

Privacy Issues in Middleware for Service-oriented Applications

2007 Middleware for Web Services (MWS 2007) Workshop, USA

Patrick C. K. Hung

Assistant Professor, Faculty of Business and Information Technology
University of Ontario Institute of Technology (UOIT), Canada

Adjunct Assistant Professor, Department of Electrical and Computer Engineering
University of Waterloo, Canada

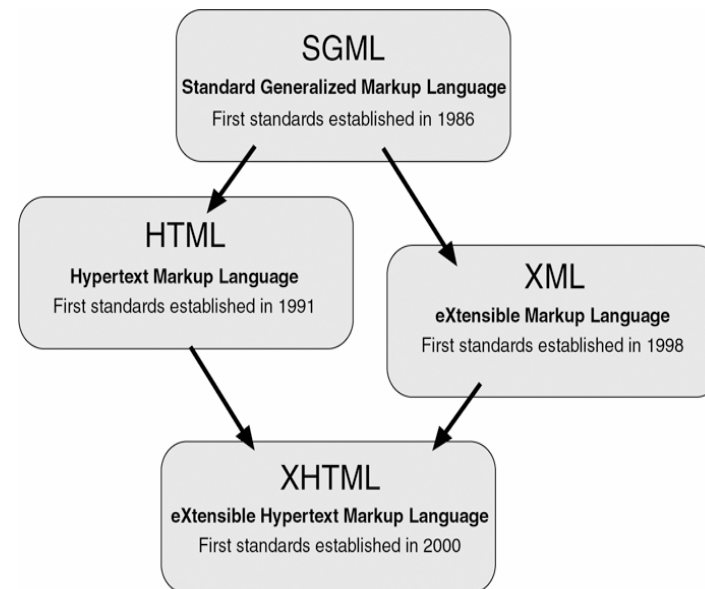
Faculty Fellow, the Center for Advanced Studies
IBM Toronto Laboratory, Canada
E-mail: patrick.hung@uoit.ca

“Middleware is computer software that connects software components or applications. The software consists of a set of enabling services that allow multiple processes running on one or more machines to interact across a network. This technology evolved to provide for interoperability in support of the move to client/server architecture. It is used most often to support complex, distributed applications. It includes web servers, application servers, content management systems, and similar tools that support application development and delivery. Middleware is especially integral to modern information technology based on XML, SOAP, Web services, and service-oriented architecture.”

