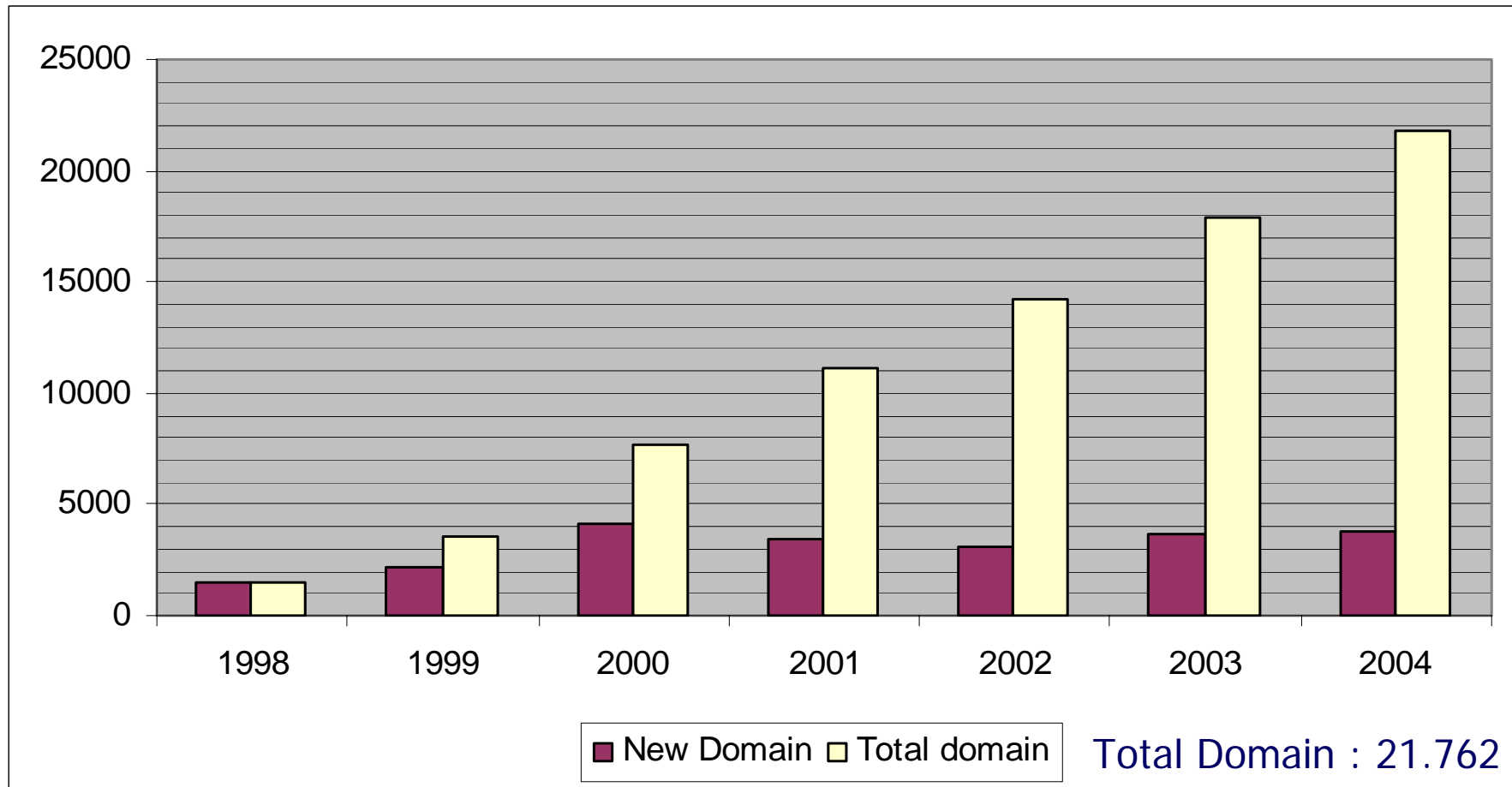
OVERALL CONDITION

- Company Expenditure for Software and Hardware:
US\$20 Million, with 20% annual growth
- B-to-C instead of B-to-B
Advertisement/Promotion
Not Continuous

Growth of Internet Subscribers and Users



WEB DOMAIN



Current report on emergency Report

	Oct-Dec 2002	2003	2004
Spam	135	8.389	3872
Spam Report	0	1.202	6770
Network Incident	44	2.267	1003
Open Proxy	-	1.21	3856
Fraud	4	210	61

Table : Abuse Report APJII

** Until end of 2004 (Non-cumulative calculation)*

Problem

- Security body that involved the whole stakeholders has not established.
- Lack of skilled worker that specialized in security issues.
- Does not have equipment that support network security.

What has been done

- Applied secure on-line transaction standard:
ISO 17799
- Government-Public partnership:
Indonesian Telecommunications Society (1993)
Telecommunication Coordination Team (2003)
- Road show
community, school, local government, etc

ICT Regulatory Update

- Telecommunication Act No. 36/1999
- Broadcasting Act No. 32/2003
- IT and e-Transaction Act being proposed by the Ministry to the Parliament
- The President Decree No. 50/2003 extended the existence of National IT Task Force (TKTI) chaired by Minister of CIT
- Government Decree No. 52/2000 on Telecommunication Operation and No. 53/2000 on Radio Frequency Spectrum
- Several Ministerial Decrees for operational guidance such as Licensing Procedures for telecommunication networks and services (including multimedia).

ICT Regulatory Update (cont.)

- Anti Monopoly and Fair Competition Law No. 5/1999 which provides provisions to encourage best practice in antimonopoly and fair competition business.
- Patent Law No. 14/2001 which was designed to create competition and fairness in business environment.
- Copyright Law No. 19/2002 enacted July 2003 which provides provisions to protect Intellectual Property Right (IPR) including ICT.

ICT Regulatory Update (cont.)

- Broadcasting Act (Law No. 32/2002)

Objectives:

- Stipulate regulation on all related broadcasting activities.
- Mandate to establish a new independent broadcasting commission to control content and code of conduct of broadcasting operators.

ICT Regulatory Update (cont.)

- **Draft of Information Technology and Electronic Transaction Act**

Status: approved by the Government in October 2004 and waiting for ratification by the Parliament.

Objectives:

- A legal umbrella for securing cyber-activities including IT and electronic transactions.

ID-SIRTII

- ID-SIRTII → Indonesia Security Incident Response Team on Indonesia Infrastructure
- It is an initiative from DGPT and Internet Community
- Involve related parties e.g. Police, Attorney General, Central Bank, Associations, Community, related Ministry and the experts.

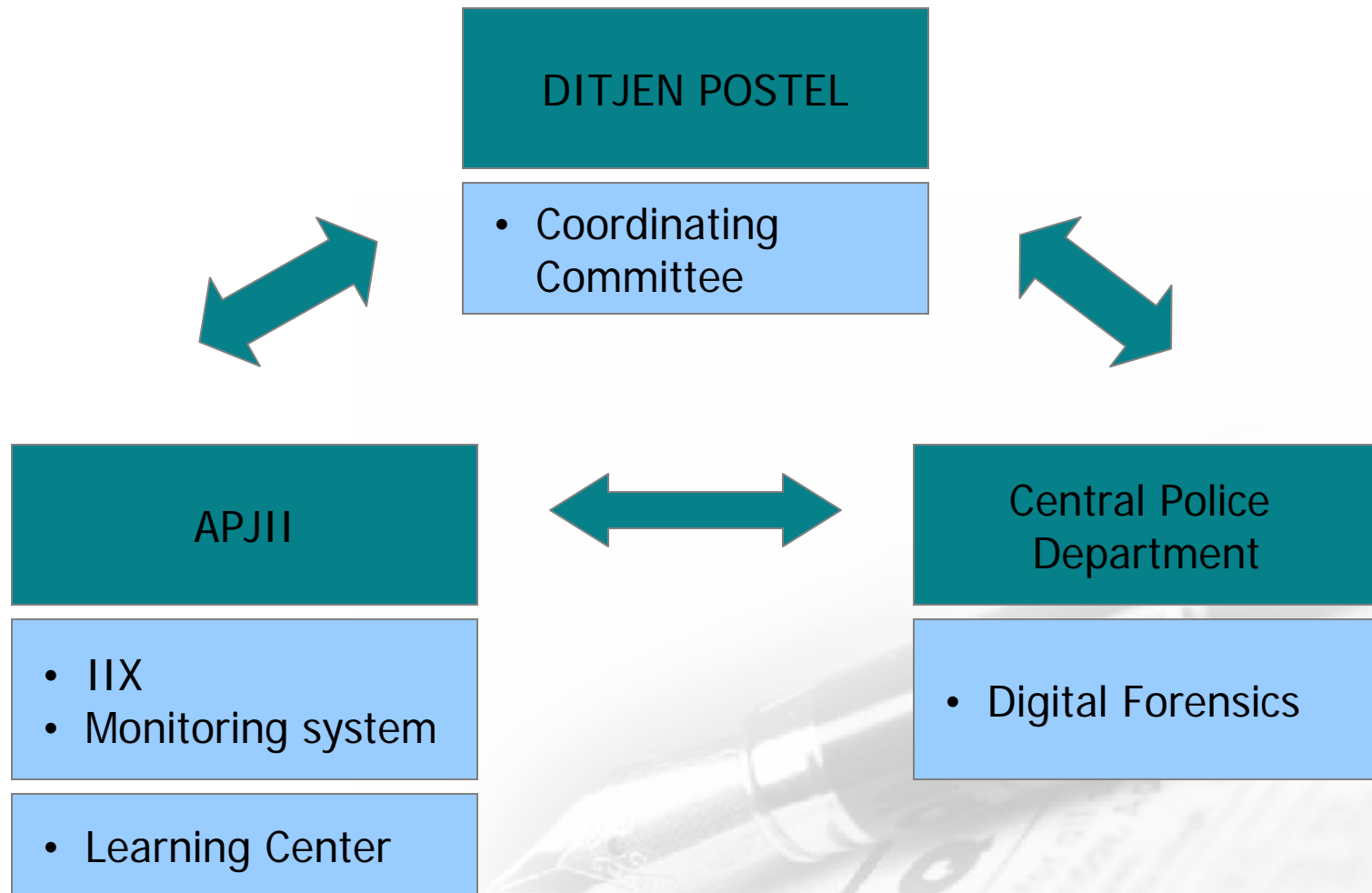
Work Scopes

- To monitor and early detection of internet networks incident in Indonesia.
- To store the evidence of Internet transaction on Secure Data Center.
- To support the availability of Digital Forensic and Digital Evident for law enforcement process.
- To be a Contact Center based on report of security disturbance of internet infrastructure (24/7) from the public.
- To provide services that include lab simulation, training, consultancy, and socialization.

ID-SIRTII Targets

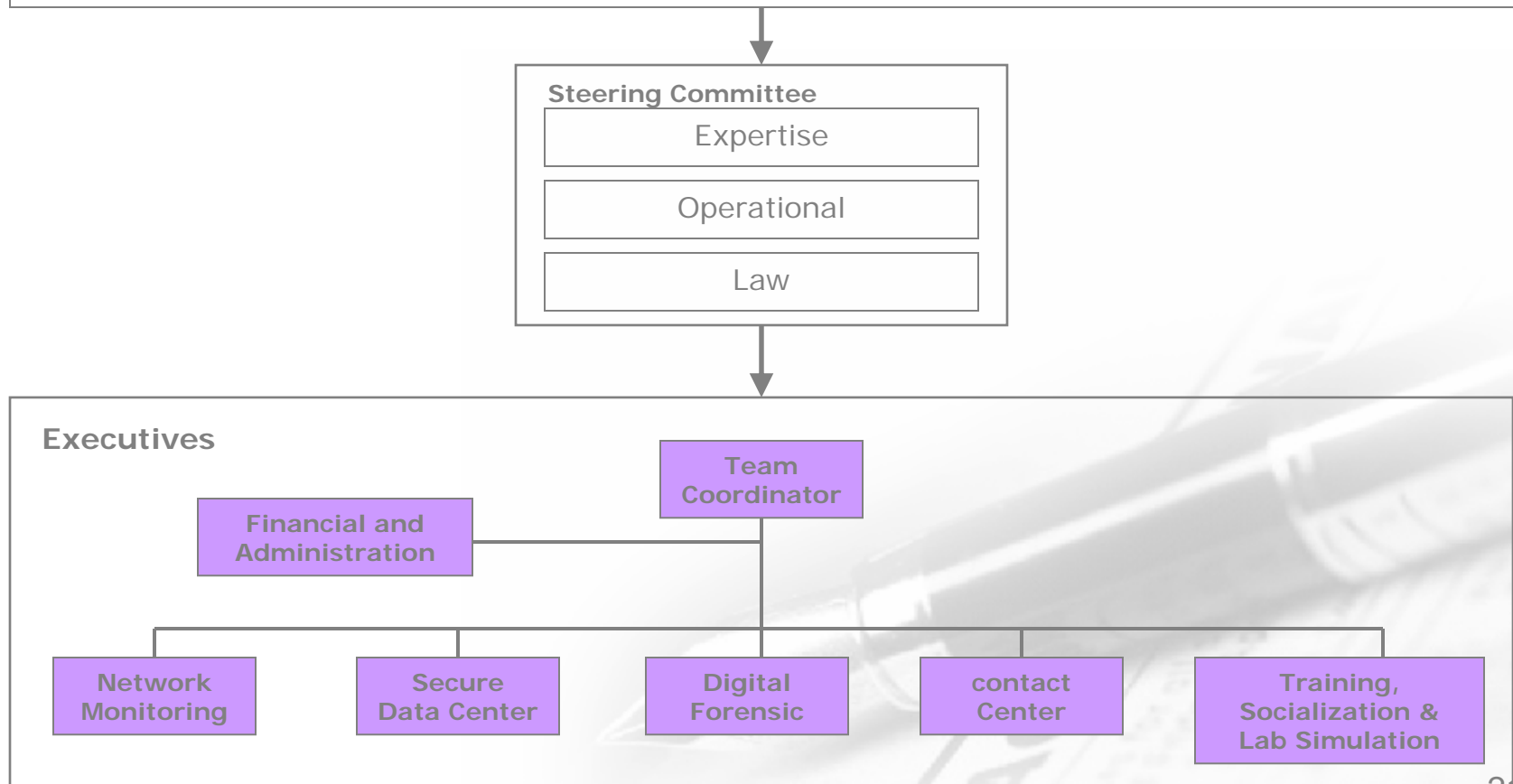
- A creation of safe infrastructure for government application, business, etc.
- The availability of digital evidence in the court so that law can be more enforced.
- Verification of attack and disturbance attempts in internet networks in Indonesia.
- A creation of good coordination with related institution either domestic or overseas to overcome the threat and disturbance and to create environment that supports internet networks.
- Availability of early warning alert.

Present Organization



Future Organization

DIRECTORATE GENERAL OF POST AND TELECOMMUNICATION





"On the Internet, nobody knows you're a dog."