Online: <http://en.wikipedia.org/wiki/Middleware>

eXtensible Markup Language

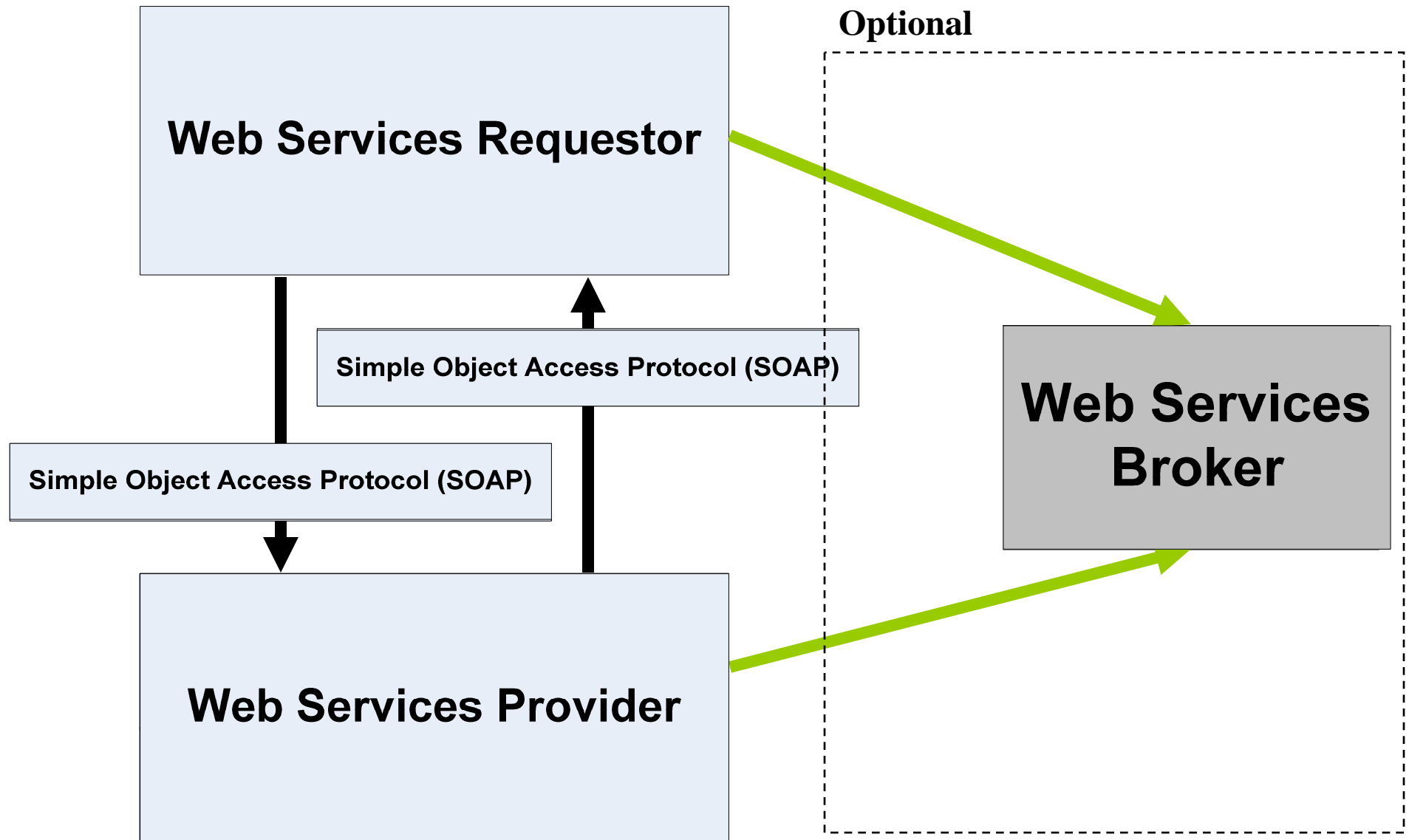
- Use XML as a data transport protocol
- Designed for machine-readable format
- Regular structure, and fine-grained data
- W3C Standard <http://www.w3c.org/XML/>



Ref: Gary Schneider, Electronic Commerce, Sixth Edition
Course Technology Incorporated, 2006, ISBN 0-619-21704-9