THANK YOU



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/020

Agenda Item: 20

Information Privacy in e-Government at SUNAT - The Challenge

Purpose: Information

Submitted by: Peru

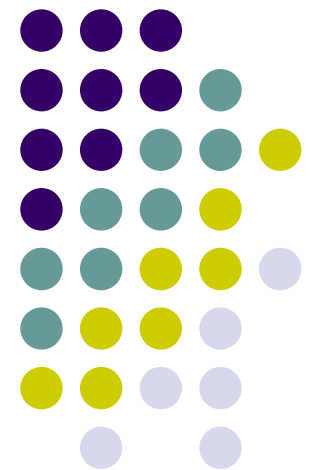


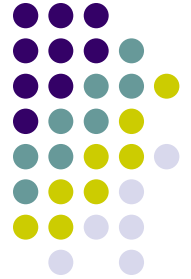
**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Information Privacy in e-Government at SUNAT

Ing. Jorge Irey
jirey@sunat.gob.pe

Technical Support Staff of Internet Platform
SUNAT - PERU

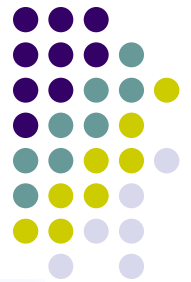


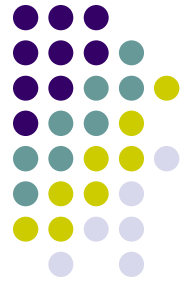


Agenda

- Context
- E-Government projects
- APEC Framework implementation
- Conclusions



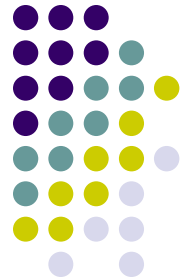




Context

- Peru is actually an economy with 26 million of people and US\$ 67,9 billions of IPB.
- The tax burden is about 14%
- SUNAT is a government agency like the IRS.
- It has presence all over the country and manages tax collections and customs control
- SUNAT is the technology engine of Peruvian State.

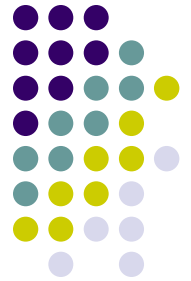




Context (2)

- Information driven at SUNAT has two premises:
 - It's SUNAT's duty to maintain the secret about information, with exceptions under laws.
 - It's taxpayer's right to have it own information send to SUNAT under confidentiality as shows as tax Code and related laws.
- IT master plans identify 3 forms to access information using internet services:
 - Applications with authentication under SSL and SOL passport
 - Applications without authentication, but with validation mechanism
 - Free applications

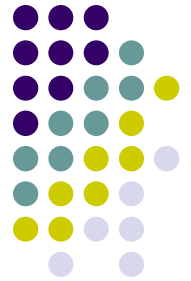




E-Government Projects

- Great web applications:
 - The payment receipts authorization (ADOC award 2005 for best e-practices)
 - The tax form reception and online payment reception
 - The “tele-dispatch” web (Unique Custom Entry Form using web - ADOC award 2005 for best e-practices)
 - The include at master record of tax payers
 - E-notifications
 - E-collections
 - E-bills





APEC framework implementation

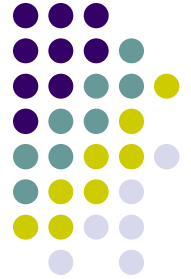
- SUNAT needs to protect taxpayer information due to law regulations.
- The protection was defined in 2000 early with IT development plans for SOL project
- Tax payers subscribes a “legal” contract within SUNAT to use the SOL services at web page.
- Tax payers not provide us their user logon or password when he/she has in problems
- All information collected is the input for other business processes along the SUNAT





APEC framework implementation (2)

- SUNAT must be guarantee the assurance, quality and timeline of the information.
- SUNAT has a special office to plans and control all the related with information security policies.
- SUNAT implemented some procedures using electronic forms to query and modify information using internet
- SUNAT doesn't publish any information that let any people to identify the taxpayer. All information in globalized.



Conclusions

- The privacy is based on legal regulations
- The technology is not all. There are many hackers
- All government agencies don't have the same level of technology adoption.
- There are some implications when information collected by government agencies is transferred to private organizations due to regulations.





Thank you !

SUNAT – Superintendencia Nacional de
Administración Tributaria

Lima – PERU

<http://www.sunat.gob.pe>

<http://www.aduanet.gob.pe>





Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/021

Agenda Item: 20

Information Privacy in e-Government at SUNAT - The Challenge

Purpose: Information

Submitted by: Peru



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Information privacy in e-Government at SUNAT - The Challenge -

I. Context

Peru, the Inka's country is located at South America¹. It is actually a stable economy in expansion process which has on about 26 million of peoples and IPB on about US\$ 67,9 billions of dollars. At this context, the tax burden reached 14% of IPB.

The SUNAT (Superintendencia Nacional de Administración Tributaria) is a government agency like the IRS in the USA. It has presence all over the country and its responsible for internal tax collection and customs control. At country level, the SUNAT is one of the technology engines of Peruvian State.

The information driving at SUNAT has been always based on two important premises:

- It's SUNAT's duty to maintain the secret about information, with exception of cases under law.
- It's a taxpayer's right to have it own information sended to SUNAT under confidentiality as shown as Tax code and related laws.

Before the Internet expansion, the information has been stored in internal databases at computer centers of SUNAT. The access to this information may be of two forms: using software applications developed for specific requirements of end-users and using direct access like the SQL by the end-users. Both cases had certain audit levels to prevent malicious uses of data. The taxpayers and external organizations don't have any access to view the data. This situation was the extreme of privacy information protection.

With the expansion of Internet, the demand for information was in growth. So, many external organizations claims for access to some information like the taxpayers master records. Here, appeared the problem to determinate which information may be view by the external end users without violated the secret principles and related laws.

Plus, appeared related themes with the information security of information uploaded or downloaded from internet which risk factors was recognizes and incorporated to IT master plans for future developments.

¹ You can know more about Peru at <http://www.peru.info/peru.asp>

As this way, one of the first IT master plans classified the information access published in the Internet within 3 forms with the objective (in mind) to assurance the data security:

- Applications with authentication under SSL and SOL passport.
- Applications without authentication, but with validation mechanism. In this scenery only the information owner has the necessary keys to access it.
- Free Applications.

II. e-Government projects

For the finally of the last decade, SUNAT had presence in Internet with querying applications. These applications were mainly queries to master record of taxpayers and tax forms stored at internal databases.

At this point, a strategic plan was written. The main idea was to deliver electronic services based on seven great web applications as follows:

- The payment receipts authorization
- The tax form and online payment reception
- "Tele dispatch" web (Unique Custom Entry Form using Web)
- The include at master record of tax payers
- E-Notifications
- E-collections
- E-bills

In all cases, the kick-off of each project must be based on legal regulations.

The first step to legalize the use of Internet transactions was with the SOL password. This was a legal regulation to determine the rights and duties of taxpayers and responsibilities of SUNAT to provide a secure environment under SSL for protect the communications between the client PC and the SUNAT server. Actually we have on about 950,000 SOL passwords and 3 million of tax payers registered at master records.

The project related to payments receipts authorization was an ADOC winner award due to best e-practices last year.

The project related to tax form and online payment reception is one of the most important project due to the process of capture income, costs and other information about each individual tax payer. This information travels the Internet under SSL and protected by cryptographic and hashing algorithms like RC4 or MD5.

All the information is stored in internal databases protected by hardware devices like firewalls, intrusion detectors and audit mechanism owned by each database.

Since 1996 SUNAT has the computer's subsystem named as "Teledespacho", which allows the importers to transmit electronically their Unique Customs Entry Form (DUA). This system, very innovative in the past, takes advantage of the potentialities of the email, the commuted communication and the transmission service supplied by private information's transport networks. However, according the technological advance and the potentialities that the internet offers at the moment, it was considered to work in the development of a new channel to offer the service of presentation of the DUA, it is the "Teledespacho WEB".

As parallel task, the SUNAT has been implement a remote access platform to facilitate the work of custom officers and internal revenue workers. This platform at first steps is based on WAP protocol and lets them to validate personal data, photo, signature of any person (tax payer or not) during customs operatives all over the country.

III. APEC frameworks implementation

Although the APEC's information privacy framework is oriented to apply to information about natural persons, under the responsibilities of SUNAT it was aim to apply to legal persons too because the imperative needs to protect tax payer information due to law regulations.

During the project SOL (SUNAT Operaciones en Linea) implementation, the advances over APEC's framework are as follows:

- a) **Preventing Harm:** All information storage in SUNAT's databases is protected by law. The legal regulations establish exceptions and mechanisms of responsibility for officers and workers. The software applications has been designed for operate under user roles. A role may view and work only with information needed to accomplish the tasks assigned.
- b) **Notice:** The taxpayer subscribes a "legal" contract within the SUNAT. This contract specifies rights and duties for working under SOL section of web page². Plus, the SUNAT processes a tracking event on web server but not using cookies or spy ware software. It's only an access log processing for statistics effects.

Neither web page has an advertise about the information recopilation nor privacy policy.

² You can reach this at <http://www.sunat.gob.pe> please locate the section "Operaciones en Linea"

The information collected won't sell to anybody. Nevertheless there are many cooperation acts with external entities. For example, for entities named "Centrales de Riesgo", the SUNAT provide information about master record of taxpayers, taxpayers with debts or taxpayers without having a tax declaration.

- c) **Collection Limitation:** All taxpayers has been instructed to not provide us their user logon or password to SOL environment when he/she has in trouble and need to call the help-desk phone.

Another example is in tax form payment process: the SUNAT can't store the bank account numbers.

- d) **Uses of Personal information:** Under this principle, all information collected is the input for other business processes along the SUNAT. The information collected may be originated at:
 - The include at master registry of tax payers.
 - The tax form presentation.
 - The informative form presentation.
 - The information exchange with external entities.
- e) **Integrity of personal information:** Under this principle, the SUNAT must be forced to guarantee the assurance, quality and timeline of the information. This is done regularly by any government agency but in may cases there are weakness by the great amount of data, so all the data can't be keep up-to-date.
 - The information is periodically updated with tax forms and informational forms.
 - For the master record of taxpayers, it is important and critic to have data up to date for purposes of notifications and communications. Other data like the phone, fax or e-mail may be phased out over the time.
- f) **Security Safeguards:** The SUNAT has a special office to plans and control all the related with information security policies. Periodically it reviews the policies and procedures to access to hardware, networks, and databases as parts of IT platform all over the country.

- g) **Access and correction:** It was necessary to implement some procedures using electronic forms to query and modify the information. Two applications were developed: “Trámites Múltiples” and “Modificación de Declaraciones”. These procedures are regulated by the corresponding laws.
- h) **Accountability:** The SUNAT doesn't publish any information or statistic that let any people to identify the tax payer (natural or legal person) according to tax code. In the practice, when the information is exchanged with external entities, the control over the destiny or use of the information is forgotten.

IV. Conclusions

The privacy framework implementation at its core is based on legal regulations.

The actual level of technology let us to protect the information privacy in government agencies and private enterprises, nevertheless none technology has 100% of effectiveness. Always has the remote possibility of hacker attacks inside or outside the organization.

All government agencies don't have the same level of technology adoption or the same budget assigned to guarantee the adequate levels of information privacy protection.

In most of cases for government agencies, the information privacy protection is regulated by the law, nevertheless in private organizations this regulations is not all clear: the example case is the sell of client databases in financial sectors to offer products and banking services.

There are some implications when information collected by government agencies is under treated with external entities.



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/022

Agenda Item: 21

Implementing the APEC Privacy Framework to Promote E-Services in the Philippines

Purpose: Information
Submitted by: Philippines



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Implementing the APEC Privacy Framework to Promote E-Services in the Philippines

MARIA LOURDES A. YAPTINCHAY
Department of Trade and Industry
Philippines

INFORMATION PRIVACY PROTECTION IN THE PHILIPPINES

**The right to privacy is a basic right
given to any Filipino under the Bill
of Rights of the Philippine
Constitution**

Information Privacy Protection in the Philippines

- **There is no specific law on privacy**
- **Right to privacy provisions are embedded in some existing laws, such as:**
 - **Law on Secrecy of Bank Deposits**
 - **Access Devices Regulation Act**
 - **Social Security System Act**
 - **Laws on AIDS Prevention and Control; Assistance and Protection for Rape Victims; Establishment of Family Courts**
 - **E-Commerce Act**

IMPLEMENTING THE APEC PRIVACY FRAMEWORK TO PROMOTE E-SERVICES IN THE PHILIPPINES

- **Our goal: the Philippines as Asia's e-Services Hub**
- **Priority areas:**
 - **Animation**
 - **Back-office operations (F&A)**
 - **Contact centers**
 - **Engineering design**
 - **Medical transcription**
 - **Software development**
- **What we need: statutory and regulatory guidelines to protect information privacy**

Implementing the APEC Privacy Framework ...

- Existing modes of protecting personal data:

market-driven contractual arrangements
and codes of practice

Implementing the APEC Privacy Framework ...

- **Proposal to ensure protection of information privacy (short-term):**

Guidelines for the Protection of Personal Data in Information and Communications System in the Private Sector (Draft)

- **Voluntary accreditation of Data Protection Certifiers**
- **Penalties for certain acts and violations**
- **Privacy complaints mechanism**

Implementing the APEC Privacy Framework ...

- **Proposal to ensure protection of information privacy (long-term):**

Legislation to Regulate the Processing of Information Relating to Individuals, including the Obtaining, Holding, Use or Disclosure of Such Information (Draft)

- **Processing of Personal Data**
- **Rights of the Data Subject**
- **Registration of Personal Data Processing System**
- **Security of Data**
- **Transfer of Personal Data**
- **Monitoring and Enforcement / creation of the National Data Protection Commission**
- **Penal Provisions**

Thank you.



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/023

Agenda Item: 22

The Philippine Experience in Data Privacy Protection

Purpose: Information
Submitted by: Philippines



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

The Philippine Experience in Data Privacy Protection

Rosemarie S. Ramos

Research Assistant

*Office of the Undersecretary for International
Economic Relations*

Department of Foreign Affairs

Why is data privacy important to the Philippines?

- E-Government: Government is keen on delivering its services online, thus it is important to ensure privacy of users.
- IT-enabled services exports (i.e., contact centers, medical transcription, financial BPOs) was estimated to have generated US\$ 1.08 Billion in revenues.

Legal Environment

"Right to privacy is a Basic Right given to any Filipino."

- *There is no general data protection law but there is a recognized right of privacy in civil law*
- **Philippine Constitution's Bill of Rights**
 - Sec. 2: "The right of the people to be secure in their persons, houses, papers...."
 - Sec. 3: "(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law."

Legal Environment

- Presidential Decree No. 1718
- Law on Secrecy of Bank Deposits (R.A. 1405, as amended)
- Anti-Wire Tapping Act (Republic Act No. 4200)
- Access Devices Regulation Act of 1998
- E-Commerce Law of the Philippines

Legal Environment

E-Commerce Law of the Philippines (R.A. 8792)

- Legally acknowledges electronic documents and transactions, and defines what is lawful for commercial and non-commercial purposes
- Contains provisions on privacy security and provides for penalties on computer hacking, introduction of viruses and piracy of copyright works

Legal Environment

Other Issues

- Mobile Phone short message scams and spams
- Push marketing
- * Scammers have pocketed an estimated US\$100,000 from text scams in 2003

Lessons Learned from the Development of an APEC Privacy Framework

- Provides framework for the development of a more comprehensive and responsive Philippine data privacy law.
- Underscores the need for a strong partnership between the government, business sector, and civil society to formulate a formidable and feasible legal framework for data privacy

END OF PRESENTATION



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/024

Agenda Item: 23

International IT Co-Operation

Purpose: Information
Submitted by: Russia




**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**



Russian Information Technology Association

International IT Co-Operation

Natalia Makarycheva
Director of International projects

R  **TA** is authorized by
Ministry for Economic development and
Trade of the Russian Federation
to represent RUSSIA in international events
in the field of Information Technologies

As part of this activities **R**  **TA** cooperates
with APEC



RH TA unites over 500 major Russian IT and Hi-Tech companies with activities in the fields of:


- Manufacturing of computer and Hi-Tech equipment
- Software Development
- System Integration
- Information Security
- Networks and Telecommunications
- Bio-Technology



RHATA members:

ADE	Non-governmental Association of IT market participants
Aladdin	The most famous company dealing with Security Solutions
SIRIUS	Non-governmental Association of System integrators
ROCIT	Public centre of Internet Technologies
IOU	Public association of Russian ISP (Internet Service Providing)
Formoza Group	№1 Russian computer manufacturer
CBOSS	The largest Russian software developer
ISA	Public organization of Russian Information Security agents
International fund of biotechnology	Russian leading organization in field of protection of health of the citizens and environment



R**TA** was created for contributing to success and prosperity of the Russian segment in IT and Hi-Tech market by solving it's most outstanding problems, therefore helping integrate Russia into the world community.

As part of this **R****TA** promotes Russian IT and Hi-Tech companies on foreign markets and in international projects



R^hTA major activities:

International activity - external economic links and coordination of international organizations' activities

Participation in National programs - contributing to development of national wide programs, improvement of cooperation between business and government

Creating IT business environment – coordination with all parties interested in IT and Hi-Tech industry



R**TA key technologies:**

Information Technologies

- Computer design and manufacturing
- Full range of ERP/MRP II software and consulting
- Business Intelligence Systems
- Full-scale Data Warehouses
- Networks LAN/WAN
- Information Security

Biotechnologies

- Water purification systems
- Biosynthesis Technologies



R  TA participates in National
governmental and public programs
concerning e-Community

Burning Information security issue for
e-Community today -
The balance between
Transparency and Privacy



R  TA calls all parties interested in
Information Security for interaction and
collaboration with Russian IT Community

**Our scope of activity and authority gives us
the opportunity to actualize wide range of
events (including international)**





Russian Information Technology Association

Thank you

Visit us at www.RitaRussia.ru

makarycheva@parus.ru

makarycheva@ritarussia.ru

Phone: +7 (495)797-89-90 (ext.318)



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/025

Agenda Item: 24

Overview of E-commerce Protection Technologies

Purpose: Information

Submitted by: Russia



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

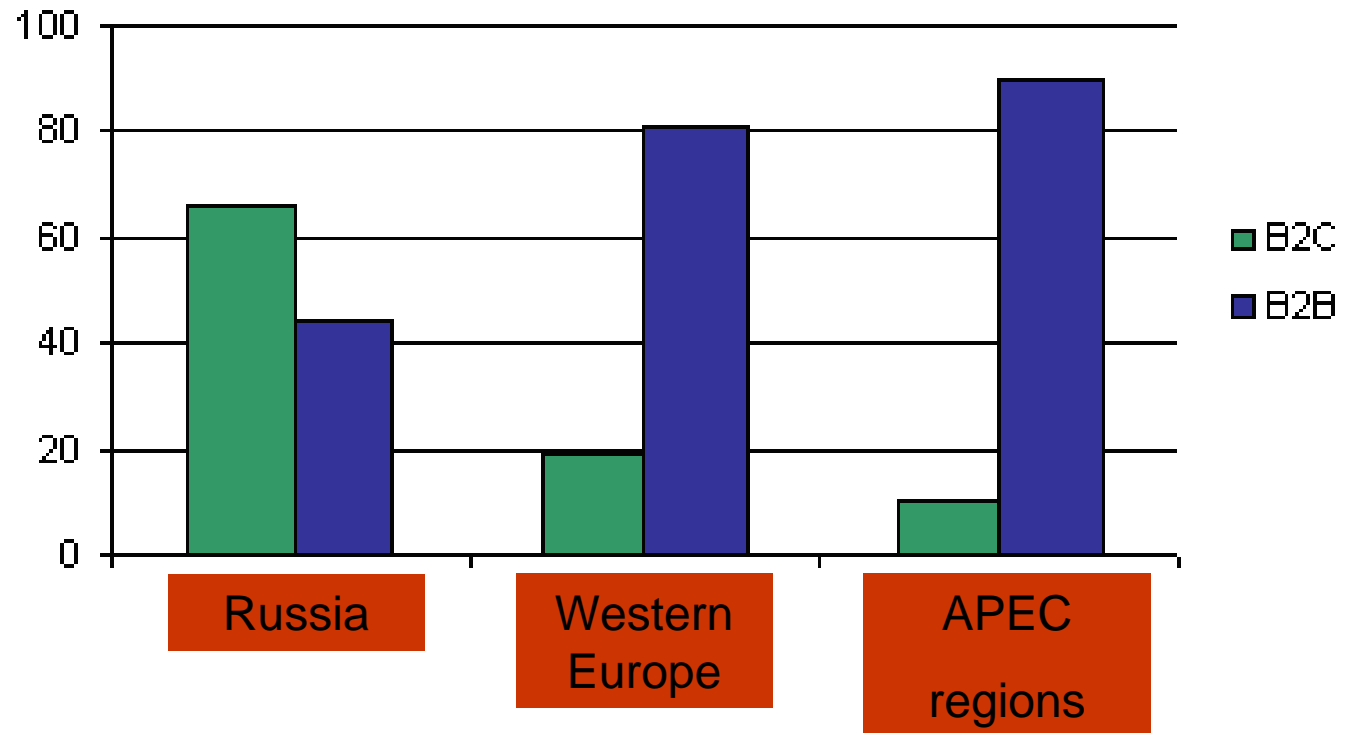
Overview of E-commerce Protection Technologies

Alexey Sabanov, Aladdin (Russia)

Contents

- Brief market analyze
- Trust Problems of E-commerce
- Identification and Authentication
- Privacy Access Control
- Hardware Authentication Devices
- Overview of Modern Protection Technologies

E- commerce market



CNews Analitics, 2004

Russia B2B market

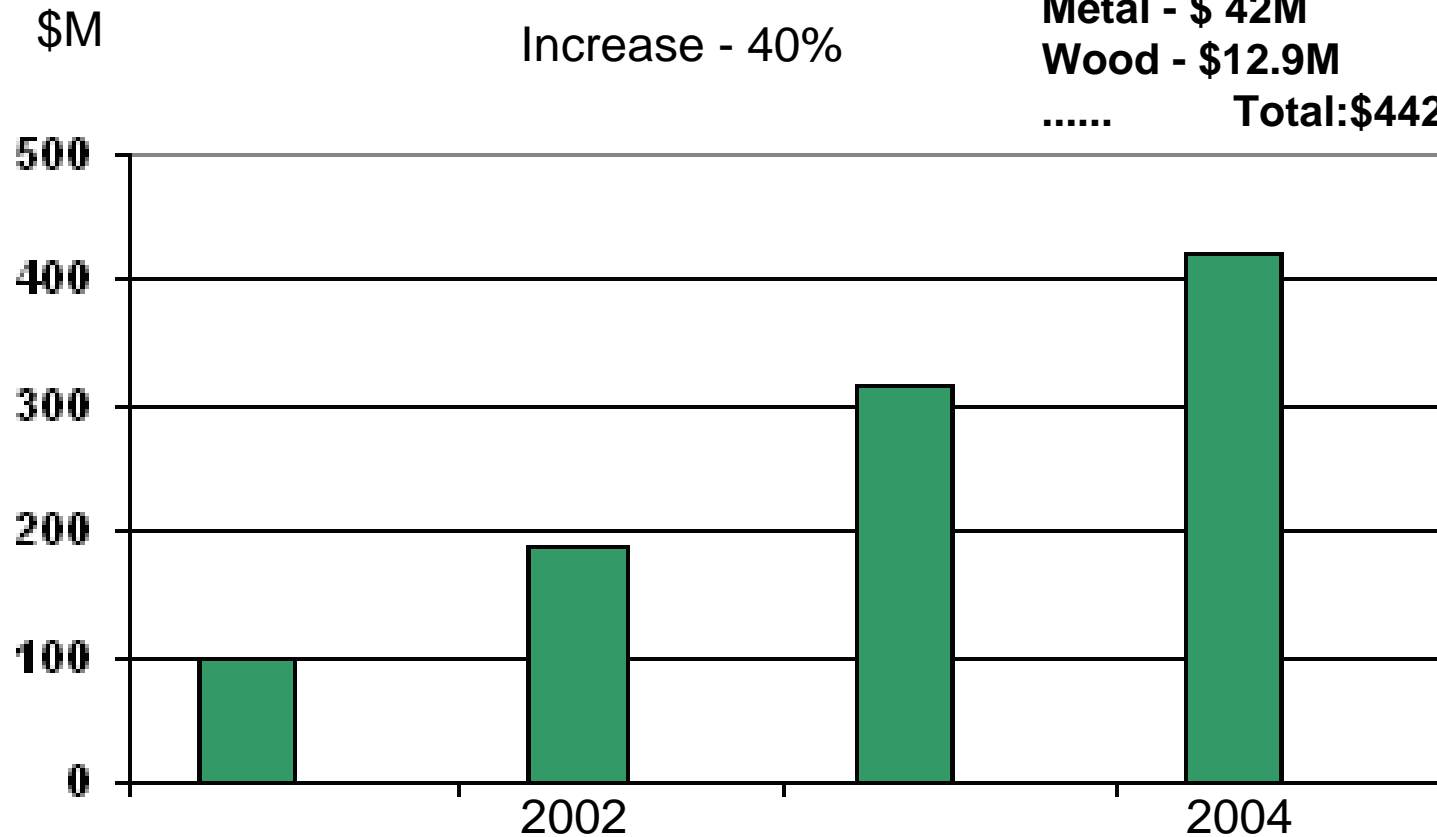
Energy - \$348.2M

Universal – \$32,6 M

Metal - \$ 42M

Wood - \$12.9M

..... Total:\$442M



www.cnews.ru: NAUET (HAYET), 2004

Topicality: financial loss

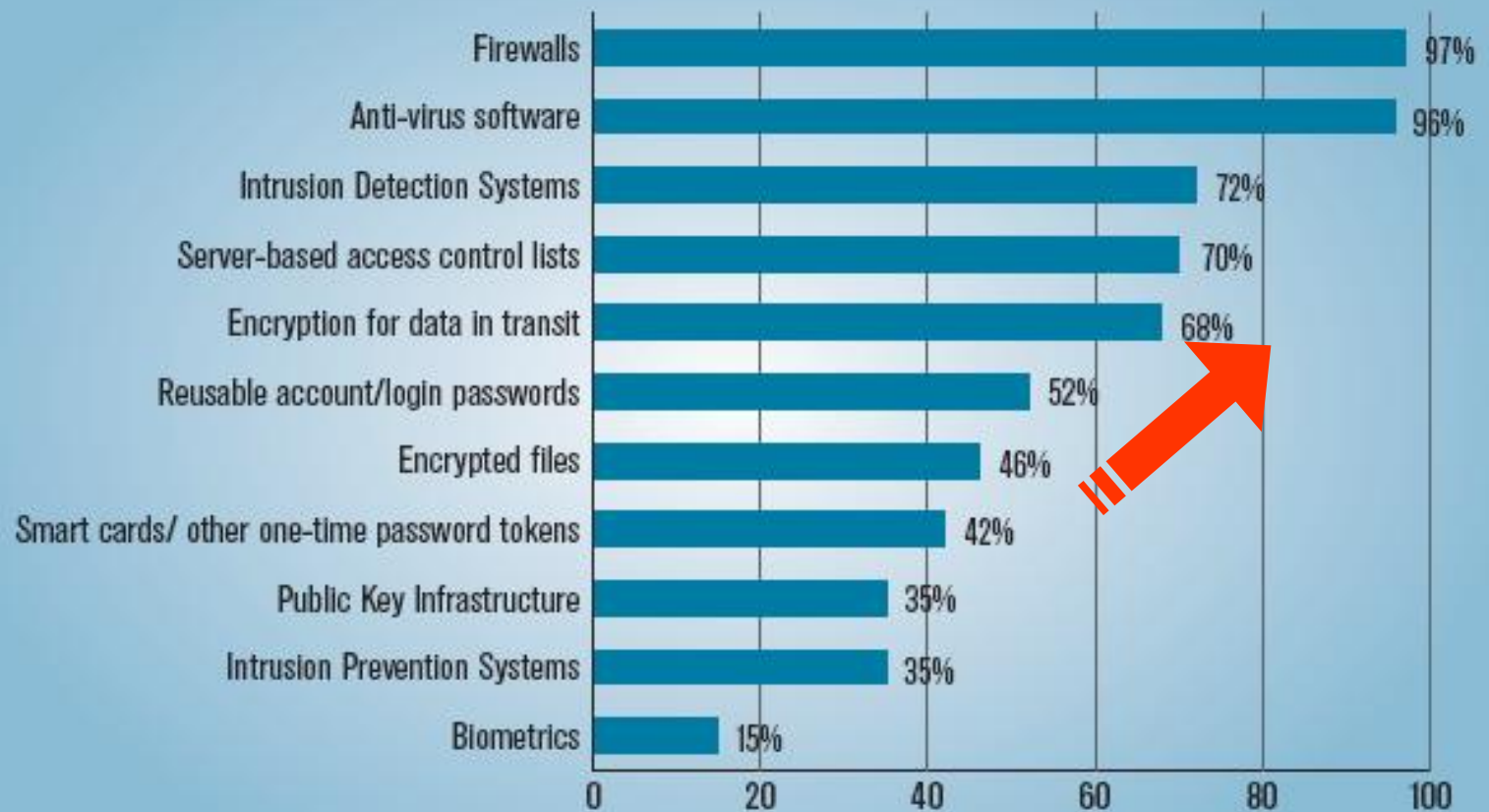


Total Losses for 2005 were \$130,104,542

CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 639 Respondents

Security Solutions Used



CSI/FBI 2005 Computer Crime and Security Survey
Source: Computer Security Institute

2005: 687 Respondents

Trust Problems of E-commerce

- Guarantee of confidentiality (number of a credit card, a delivery date of the goods, the address,...)
- Guarantee of data integrity
- Sufficient level for controlling of operation participants:
 - The seller should be assured that the buyer will not refuse purchase and in solvency of the buyer
 - The bank-emitter should check up the seller before realization of his requirement for payment of purchase
 - The buyer should be assured that seller is real, instead of false

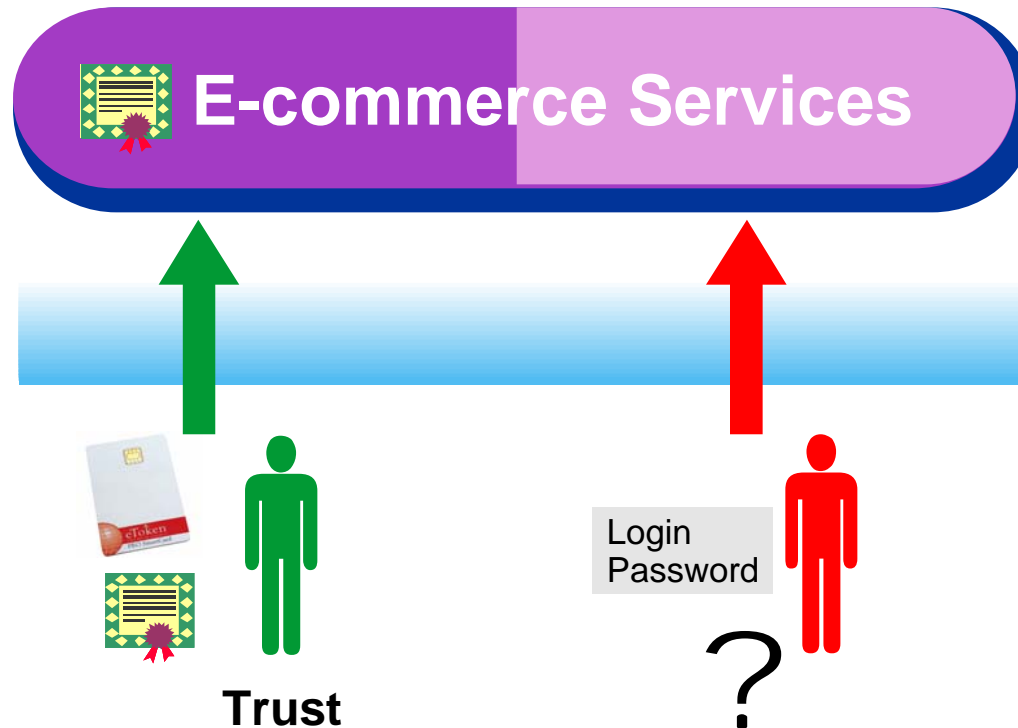
Some Trust Problems of E-commerce: Security weaknesses

- sensitive financial details for online paying ;
- trade secrets and other confidential information;
- privacy of e-commerce actions:
 - pay bills,
 - trade stocks and shares,
 - file our income tax returns,
 - conduct legally transactions;
 - vote in government elections;
 - ...