FIGURE 2-5 Development of markup languages

Services Oriented Architecture



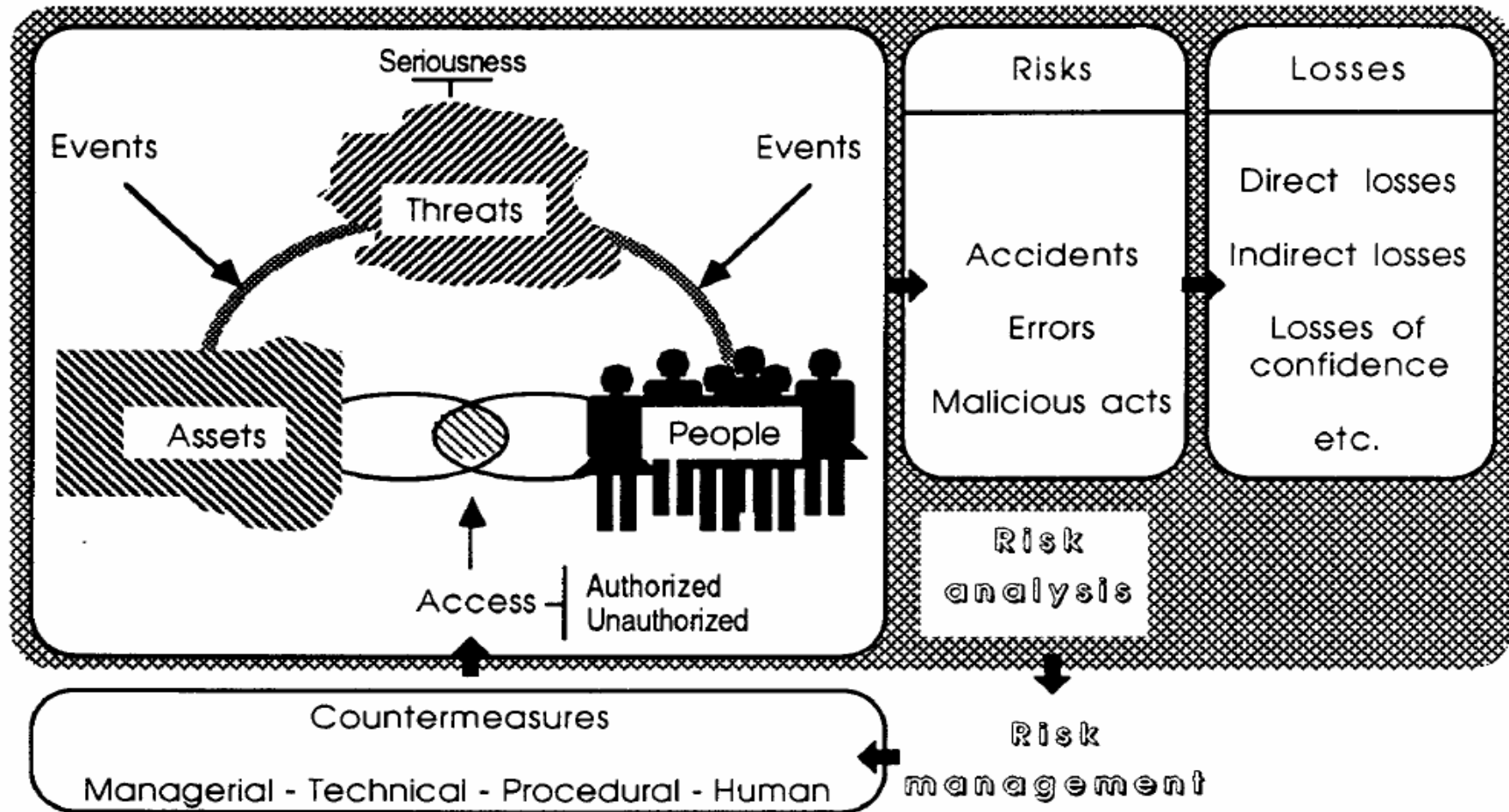
- Private Information may be managed by a (distributed) middleware system.
 - The middleware's core should constitute an access control enforcement on private information.
 - Protecting private information is always seen as enhancing the reputation and goodwill, value-added service/product, and benefiting stakeholders of the organization.
-

- ■ Privacy protection of private information requires integration at three levels:
 - ■ Organizational level: senior management needs to appreciate that a proper privacy policy will benefit its business.
 - ■ Legal level: need understanding of applicable laws.
 - ■ Technical level: measures and technologies for data security must be adopted to protect private information from improper access while it is being collected, stored, used, processed, and transferred.
-

Threat and Risk Analysis

- Threat and Risk Analysis (TRA) helps organizations understand vulnerabilities they have, threats they face, and the possibility that they may be exploited.
 - *Vulnerability*: any weakness found in systems, either through design, configuration, or implementation, that could be exploited
 - *Threats*: actions that could be implemented against systems to disrupt their good operation by breaching existing security measures and exploiting their vulnerabilities.
 - *Attacks*: threats acted upon – have a direct impact on confidentiality, integrity, and availability of the organization’s information assets.
 - The risk of each threat is evaluated against destruction, modification, and disclosure of information and the impact this will have on confidentiality, integrity, and availability of data.
-

Risk Analysis



Adapted from: Guinier, D. 1992. Object-oriented software for auditing information systems security: following a methodology for IS risk analysis and optimisation per level. ACM SIGSAC Review, Volume 10, Issue 4, Pages 22-30.