PKI Trusted Services

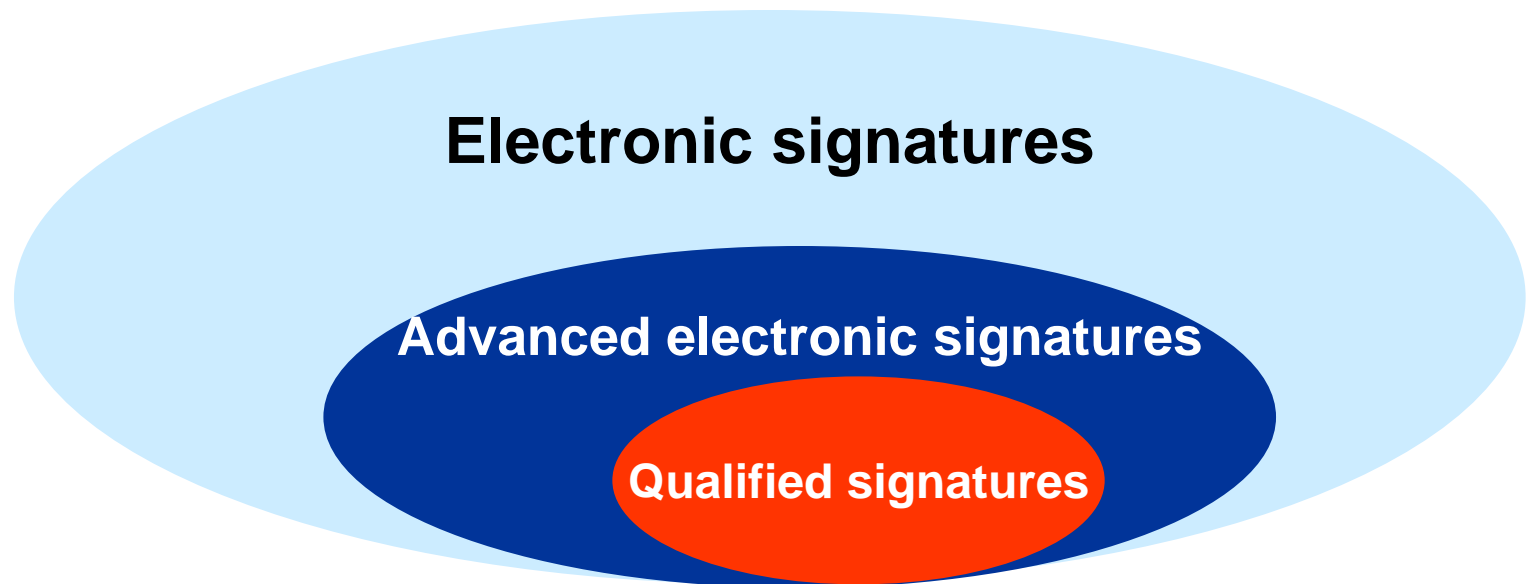
- Authentication,
- Access control,
- Trust internet - banking services,
- Assured privacy data delivery,
- Encryption,
- E-signature.

The role of Authentication



Use of strong authentication may be one of the way for trust users to e-commerce

E-Signatures Types



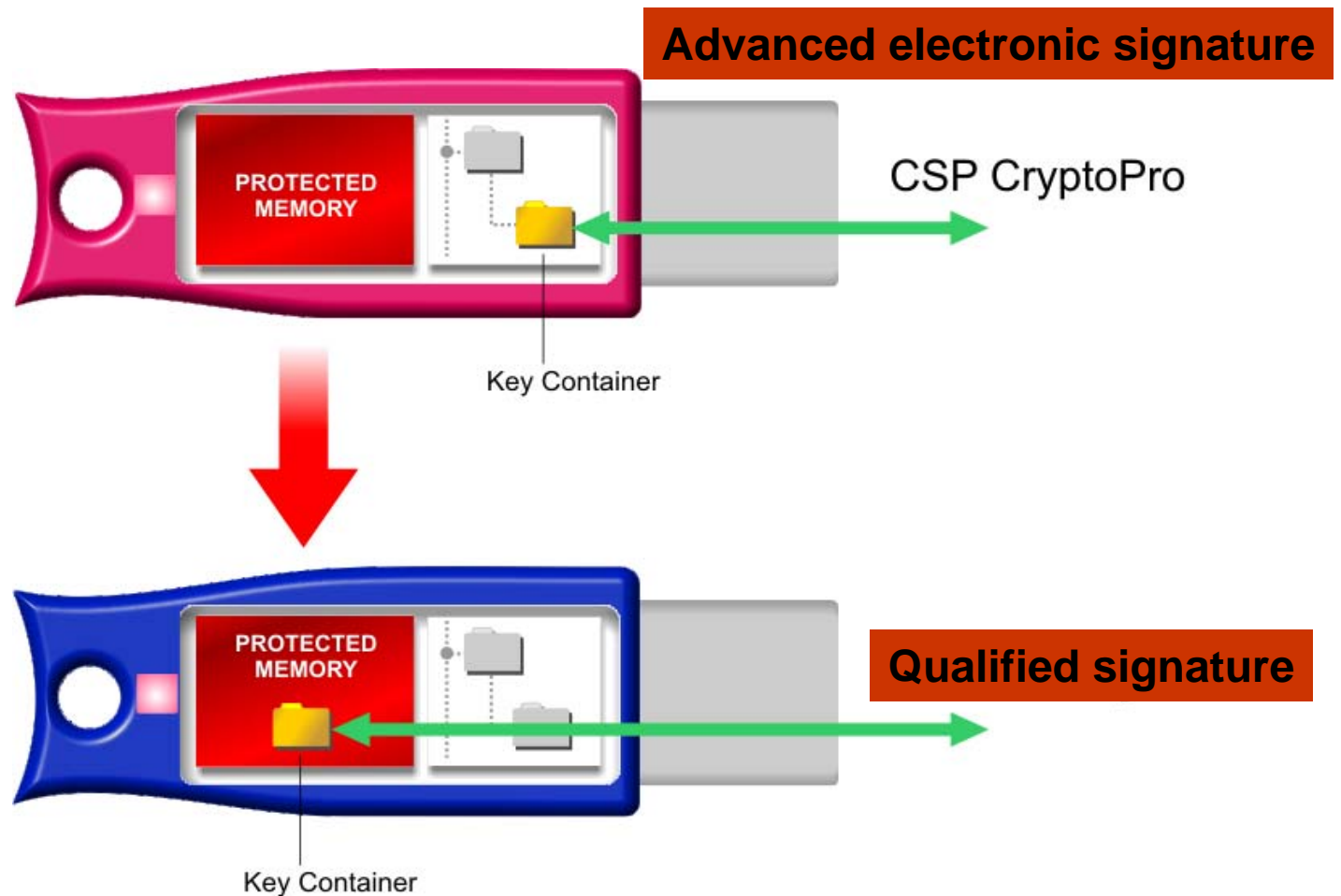
Advanced electronic signature:

- qualified certificate
- certificate is in file system of smart card or token
- private key protected by PIN

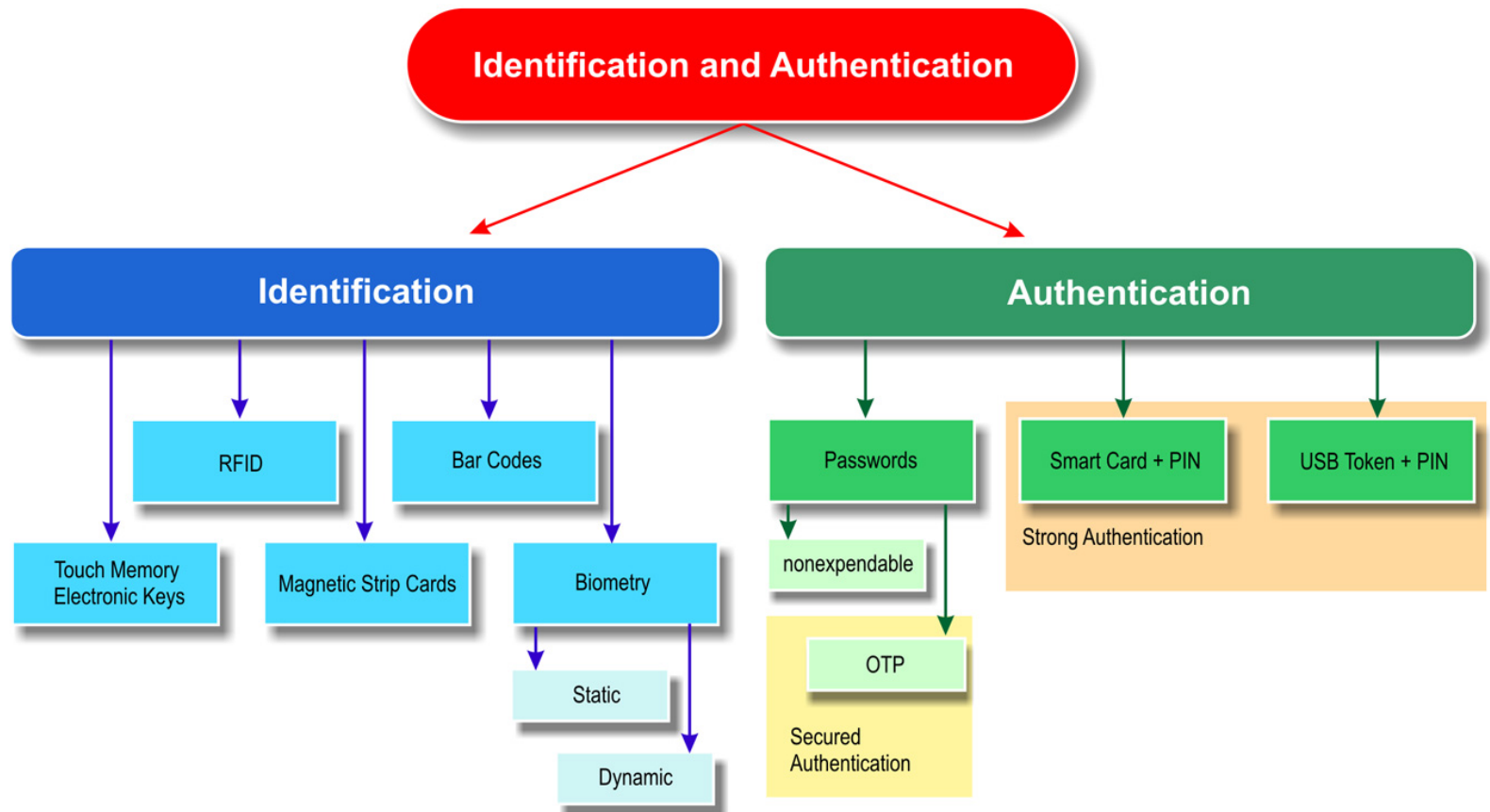
Qualified signature:

advanced electronic signature
secure signature creation token
private key can't leave token

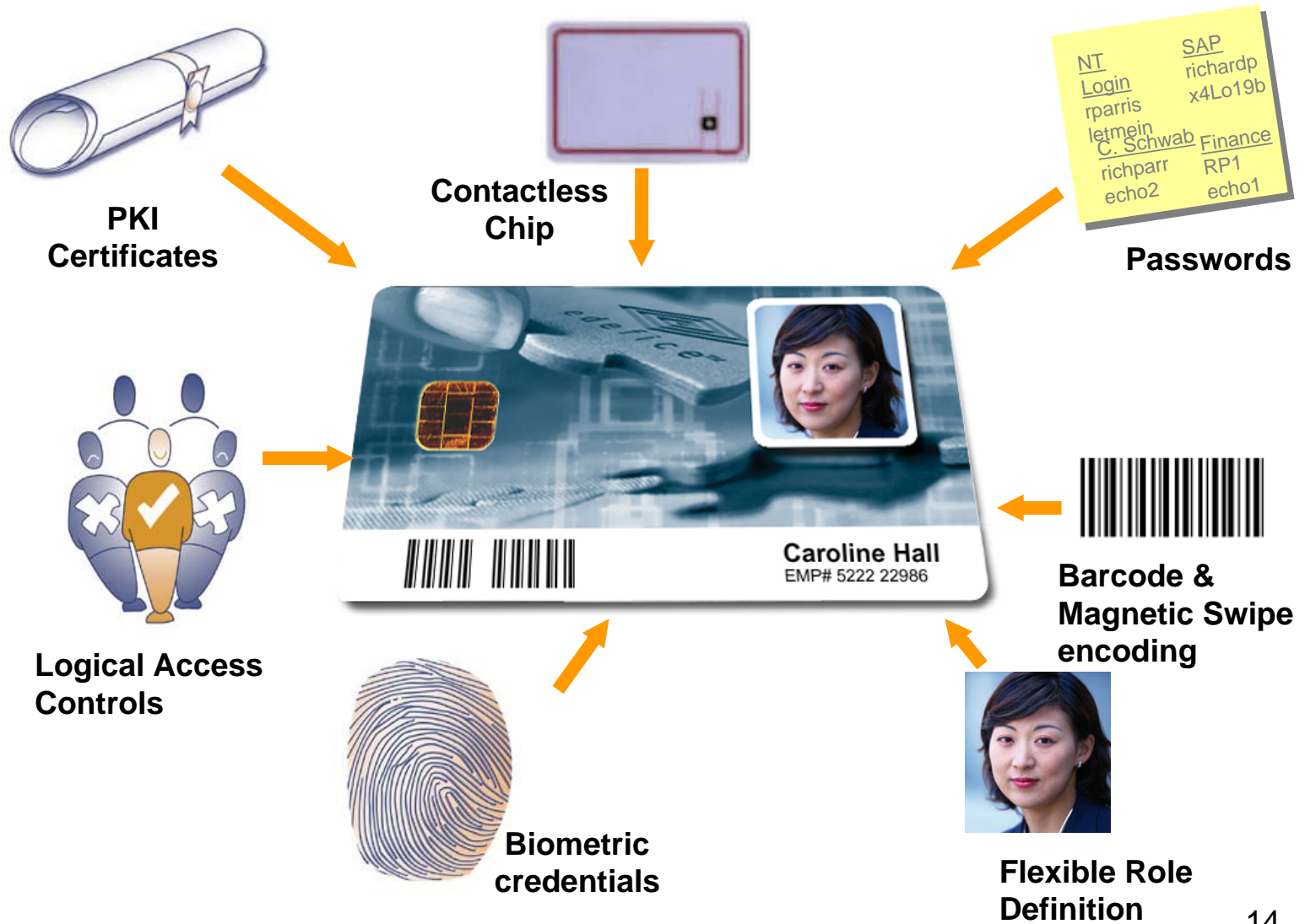
Signatures Types



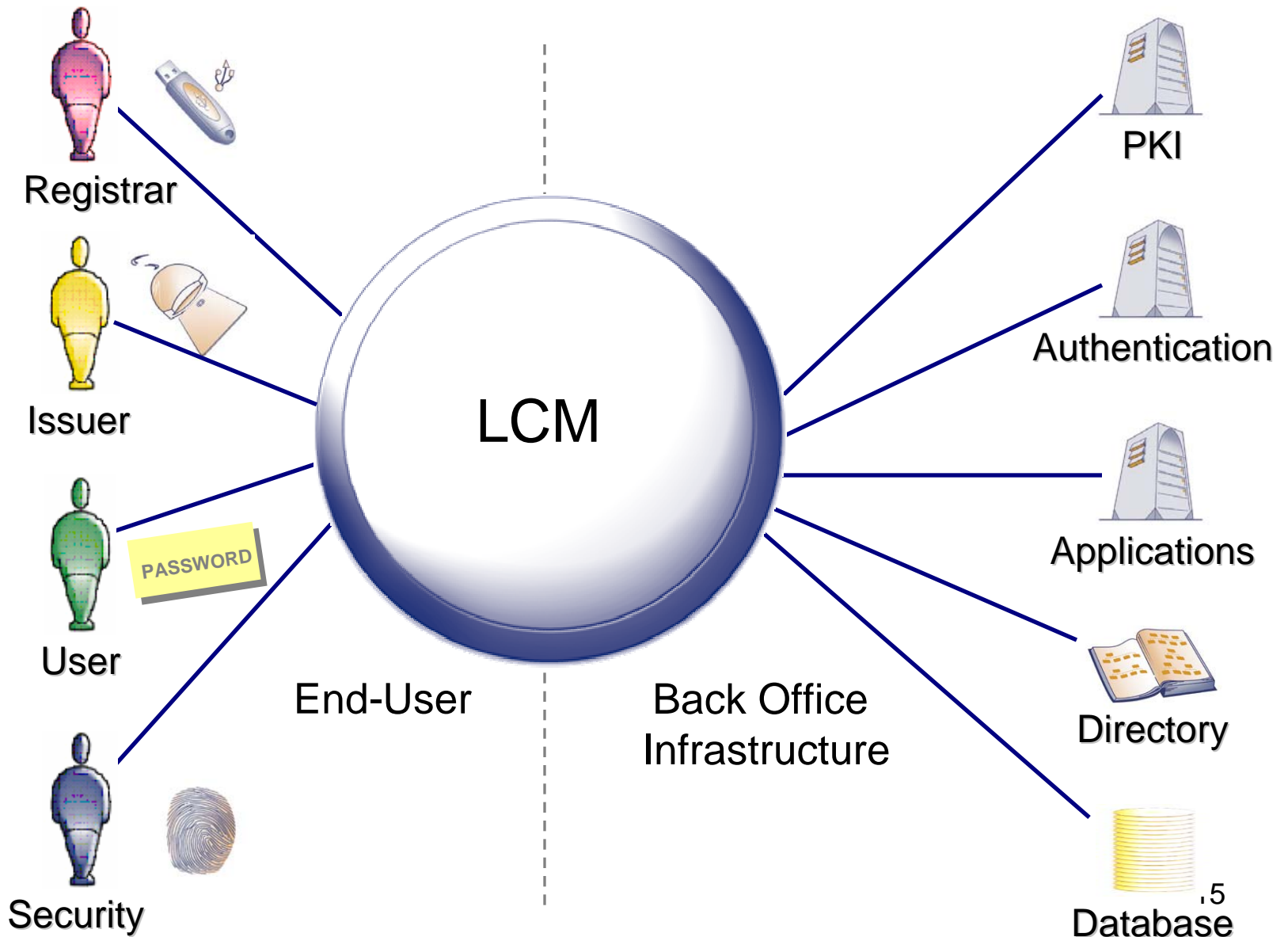
Identification and Authentication



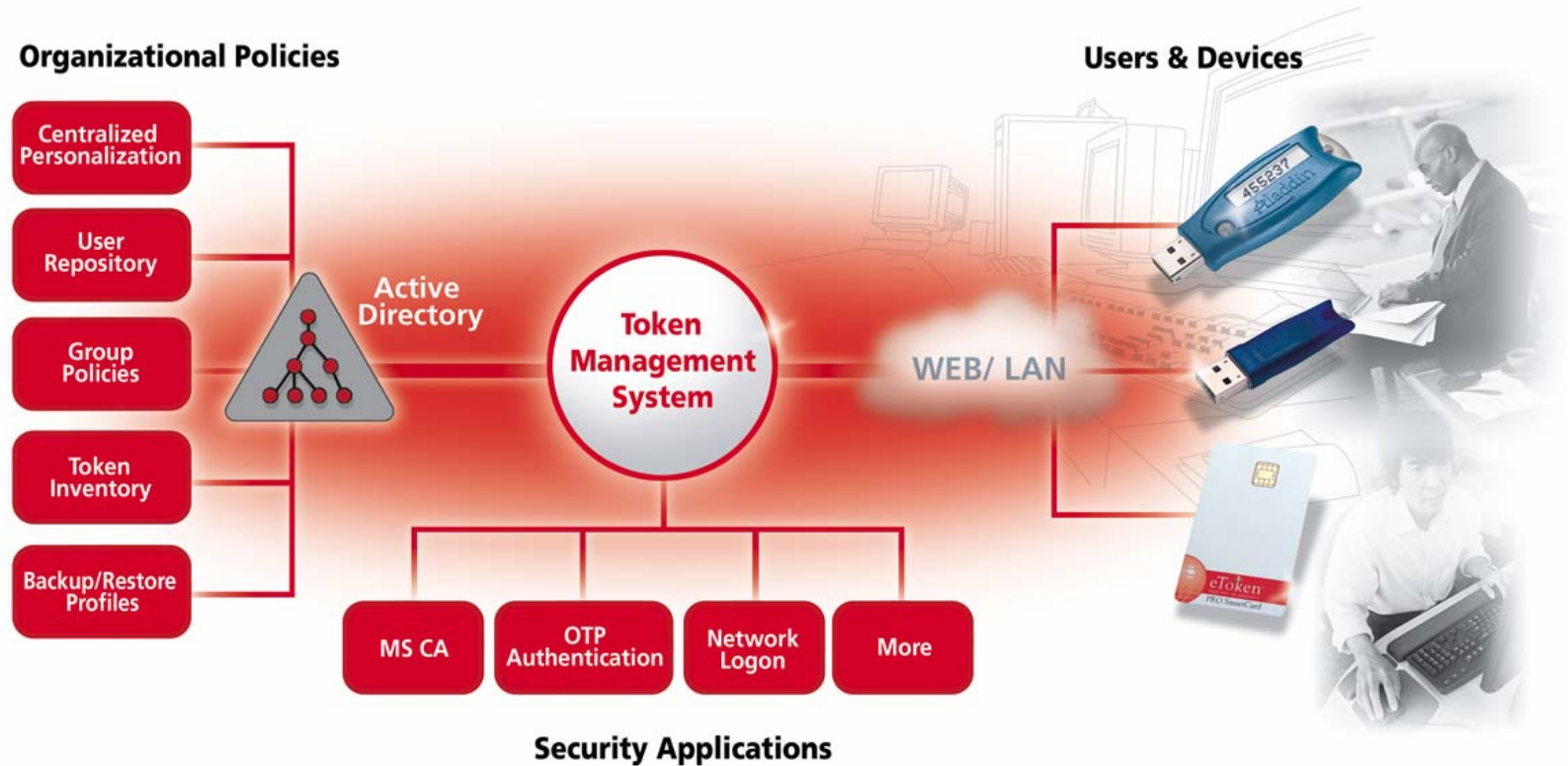
Single (universal) Smart card



Life cycle management

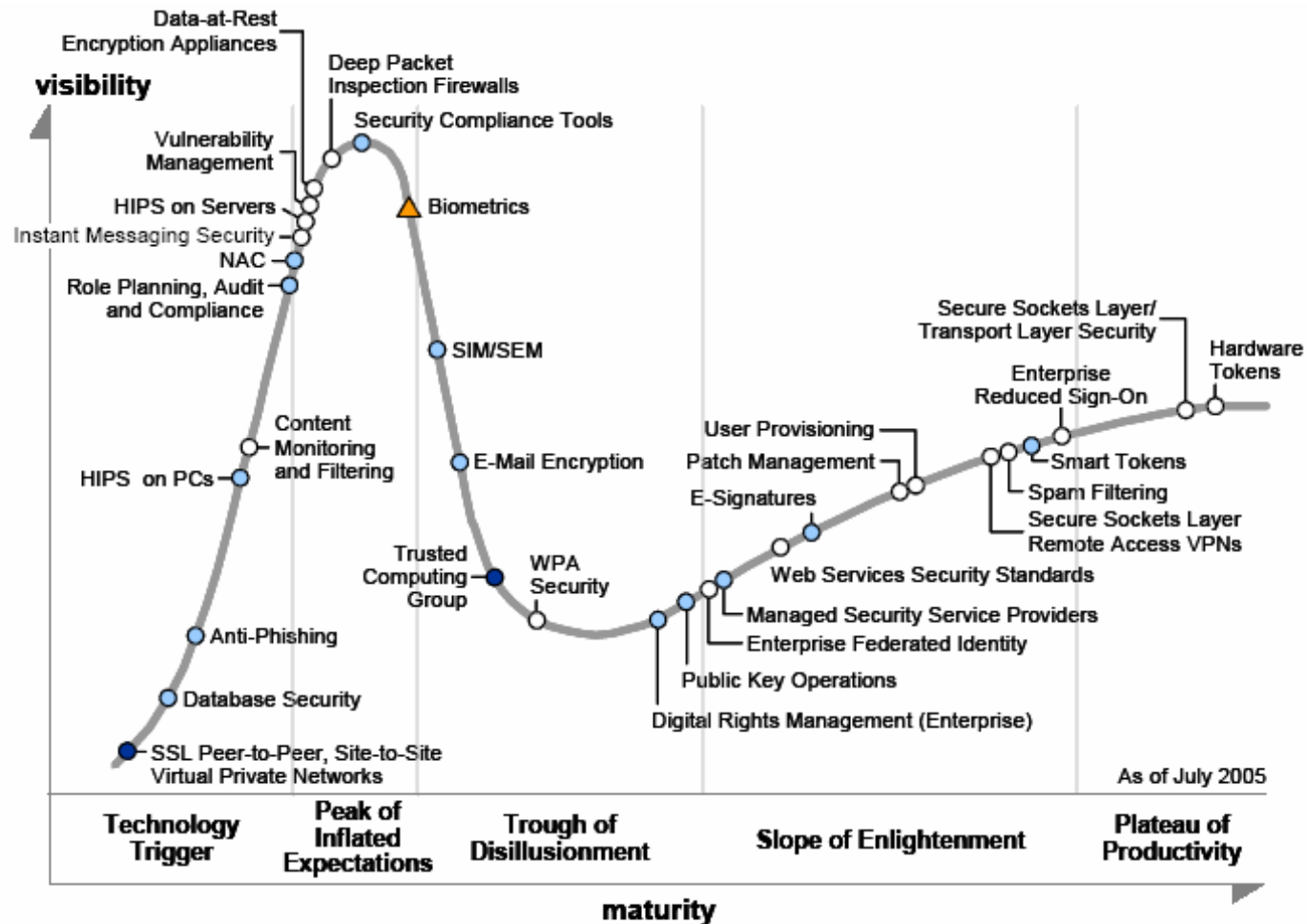


Example: Token Management System



Information Security Technologies

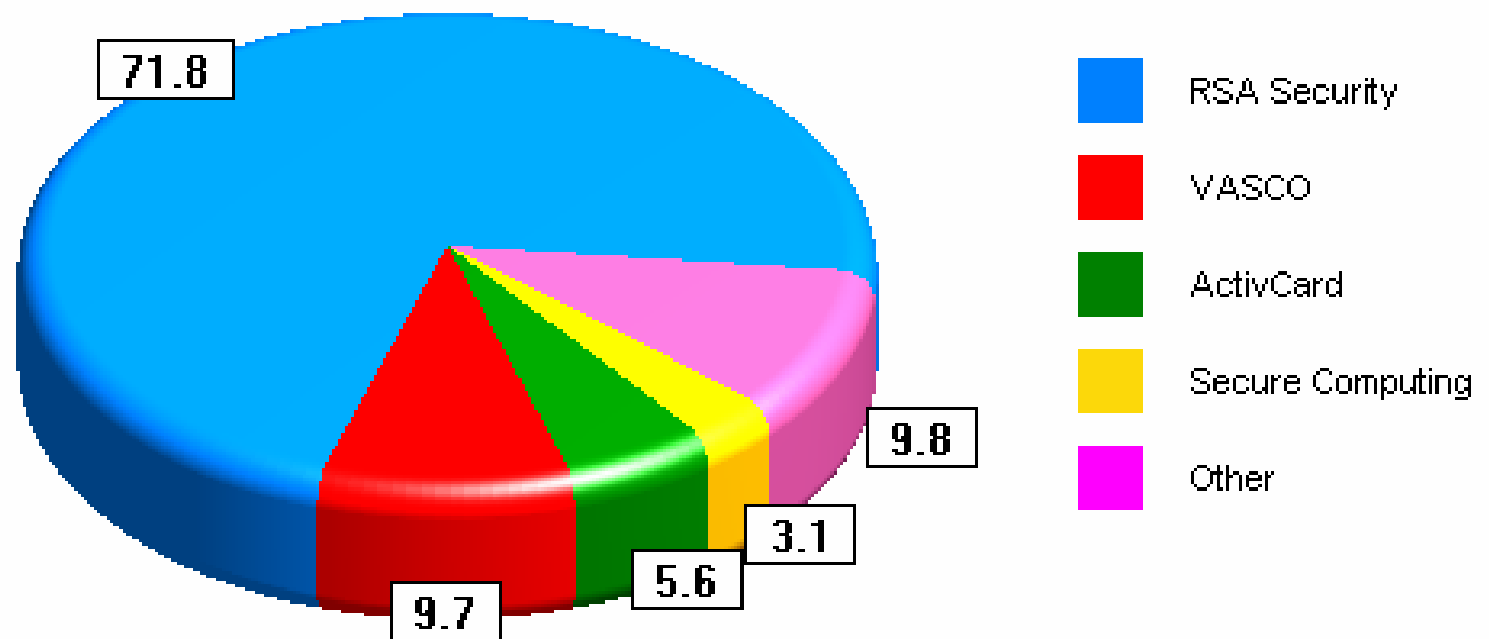
Gartner Group, Hype Cycle for Information Security, 2005



Plateau will be reached in:

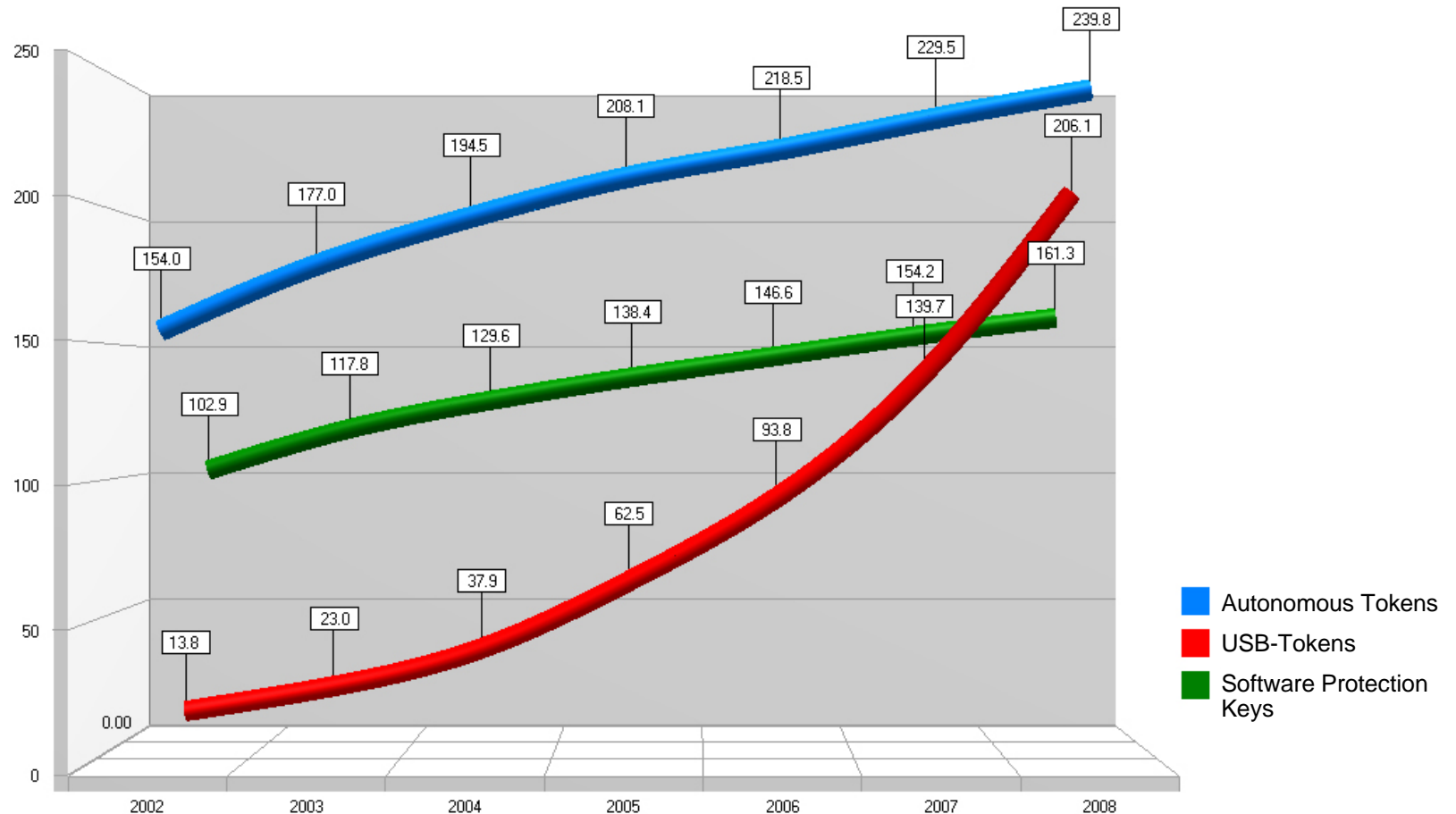
○ less than 2 years ● 2 to 5 years ● 5 to 10 years ▲ more than 10 years ⊗ obsolete before plateau

Hardware Tokens

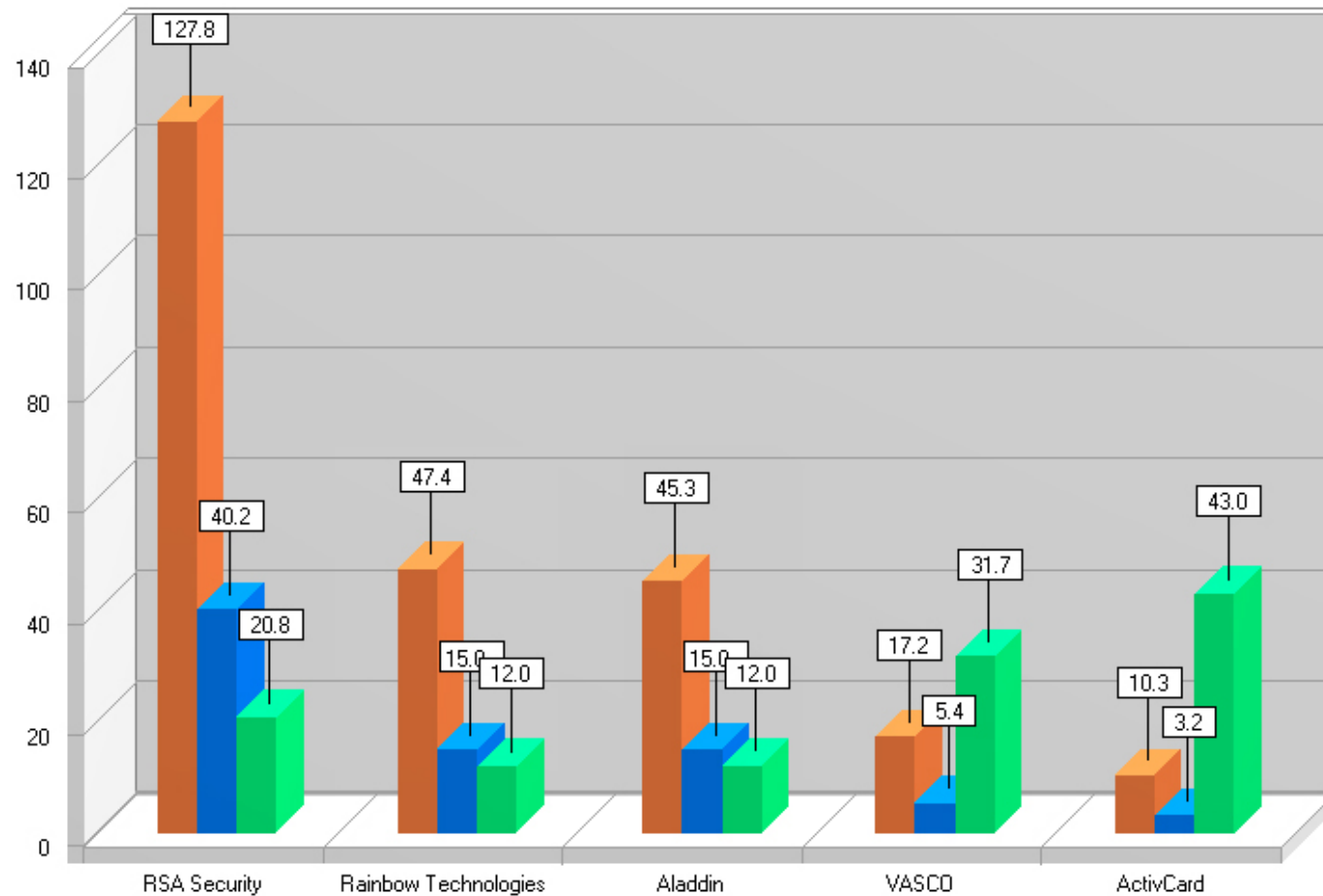


IDC, 2004

Expected dynamic of market



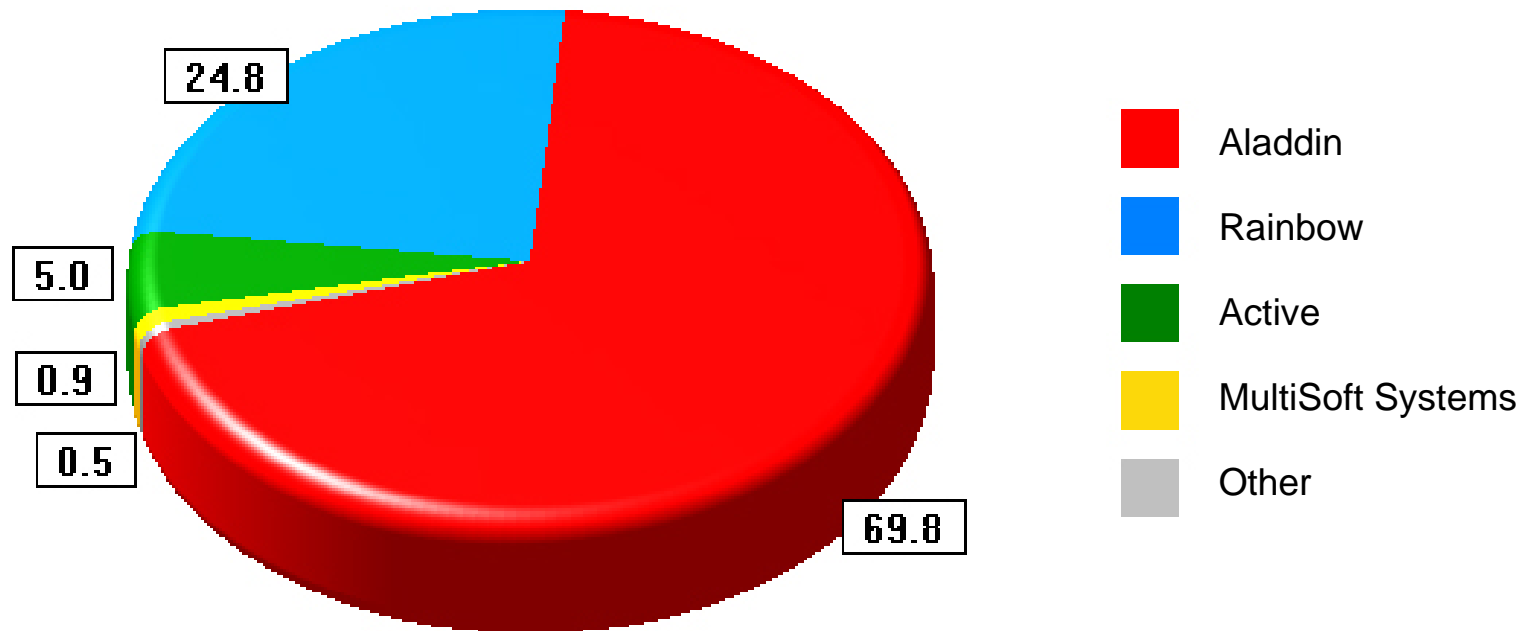
USB Tokens Market



- Revenue, \$M
- Share of the Market, %
- Increase Annual Profit, %

IDC, 2004

USB Tokens Market in Russia



Own evaluations

Thanks you for attention

Alexey Sabanov asabanov@aladdin.ru, tel.: +7(495)231-31-13



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/026

Agenda Item: 25

APEC Privacy Seminar Summary

Purpose: Information
Submitted by: Australia



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

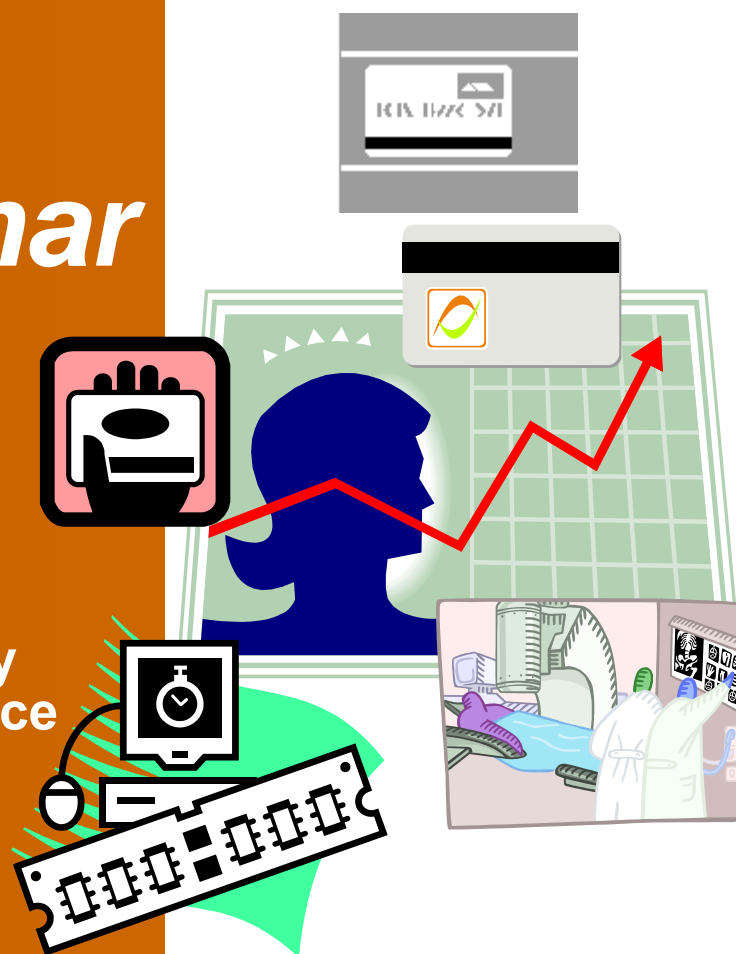


Malcolm Crompton

Summary of Seminar

APEC Symposium on Information Privacy
Protection in E Government & E Commerce

Hanoi
21 February 2006



The underlying issues & instruments

► Control ► Trust ► Risk ► Accountability

Law

Technology

Governance

Safety Net

Privacy ?



A well behaved
market place

The underlying issues & instruments



Themes

- Integrate privacy with all initiatives:
Privacy by Design
 - Security AND privacy; not Security OR privacy
 - Privacy built in, not built on
 - Privacy Impact Assessment
 - Most technology can support multiple needs in the organisation
 - Prove it! AUDIT
- Information Security + Information Privacy = Information Policy

Themes

- eGovernment and eCommerce have much to learn from each other
 - Much more in common than you think
- Integrate economy level policies & frameworks into the regional framework & from there into the global framework
 - UNCITRAL
 - Capacity building
 - VERY rapid growth in some Economies; includes cybercrime
- Respect culture – this is the APEC way

Themes

- “Art of balance” – control use of information
 - Need a framework and method that is also trustworthy
 - Example: access to data for law enforcement
 - Focus on harm – BROADLY defined; APEC Privacy Principle 1
- Be strategic; plan; simplify regulation and frameworks; watch out for overlap
- Safeguards and governance structures

Themes

- Create an environment where information can be used to create value for society AND the individual
 - We can all have confidence
 - Accountability follows the data, ie no avoiding obligations – APEC Privacy Principle 9
- Future is here today – PITs or PETs?
 - Data mining done well = we have both privacy & value
- No magic bullet – People, Policy, Process AND Technology
 - Build in communication & awareness too

Building a “Secure & Favourable Business Environment” – APEC 2006 Sub-Theme 3

- Governance & safeguards best practice; remedy
- Privacy Impact Assessments – eGov, eCommerce
 - Do some!
 - How?
- Regulator cooperation
 - Exchange of information
 - Support of corporate rules
 - Investigation of cross border cases
- Economy partnerships



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/027

Agenda Item: 26

An Overview of Information Privacy

Purpose: Information

Submitted by: Canada



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

An Overview of Information Privacy

David Loukidelis

Information & Privacy Commissioner for British Columbia
(Canada)

APEC Symposium on Information Privacy in E-Government &
E-Commerce

Ha Noi, Vietnam

February 22, 2006

Introduction—Today's Objectives

- First, discuss what information privacy is and why it is important
- Second, discuss the role of the APEC framework in implementing information privacy principles
- Third, discuss some examples of how information privacy is protected in various economies
- Fourth, discuss some approaches for regulators to take in promoting and enforcing information privacy compliance
- Discussion will focus largely on private sector privacy issues, not public sector

1a. What is information privacy?