Risk Management Model

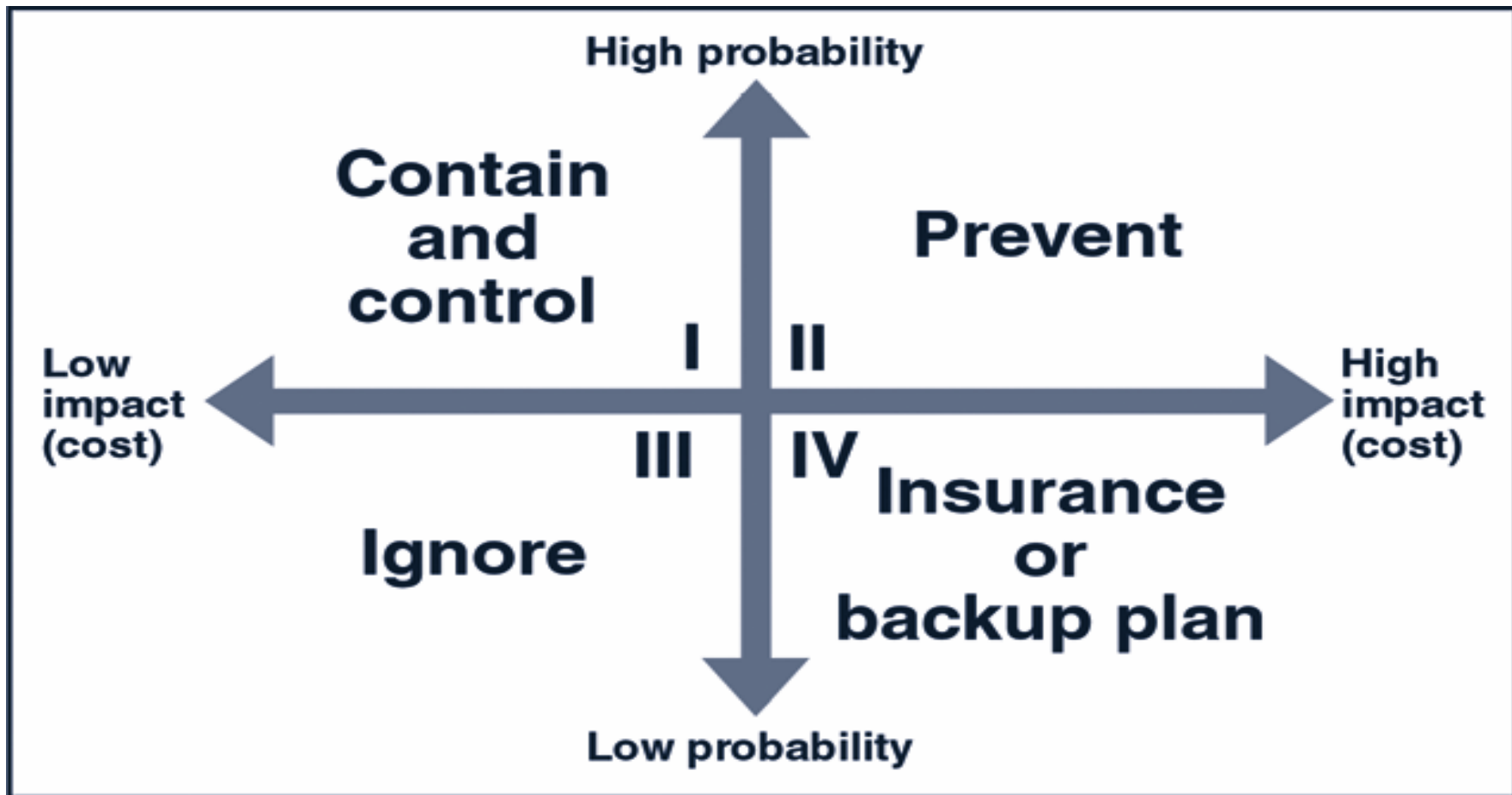


FIGURE 10-1 Risk management model

Adapted from: Gary Schneider, Electronic Commerce, Sixth Edition
Course Technology Incorporated, 2006, ISBN 0-619-21704-9

Introduction to Privacy

■ ■ Privacy is a state or condition of limited access to a person.

Ref: SCHOEMAN, E. D. 1984. Philosophical Dimensions of Privacy: An Anthology. New York, NY, Cambridge Univ. Press.

■ ■ Information privacy relates to an individual's right to determine how, when, and to what extent information about the self will be released to another person or to an organization.