- Privacy has different meanings in different cultures and in different situations
- It can mean being free from unwarranted intrusion by the state into your home or your body
- Information privacy is about information, not your body or home
- It is about having some control over collection, use and disclosure of information about you as an individual
- Many see privacy as a human right (example: 1948 UN International Declaration of Human Rights)
- Others see privacy as an economic matter
- Many see privacy as a matter of individual autonomy but it is also a community interest

1b. Why does information privacy matter?

- In many cultures, people care about their privacy and are concerned about misuse of their personal information
- People may be worried about information security risks, such as ID theft, more than anything else
- But in many cultures, the concerns go further and extend to uncontrolled collection, use and disclosure of personal information by the private sector or the public sector, or both
- Information privacy matters because it offers protection against inappropriate collection, use or disclosure of our information by governments and by private sector organizations

1b. Why does information privacy matter? (cont'd)

- For example, without reasonable protections, the wrong information may be used to make a decision affecting someone, often without the individual knowing about it
- Another example is ID theft—privacy protections can help reduce ID theft risks by ensuring appropriate security for information such as credit card numbers

2. APEC Privacy Framework's role internationally

- Harmonization of privacy standards is important to ensure that privacy protections are as similar as possible across borders
- This is because different rules can inappropriately hinder or even stop trans-border data flows that are necessary for economic activity and development
- International privacy statements such as the APEC Privacy Framework are vital in harmonizing domestic laws or practices for privacy protection
- The APEC framework serves as a guide for member economies to what standards they should have, while giving them flexibility in deciding which approaches work best for their economies

2. APEC framework's role (cont'd)

- International community has for 30 years recognized the need to harmonize privacy protection in order to protect privacy and also economic activity
- Examples of international efforts include the Council of Europe Convention 108 (1978), OECD Guidelines (1980), EU Directive (1995)
- International privacy commissioners issued Montreux Declaration (2005) recognizing that work remains to be done in harmonizing privacy
- APEC framework can play an important role, perhaps working with OECD, noting growth of APEC economies

3. Approaches to information privacy

- Economies have taken different approaches to privacy protection
- Some have no protection, public or private sector
- This may be for cultural reasons or political, or both
- There may be no economic push for it
- Hong Kong China has an ordinance, or law, that specifies rules but allows the regulator to issue codes
- In Canada, public sector privacy law followed US developments in the 1970s, spreading across Canada in the 1980s to now
- For the private sector, Quebec passed a law in 1994, but rest of Canada did not act until EU Directive forced action (federal law in 2001, provincial laws in 2004)

3. Approaches to information privacy (cont'd)

- Canada also offers example of private sector action
- The Canadian Standards Association Code adopted by the business community in 1995 was a voluntary code of privacy conduct (forms the core of our federal law)
- An example of self-regulatory approaches by the private sector
- In Australia, the federal *Privacy Act* allows business sectors to adopt sector-specific codes that are largely self-enforcing
- In the US, the Safe Harbor accord with the EU allows US companies to agree to comply by Safe Harbor requirements, with enforcement ultimately being left to the Federal Trade Commission

3. Approaches to information privacy (cont'd)

- Under frameworks like APEC's, businesses are trying to find new ways to meet customer expectations, and laws, for their global operations
- Global corporations are adopting rules or codes to cover their global operations, with the codes designed to meet all legal requirements around the world
- To deal with concerns about transborder data flows, businesses are using contracts to regulate privacy issues related to transfer of personal information between companies and across borders
- EU appears to be starting to see the benefits of these approaches, which we can call 'mixed' or 'hybrid'

3. Approaches to information privacy (cont'd)

- In the transborder context, we will see more use of mixed forms of privacy protection in the coming years
- We will see private sector self-regulation and private dispute resolution in relation to transborder data flows, often within the framework of national or sub-national privacy laws and oversight of data protection authorities

4. Tools for privacy compliance

- Hybrid tools are evolving even in economies that have a traditional model that uses a privacy law and an enforcement agency
- Will now discuss examples of this from Canada, specifically, the Province of British Columbia (“BC”)
- The situation is similar under our federal privacy law and in other Canadian provinces such as Alberta and Quebec
- We have a private sector privacy law in BC, the *Personal Information Protection Act*
- It is enforced by the Office of the Information and Privacy Commissioner (“OIPC”), an administrative tribunal and investigative agency independent of the government

- OIPC can receive and investigate complaints about privacy breaches or investigate without complaint
- OIPC can require a complainant to first try to settle the matter with the business involved
- OIPC can mediate settlement of complaints
- Where a complaint is not settled in mediation, OIPC can hold a formal hearing
- The Commissioner has the power to make findings on the evidence and legal determinations
- The Commissioner can make a binding order
- Fines or damages may be awarded in court
- OIPC can order an organization to cease illegal practices or destroy information

- These are very formal powers, but BC's regulatory approach actually offers a mixture of formal powers and processes and less formal tools
- OIPC also has less formal powers to promote and ensure compliance
- For example, the OIPC can comment on the privacy implications of proposed programs, policies or business activities
- OIPC can comment on the implications of data linkage proposals or automated information systems

- OIPC has an explicit mandate for public education
- OIPC can commission research into any matter affecting achieving the law's purposes
- The mixture of formal and less formal tools offers flexibility, giving the OIPC discretion as to which tools to use in specific cases and discretion in creating an overall mix of approaches

Risks & Benefits of Various Powers and OIPC Practices

- OIPC practice has, in several ways, built on the OIPC's explicit statutory powers
- Each has benefits but also presents risks

1. *Providing Advice on Proposed Programs*

- The OIPC is regularly asked to advise public bodies and organizations on their proposed laws or programs
- OIPC's advice often is informal, but may be written

Benefits of Giving Advice

- OIPC's advice gives organizations the heads-up, often early in the design phase, and before major commitment of funds, of privacy risks or roadblocks
- Advice-giving is pro-active and often more systemic in nature than a complaints-handling focus

Risks of Giving Advice

- Advice-giving raises the litigation risk of claim of pre-judgement, or bias, where a complaint is later made about the matter
- Giving advice can also, of course, be reactive—and focussed *ad hoc* on narrow initiatives

- It can also be difficult for the OIPC to capitalize on advice given in terms of publicizing lessons learned—advice is given in confidence, so without public body or organizational consent to disclosure, the advice only builds capacity within the OIPC
- Technical competence of regulator's staff may be raised by IT-related proposals

2. Publication of Support Tools

- The OIPC's practice is to publish support tools for compliance where the OIPC has, through OIPC research or stakeholder consultation, identified needs
- Example: Guidelines for police CCTV of public places
- Example: Guidelines for contracts to outsource data processing
- Example: Privacy impact assessment tool
- Example: Model privacy policy and consent language for doctors

Benefits of Publishing Support Tools

- Support tools/resources promote both technical compliance *and* best privacy practices
- They do so pro-actively, by anticipating trends and needs

Risks of Publishing Support Tools

- Necessarily generic nature of support resources may lead to overly-general material
- By contrast, too narrow a focus leaves gaps
- Resources to invest in creating materials, or technical expertise, may be lacking

3. Sending Would-be Complainants Back

- OIPC policy is to require would-be complainants to first try to resolve their dispute with the relevant organization or trade association

Benefits of Referral-Back

- It treats privacy compliance—certainly in the private sector—as primarily a matter of customer relations
- It forces parties to private transactions to bear the costs of compliance and reduces resource demand for OIPC and thus taxpayers

Risks of Referral-Back

- OIPC loses sight of the matter, raising risk that a dispute will settle for unrelated reasons, leaving a privacy problem untreated
- Even where complaints are settled on the privacy merits, no lessons are gained for the OIPC or a broader audience

4. Mediation

- OIPC policy under both privacy laws is to refer all complaints to mediation by an OIPC mediator
- Most complaints settle in mediation—formal hearings are almost unheard of under the public sector privacy law

Benefits of Mediation

- Interests-based mediation achieves mutually-beneficial outcome at lower cost than formal hearing
- Complainant's privacy is respected—further victimization possible in formal hearing process is avoided

Risks of Mediation

- Training of mediators can be time-consuming
- Possibility that participant unhappiness with outcomes may (among other things) reduce regulator's credibility
- In any system where complaints are mostly settled through mediation, lessons learned about the law and compliance are confined to the regulator and the parties to each dispute—and this hinders broader understanding of the law and how to comply with it

5. Formal Hearings & Binding Orders

- OIPC can issue an order, after a formal hearing, that binds the respondent

Benefits of Formal Hearings & Binding Orders

- Obviously, a binding order will, subject to a successful court appeal, ensure compliance—it gives the complainant a real, personal remedy
- Publication of the decision deters bad behaviour through embarrassment (and rewards compliance where a complaint is dismissed)

Risks of Formal Hearings & Binding Orders

- They depend on complaints and are therefore reactive, *ad hoc* and bilateral
- They can be resource-intensive, yet yield small return in terms of compliance generally

6. Audits

Benefits of Audits

- With institutional data-holdings, audits can identify systemic problems and allow repair
- Educational benefits can flow from publication of methodology, targeted data-holdings or systems and outcomes (both regulator's recommendations or requirements and compliance response)

Risks of Audits

- Formal compliance audits can be very resource-heavy—in terms of staff or consultant time and expertise

- Without careful targetting of audit resources, to maximize generalization potential of outcomes, the resources invested may be wasted—but over-ambitious audits can collapse
- Example: Would it be best to audit BC's central cancer treatment agency or a small rural hospital? Would the latter yield any generally-applicable findings? Would the former swamp the OIPC's resources and expertise?

7. Providing Education

- The OIPC periodically holds, around BC, training workshops and conferences (on a cost recovery basis)
- Training workshops focus on education and skills-improvement for privacy officers in public bodies or organizations—they offer hands-on, practical exercises in privacy compliance
- OIPC conferences fulfill the broader goals of generating policy discussion *and* educating the public about their privacy rights and current issues

- OIPC and staff regularly speak to seminars and conferences about privacy compliance, again to promote compliance and educate a broader audience

Benefits of Education Efforts

- Training of organization staff builds and maintains compliance capacity and promotes good practice—and it can reduce demands on OIPC resources
- Conferences maintain dialogue, over time, on merits of the legislation and assist in identifying gaps or areas for reform as circumstances evolve

Risks of Education Efforts

- Training events do not always capture the right audience—entry-level staff often attend, not IT or other program managers
- This can reduce impact in terms of capacity building or organizational cultural change
- Conferences may similarly suffer from the wrong focus
- They may also fail to target the right audience or most important topics

Concluding Comments

- The Canadian practice has—as in BC—been to combine freedom of information (FOI) and privacy oversight duties in one agency
- Incidence of demands can, as in OIPC's case, skew the agency's focus (compare the OIPC's 1,000 FOI appeals a year to the roughly 200 (public sector) privacy complaints)
- Also, regardless of which enforcement tools have been given to the agency, good privacy enforcement depends on adequate resources for the agency

- For the OIPC, fiscal restraint has meant imposed budget cuts of 35%
- Remaining OIPC staff are forced to focus on responding to complaints and FOI appeals
- The government's fiscal direction has seriously undermined our ability to pursue most of the pro-active avenues identified above—advice-giving is greatly reduced, creation and updating of support tools has been greatly reduced, *etc.*

- Resource scarcity forces the OIPC into damage-control mode—pre-occupied with responding to complaints and appeals, merely keeping the listing ship afloat
- This perversely hinders or precludes strategic planning, and thus targetting of remaining resources for outreach, support and advice
- OIPC's shift from pro-active, systemic work to reactive complaints focus may increase compliance costs for public bodies and organizations in the medium term
- Without adequate resources for the oversight agency, ultimately there is a real risk of having only an illusion of data protection

Possible Elements of APEC Framework

- An oversight agency independent of government is key to public confidence and stakeholder co-operation
- A broad range of enforcement tools is desirable
- On the formal end, formal investigative powers (including audit power) and power to issue binding orders—not just recommendations—is desirable
- On the other hand, it would be useful to have general authority to comment on privacy implications of programs and laws, to educate stakeholders and the public, to issue guidance on emerging issues

- Authority for the agency to issue or approve of sectoral codes or issue guidance notes (binding or only advisory) is missing from BC's scheme—it is well worth considering
- Agency should be structured to enhance strategic planning that is crucial to an effective mix of oversight approaches, formal and informal
- Continuous, unrelenting communication with identified stakeholders is key—agency perhaps should be required to create an external advisory body (e.g., Privacy Commissioner of Canada's EAP)

- Agency must be open to constructive criticism and feedback
- More pragmatically, ensuring adequate, long-term funding for the agency is critical to success for public and private sector legislation
- Independence of the agency could perhaps be best assured if a body at arm's-length to government were to set the agency's budget

Conclusion

- This presentation was intended to give you a brief description of what information privacy is, of the international context for modern privacy standards and enforcement approaches, and to offer one example of how an economy might approach oversight of privacy compliance
- The Office of the Information and Privacy Commissioner for British Columbia is always happy to provide information, assist or collaborate with privacy compliance issues
- Thank you for your kind attention

Office of the Information & Privacy Commissioner for
British Columbia
Victoria, British Columbia
Canada

Email info@oipc.bc.ca

Web www.oipc.bc.ca



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/028

Agenda Item: 27

Privacy - Enhancing Tools List

Purpose: Information

Submitted by: Peru



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

| CPSR Perú.

Ciudadanía y Derechos en la Sociedad de la Información



Information Privacy Tutorial

Katitza Rodríguez, Director of CPSR-Perú
*APEC Symposium on Information Privacy Protection in
E-Government and E-Commerce
Ha Noi, Vietnam, February 2006*

Index

- About CPSR-Perú
- What is Data Protection?
- Identity Theft
- Financial Privacy
- Internet insecurities & Basic internet safety
- E-mail insecurities & Basic safe e-mail.
- Basic safe browsing tips.
- Basic computer and files securities.
- Online Privacy tools

About CPSR-Perú

CPSR-Perú is a public interest research centre of information and communications technology (ICT). Founded in Lima in October of 2002, its mission is to promote the socially responsible use and development of information and communications technologies, highlighting the social benefits that derive from their correct use and guarding against their use for detrimental, socially harmful purposes. CPSR-Peru attempts to influence government policy on ICT and carries out research into the regulation of ICT and their impact on society.

In addition, it provides legal representation for citizens and organizations whose rights to access to the Internet under threat. It is conformed by lawyers and technicians, with strong links with main local universities.

About CPSR-Perú

CPSR-Perú is working in privacy and data protection issues
<http://www.cpsr-peru.org/privacidad/> from three different perspectives:

- **Academic**: Doing legal research in Peru and Latin America on legislation, regulations, public policies and private practices.
- **Advocacy and public policy at the local, regional and international level**: CPSR-Perú participated at the World Summit of Information Society, Asia Pacific Economic Cooperation Forum, the Ibero American Data Protection Network.
- **Practical**: Researching and organizing workshops on privacy enhancing technologies to protect our online privacy, secure communications and digital information. CPSR-Perú has trained journalist and human right workers in tools and methods for secure communications and the protection of sensitive data in Latin America: Mexico, Perú, Colombia and Venezuela.