■ ■ Consumers or even organizations often indicate that the privacy of their sensitive information is their foremost concern with the data transactions.

Introduction to Privacy (cont.)

■ ■ Web Firms Choose Profit Over Privacy - Washington Post – July 1, 2003.

■ ■ “..., almost all companies promise not to sell consumer data. But many don't mention that such information is rented. This means that the list owner won't release the data to an outside marketer, but it will send messages to the list on the outsider's behalf...”

■ ■ Protecting the sensitive information over the “lawless” Internet is becoming more and more important nowadays.

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying <http://www.washingtonpost.com/ac2/wp-dyn/A54888-2003Jun30>. The page content includes the Washington Post logo, navigation tabs (Home, News, On Politics, Entertainment, Live Online, Camera Works, Marketplace, Jobs), and a main article titled "Web Firms Choose Profit Over Privacy" by Jonathan Krim, a Washington Post Staff Writer, published on Tuesday, July 1, 2003, on page A01. The article text reads: "To parents interested in buying the popular Hooked on Phonics learn-to-read programs, the company made a firm promise on its Web site: It would never sell or rent their personal information to other marketers. But that pledge was empty. In the pages of a marketing trade publication, Gateway Learning Corp., the product's California-based parent company, was advertising to rent the list of Hooked on Phonics buyers to other". The browser interface also shows a search bar with "News" entered, a sidebar with "TechNews.com" navigation links, and several advertisements, including one for Lotus software and another for Cisco Systems.

Introduction to Privacy (cont.)



- ■ The US relies mostly on self-regulation and limited legislation.
- ■ The Privacy Act of 1974 requires that federal agencies:
 - ■ Grant individuals access to their identifiable records that are maintained by the agency;
 - ■ Ensure that existing information is accurate and timely and limit the collection of unnecessary information; and
 - ■ Limit the disclosure of identifiable information to third parties.

Ref: DAVIS, J. C. 2000. Protecting Privacy in the Cyber Era. IEEE Technology and Society Magazine, Summer 2000, 10-22.

■ ■ Two of the requirements of the Europe Union Data Protection Directive are:

- ■ An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization and the types of third parties to which it discloses the information.
 - ■ Personal data on EU citizens may only be transferred to countries outside the 27 nation block that adopt these rules or are deemed to provide “adequate protection” for the data.
-