What is data protection?

- The fundamental right of the protection personal data recognizes all citizens the faculty to control its personal data and the capacity to arrange and to decide on the same ones. This means that all people have the right to know why and how their data are treated.
- Going online and taking advantage of the technology may require the disclosure and treatment of personal data. Nevertheless, most of the consumers are not aware about this issue.

Data Protection

- CPSR-Perú believed that to assure the privacy of our personal information, consumers must have the protection provided by basic law and law enforcement. However, protected by law or not, we thought consumers needs information to understand the risk associated when they use the technology.
- Consumers needs to be ever vigilant in terms of who gets our data. We need to learn to ask certain questions before giving out our data and to find out which information about us, they had.

Identity theft

- Criminals use personal data in order to theft the identity of another person. Criminal use your **existing credit information** or **open new accounts** in your name.

For example: Criminals use to steal

- ID cards
- Credit and debit card numbers,
- telephone calling cards,
- Find out the date of birth,
- Find out work and personal address.

Financial information

Your credit report is actually a credit history. It may contains information such us:

- Delay payments;
- Information of those to whom you owe money that may report this information to the credit bureau.
- If you do not make credit card, auto loans, or mortgage payments on time.

Information in your report may contains

- Name, address, telephone number, year and month of birth, employment information. Also includes matters of public record such as civil judgments, tax liens and bankruptcies.

Enforcing your data protection rights!

- In Perú, you have the right to free access to your credit report once a year or when your information is rectify.
- A creditor has the duty to report only legal, accurate, complete, and updated information to the CB.
- Look in depth your credit report. You have the right to access to your information, modify it or cancel it. An in case the CB gave this incomplete or inaccurate information to a third party, they had the obligation to rectify it.
- In Perú, the liability for the credit bureau is objective if they do not grant the right to access, modify, cancel or rectify the information.

Enforcing your data protection rights!

- Depends on your national law, after a period of time, 5 years in Peru, and in specific cases, negative information that was paid or extinguished, should be deleted from your credit report. This is called the right of oblivion or right to be forgotten.
- Filing suit and complaining to government Agencies. If you win, you may be entitled to recover an amount of money for damages.

Internet insecurities & Basic internet safety

- The Internet connects computers to each other over a global network. The computer can be your laptop, your personal or family desktop or your computer at work. The software that your computer runs deliver, in some cases, information about their customers of their web sites.
- Browsers pass along information about the brand of the browser, the version and plug-ins that are available.
- The web server logs include the IP address that identifies “a computer” that visits that site.

Internet insecurities & Basic internet safety

- Cookies create an identity on the Internet but this identity is still tied to a computer, unless you disclose personal information. How? Filling out a form for subscription services, personalizing your site for example with My Yahoo account.
- Companies could triangulate information in order to identify you through the use of outside sources, not only the information you give through an online services.
- It isn't just the data that you give out today that may identify you, it's data that you have given out or that has been gathered about you your entire life.

Internet insecurities & Basic internet safety

- **Anti- Virus**: Install and keep up to date virus protection software to prevent causing problems to your computer or sending out files or another stored information.
- **Keylogger attack**: A “key logger” system can track every keystroke you make. These programs are spread either by someone putting it on your computer while you are away, or through a virus or Trojan you get over the Internet that attacks your system. Key loggers track your keystrokes and report back your activities, usually over the Internet.
- **Intrusions**: Install a firewall on your home computer to prevent crackers from enter to your computer.

E-mail insecurities & Basic e-mail practices

- Your email does not fly directly from your computer to the computer of the intended recipient. It goes through several nodes and leaves behind information as it passes. No matter if you are sending me an email from your computer in this room to my computer here in this room, email flies among several nodes.

Encrypt your email whenever possible

- It is always good to encrypt your email whenever possible. An unencrypted email is like a postcard that can be read by anyone who sees it or obtains access to it. An encrypted email is like a letter in an envelope inside is safe.
- When you are entering to your password of your email, someone can be looking over your shoulder as you type, in order to see your password.
- If your computer are connected to a network your email maybe accessible by everyone else in the office.
- The system administrator may have special administrative privileges to access all emails accounts.

Email insecurities & Basic email practice

- The Internet Service Provider has access to your e-mail. Anyone who has influence over your ISP may be able to pressure it to forward him or her copies of all your email or to stop certain email from getting through.
- As it passes through the Internet your email flows through hundreds of insecure third-parties: crackers can access email messages as they pass.
- The ISP of your intended recipient may also be vulnerable, along with the network and office of your intended recipient.

- **On line service:** Think twice, maybe three times, before signing up (filling a form with lot of personal information) for a web site's services. Be aware that by signing up you are creating an identity. Do you have reason to believe that you can trust the company with your information? Do you think it is necessarily to give to them all the information they are requesting to you?
- **Shopping online:** When shopping online, do business with companies that provide secure transaction platform and that have strong privacy policies. It could be good to do online shopping in countries that have strong data protections laws.

- **Going anonymous:** One of the best ways to protect your privacy is going anonymous. If you wish to maintain some anonymity, you can register for a free web-based e-mail account using fictitious information and then use that address for contact with potentially invasive services.
- If you feel strongly about controlling your identity on the Internet, there are services that can allow you to surf the web either anonymously or pseudonymously. Please see your materials for more information.

- **Passphrase protected:** To avoid someone accessing your computer while you are away, pass phrase protect your computer and always shut off your computer when you leave it. Create passwords that combine 8 numbers and letters, upper and lower case and or symbols.
- **Encrypted data/disk:** If they can get by your pass phrase protection, or if you have left your computer on, your files can still be secure if you encrypt your files. In your materials, you will find tools that help you encrypted your data.
- **Back up:** If your computer is stolen, you can get back your files if you have created a secure backup every day. Keep the encrypted backups away from your office in a safe place.
- **Wipe:** Do not rely on the "delete" function to remove files containing sensitive information. There are ways to recover that information. If you want that your delete files not be reconstructed, please wipe it. There are tools (see your materials) to wipe information. Use that tool instead of just throwing them into the Trash or Recycle Bin.

Privacy - Enhancing Tools List

Email encryption

- PGP
- GnuPG
- S-Mail
- Stealthmessage
- Hushmail
- CryptoHeaven
- MailVault

Disk encryption

- PGP Disk
- DriveCrypt
- BestCrypt

Anonymous Remailer and Surfing

- Anonymizer
- AnonymSurfen
- Anonymouse.com
- Anonymous Remailer
- Tor

Privacy - Enhancing Tools List

DATA STORAGE/Backup

- Martus
- CDRWs (CD read/write)
- Extra hard drive in computer

Backup software

- Retrospect.com
- DIY (Do It Yourself)
- USB, Compact Flash Memory or Memory Stick

Other

- PGP SDA (self decrypting archive)
- S-Mail S-Disk:
- Virtual shredder
- Keyboard popup
- Tempest



Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/029

Agenda Item: 27

Privacy - Enhancing Tools List

Purpose: Information

Submitted by: Peru



**APEC Symposium on Information
Privacy Protection in E-Government
and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006**

Privacy - Enhancing Tools List

Email encryption

PGP – www.pgpi.org (free) or www.pgp.com (paid)

- Pros: trustworthy, free, relatively easy to use, cross-platform, can import and export files from the Web, standard encryption system used by most in the industry
- Cons: free version is not supported, installation not completely intuitive, Key system can be confusing. Key management can be difficult (policy level issues).

GnuPG, the free software version of PGP can be found at www.gnupg.org and is available in several different languages.

S-Mail – www.s-mail.com

- Pros: easy to use web-based email; supports Unicode, which has the capability of displaying characters of almost all languages on the world; integrates with MS Outlook with a plugin.
- Cons: not all features available in free version; developers are of unknown trustworthiness.

Stealthmessage – www.stealthmessage.com

- Pros: free, easy to use, Web-based secure messaging to email; can be used at Internet cafes; has “auto destruct” feature that erases very sensitive messages; 160-bit encryption within 128-bit SSL; can best be used to send a short message to yourself for later pickup, as there is no need to share your “secret code” with anyone else, which makes it a good way to send messages to yourself from the field at an internet café.
- Cons: can only type messages up to 20,000 characters; need to transmit shared password securely or at least separately; lower level of encryption than other systems based on PGP; developers are of unknown trustworthiness.

Hushmail – www.hushmail.com

- Pros: free lite version, supported, trustworthy (due to personal contact), easy to use, Web-based, can be used at Internet cafes, safe key generation; can use with other hushmail users and with “regular” PGP email users.
- Cons: lite/free version users must use every three weeks or account is deleted. Purchase without limitations is available for \$30 per year. Does

not work on Macintosh computers. Some reported problems in loading makes it inconsistent.

CryptoHeaven – www.cryptoheaven.com

- Pros: Uses 256-bit encryption for secure email and secure file sharing; data never travels on public internet, which enormously cuts risks. Available for all major platforms: PC, Mac, Linux.
- Cons: Relatively new and untested by cryptocommunity; costs \$30/year for advanced features like secure online file storage. Downloadable application – must be able to install new software on each computer using it.

MailVault – www.mailvault.com

- Pros. Supports 256-bit AES for SSL transmission security if your browser also supports it. Clients have the ability to send and receive encrypted e-mail from any location, not just from their own computers using Mailvault's secure web-based login. Non-encrypted e-mail messages can also be written and sent via MailVault. Encryption keys are created by the MailVault engine and stored on distributed offshore servers.
- Cons: Relatively new; You can not use your own domain name, just use the domain name mailvault.com.

Disk encryption

PGP Disk

Can be obtained on www.pgpi.com freeware version 6.0.1. New version 8.0 was released by PGP Corporation and is actively being supported by them.

- Pros: trustworthy; older version may be free. Paid version is a benchmark in the field.
- Cons: Not completely intuitive, and free versions do not work with modern/up to-date operating systems; older free versions may require a separate patch to be installed.

DriveCrypt – www.drivecrypt.com

- Pros: supported, trustworthy, has more features than PGP Disk
- Cons: \$40

BestCrypt – www.bestcrypt.com

- Pros: works on Windows & Linux, supported, many features including Wipe, free trial version
- Cons: does not work on Macintosh, proprietary so not free

Anonymous Remailer and Surfing

Anonymizer – www.anonymizer.com

- Pros: Author is very credible within the security field.

- Cons: Proprietary, you must trust the author, no peer review.

AnonymSurfen - <http://www.anonymsurfen.com/>

- Surfing anonymous in the Net. Free web-based proxies that can be used directly from the website.

Anonymouse.com - <http://nonymouse.com/>

- Offers anonymous Web surfing and newsgroup posting. It is free.

**FAQ Anonymous Remailer - <http://www.andrebacard.com/remail.html>
<http://www.panta-rhei.eu.org/pantawiki>**

Tor – <http://www.eff.org>

- Anonymous web browsing, instant messaging, etc. Also allows users to offer "hidden" web servers and other services, even from behind firewalls.

DATA STORAGE/Backup

Martus – www.martus.org

- Pros: very easy to use; trusted source, will be open source; built in encryption; support and training readily available; based on basic database system; platform independent; can make parts of "bulletins" available to the public; can search and retrieve items easily.
- Cons: Should not be used as communication system, only as information storage and retrieval system; must rely on other organizations to host Martus servers (however, there are already several reputable ones in operation)

CDRWs (CD read/write)

- Pros: inexpensive and easy to use
- Cons: user-based so you must remember to perform the backup. Backup must be placed in secure, separate location.

Extra hard drive in computer

- Pros: easy to use and usually readily available, relatively inexpensive
- Cons: raid or surveillance/hacking could result in both original and backup destruction; can accidentally be overwritten – prone to user error.

Online backup company

(novastore.com, bitstore.com, virtualbackup.com and many more)

- Pros: easy to use
- Cons: cost, must send all documents encrypted as source is not necessarily trusted.

Backup software

Retrospect.com (NovaStore, Symantec Norton Ghost and more are similar)

- Pros: cross-platform, desktop and server versions, can be automated to save time, relatively easy to use, one time setup, then transparent to user, backs up to multiple media – disk, internet, etc.
- Cons: proprietary code, costs money

DIY (Do It Yourself)

- A knowledgeable computer systems administrator can set up a regular backup cycle, preferably to an off-site location, sent in a secure manner so that your files can't be read in transit. Some of the utilities that will do this are "rsync" and "ssh". Please either contact us for assistance or make sure you have an experienced person helping you
- Pros: Cheap and fast to implement
- Cons: Can be complicated; must be an experienced computer user/technician

USB, Compact Flash Memory or Memory Stick

- Pros: extremely portable, can easily be hidden by casual inspection, can hold up to 1 GB (gigabyte), which is about a million one-page emails or 1000 1MB formatted documents
- Cons: must purchase hardware, user-based so you must remember to perform backup. Uses battery consumption so will wear laptop battery faster.

Examples of these can be found at:

<http://www.rtsz.com/cryptostick.shtml> - USB memory

<http://www.memorysuppliers.com/memorystick.html> - memory stick

<http://www.memorysuppliers.com/compactflash.html> - compact flash memory

Physical Security

Biometric (Fingerprint) Identification

- Siemens and other companies now make USB mice that have fingerprint recognition features built-in, preventing unauthorized users from using your computer.

Cameras

- Small, inexpensive cameras can be discreetly mounted to monitor who enters your doors and/or windows for when your computers are completely unattended.

Locks, etc

- Judicious use of locks, security personnel and placement of computers away from windows provides better protection.

Other

PGP SDA (self decrypting archive)

- Pros: Enables you to send a PGP-encrypted document to a user that doesn't have PGP installed on computer. Is bundled with PGP versions 6.5 and higher.
- Cons: Must get decrypting passphrase to end-user somehow in a secure manner.

S-Mail S-Disk:

- Pros: Allows you to share sensitive documents in an online encrypted space.

Virtual shredder

- Pros: Bundled with PGP, Diskwipe shreds files.
- Cons: Simply deleting a document does not wipe it from your system – you must remember to wipe it.

Keyboard popup

- “Type” your passphrase in a keyboard on your screen when you suspect that the emissions from your keyboard strokes are being logged. This is built into CryptoHeaven and Martus software, but we aren't aware of any others that have this feature built in.

Tempest

- Use of “tempest” shielded fonts in your email client (built in to PGP using “secure viewing”) and others will protect you if you suspect eavesdropping on unintentional emissions produced by most electronic equipment. See www.tempest-inc.com/ for examples, additional information.

Acknowledgments: *This material was created for the workshop on privacy and secure communications for human rights non-governmental organizations organized by Privatterra (<http://www.privatterra.org>), an on-going project of Computer Professionals For Social Responsibility (CPSR) with the cooperation of CPSR-Perú (<http://www.cpsr-peru.org>) in Lima, Peru 2003. It was prepared by the Privatterra team conformed by Robert Guerra (Managing Director), Caryn Mladen (formerly Privatterra), Jo Hasting (formerly Privatterra) and Katitza Rodríguez (formerly Privatterra and CPSR-Perú). A minor update was done by Katitza Rodríguez, Director of CPSR-Perú, specially for this workshop.*

Copyright notice: *This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 2.5 License. <http://creativecommons.org/licenses/by-nc-sa/2.5>*

Disclaimer: *The speaker does not lobby for, consult, or advice companies, nor do we endorse specific products or services. This list merely serves as a sampling of available privacy-enhancing tools including our comments based in our own experience. If you have comments to share regarding one or more of the tools that are already listed, send an e-mail to katitza@cpsr-peru.org. If you have questions about a tool on this list, visit their own website directly for more information.*