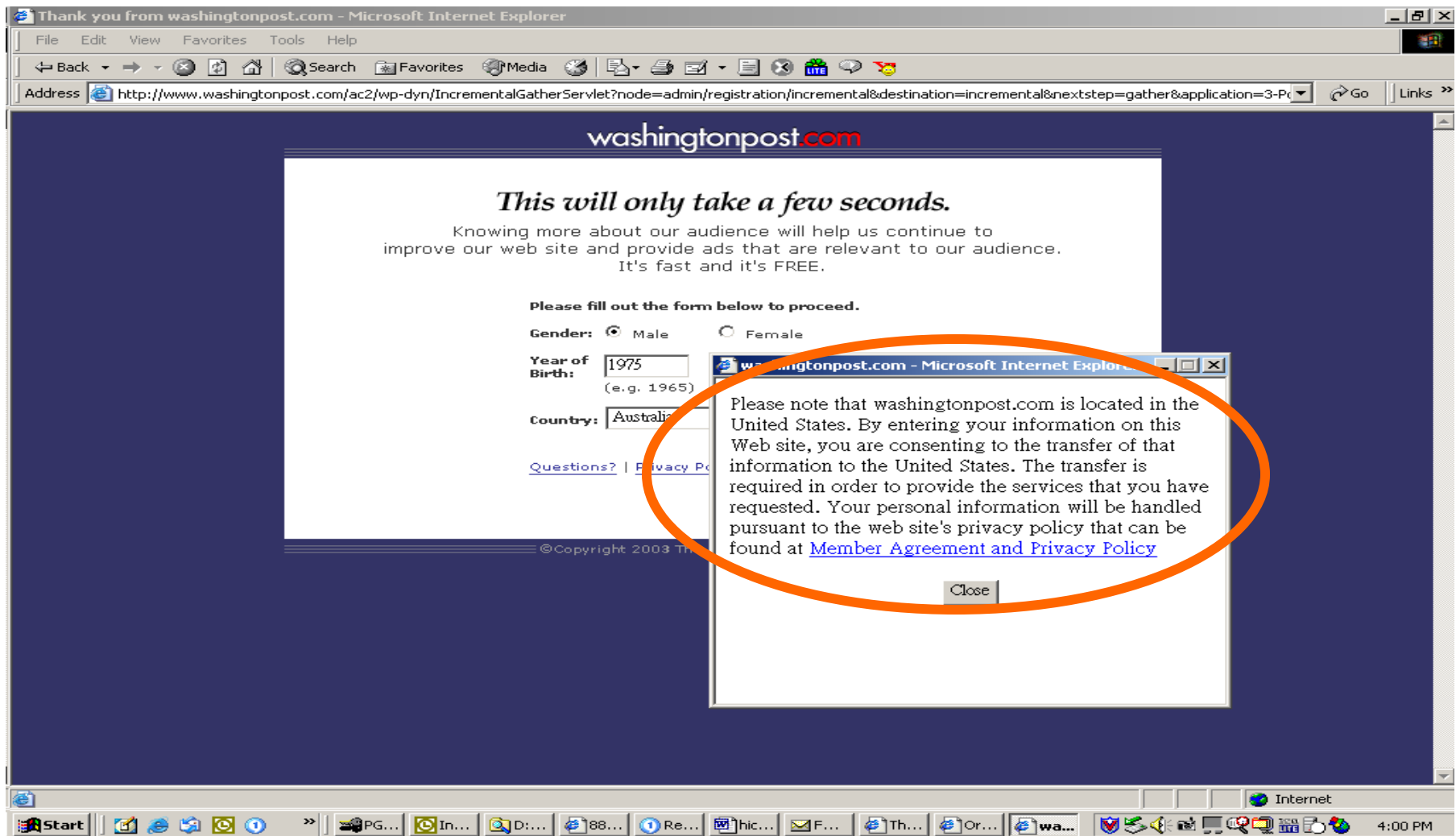
Introduction to Privacy (cont.)

- ■ The US government already has a voluntary scheme called “Safe Harbour” to provide an adequate level of data protection which can safeguard transfers of personal data to the US from Europe.

- ■ The US companies doing business in the EU must certify to the Commerce Department that they will follow the regulations of the EU directive.

- ■ Any violation would be subject to prosecution by the Federal Trade Commission (FTC) for deceptive business practices.

Introduction to Privacy (cont.)



Thank you from washingtonpost.com - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.washingtonpost.com/ac2/wp-dyn/IncrementalGatherServlet?node=admin/registration/incremental&destination=incremental&nextstep=gather&application=3-Pr> Go Links >>

washingtonpost.com

This will only take a few seconds.

Knowing more about our audience will help us continue to improve our web site and provide ads that are relevant to our audience. It's fast and it's FREE.

Please fill out the form below to proceed.

Gender: Male Female

Year of Birth:
(e.g. 1965)

Country:

[Questions?](#) | [Privacy Policy](#)

© Copyright 2003 The Washington Post Company

Please note that washingtonpost.com is located in the United States. By entering your information on this Web site, you are consenting to the transfer of that information to the United States. The transfer is required in order to provide the services that you have requested. Your personal information will be handled pursuant to the web site's privacy policy that can be found at [Member Agreement and Privacy Policy](#)

Close

Start | PG... | In... | D:... | 88... | Re... | hic... | F... | Th... | Or... | wa... | Internet | 4:00 PM

Sample Privacy Legislations

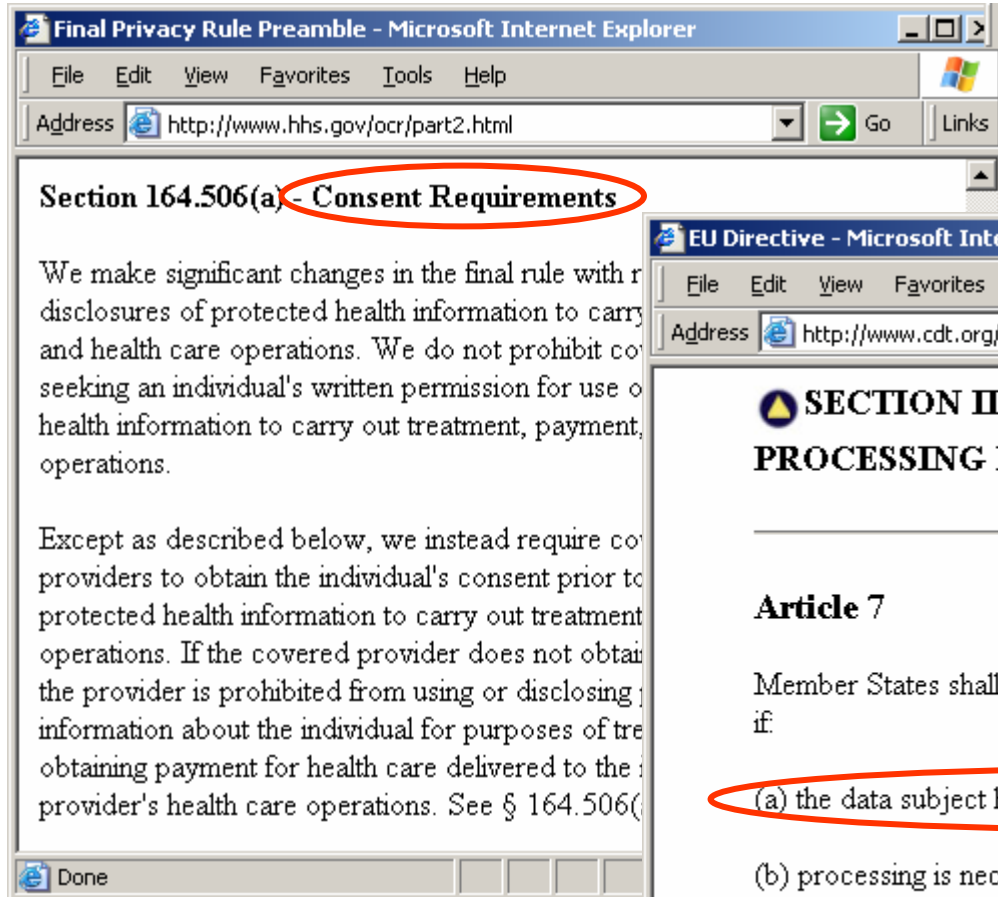


- ■ Australia
 - ■ National Health Act in 1953
 - ■ Privacy Amendment Privacy Sector Act (PAPSA) in 1998
 - ■ Canada
 - ■ Privacy Act in 1983
 - ■ Personal Information Protection and Electronic Documents Act (PIPEDA) in 2004
 - ■ European Union
 - ■ The European Data Privacy Directive in 1998
 - ■ Hong Kong
 - ■ Personal Data (Privacy) Ordinance (PD(P)O) in 1995
 - ■ United States
 - ■ Health Insurance Portability and Accountability Act of 1996 (HIPAA) in 2004
-

6 HIPAA Privacy Rules

- 1. The right to access, copy, and inspect a patient's own PHI.*
 - 2. The right to request the correction of any inaccurate health information.*
 - 3. The right to find out where PHI has been shared for purposes other than care, payment, or healthcare operations.*
 - 4. The right to request special restrictions on the use or disclosure of PHI.*
 - 5. The right to request confidential communications of PHI, for example, to a certain address or a certain telephone number.*
 - 6. The right to file complaints.*
-

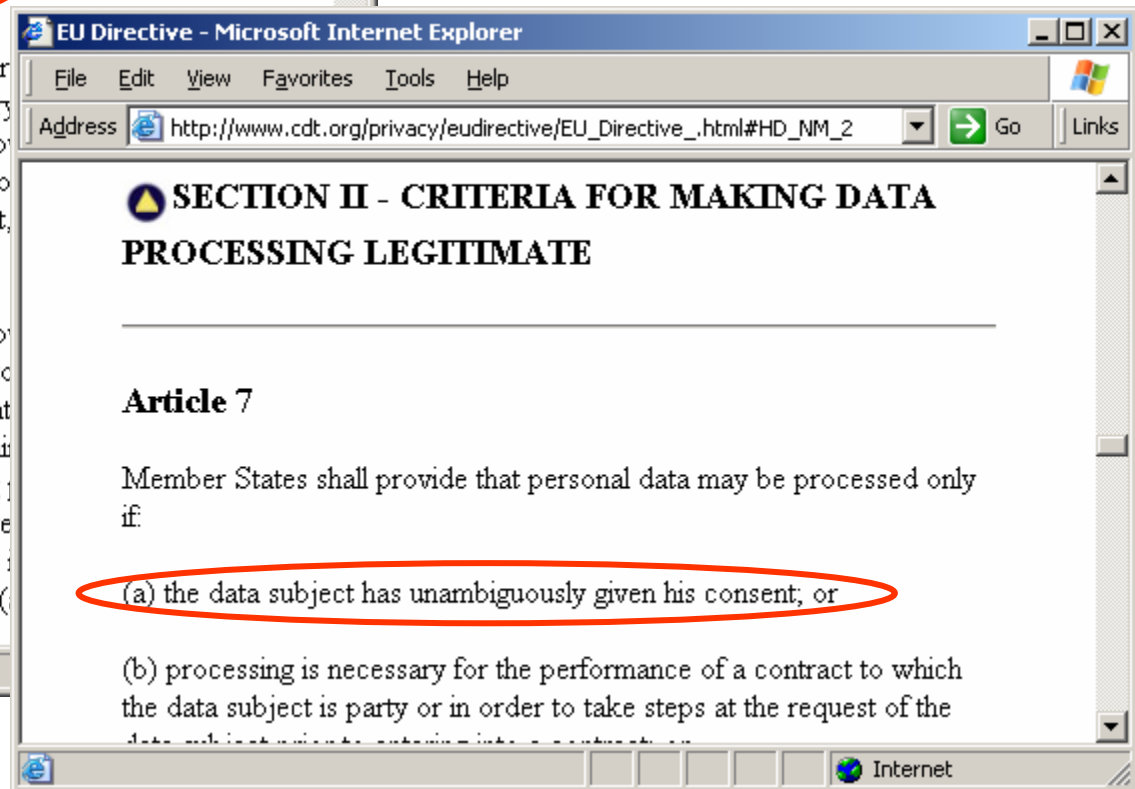
Consent Requirement



Section 164.506(a) - Consent Requirements

We make significant changes in the final rule with r disclosures of protected health information to carry and health care operations. We do not prohibit co seeking an individual's written permission for use o health information to carry out treatment, payment, operations.

Except as described below, we instead require co providers to obtain the individual's consent prior to protected health information to carry out treatment operations. If the covered provider does not obtai the provider is prohibited from using or disclosing information about the individual for purposes of tre obtaining payment for health care delivered to the provider's health care operations. See § 164.506(



SECTION II - CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE

Article 7

Member States shall provide that personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract on

Purpose

Privacy Act - Microsoft Internet Explorer
Address: http://laws.justice.gc.ca/en/P-21/255

Definitions

3. In this Act,

"administrative purpose", in relation to the personal information about an individual, means information in a decision making process that directly affects that individual;

"alternative format", with respect to personal information, means a format that allows a person with a disability to access the information.

Privacy Act - Microsoft Internet Explorer
Address: http://laws.justice.gc.ca/en/P-21/255104.html#rid-255123

be disclosed to the institution under subsection 8(2).

Individual to be informed of purpose (2) A government institution shall inform any individual from whom the institution collects personal information about the individual of the purpose for which the information is being collected.

Exception (3) Subsections (1) and (2) do not apply where compliance therewith might

(a) result in the collection of inaccurate information; or

PCO - The Ordinance at a Glance 1 - Microsoft Internet Explorer
Address: http://www.pco.org.hk/english/ordinance/ordglance1.html#dataprotect

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.

Principle 2 -- Accuracy and duration of retention This provides that personal data should be accurate, up to date and relevant.

EU Directive - Microsoft Internet Explorer
Address: http://www.cdt.org/privacy/eudirective/EU_Directive_.html#HI

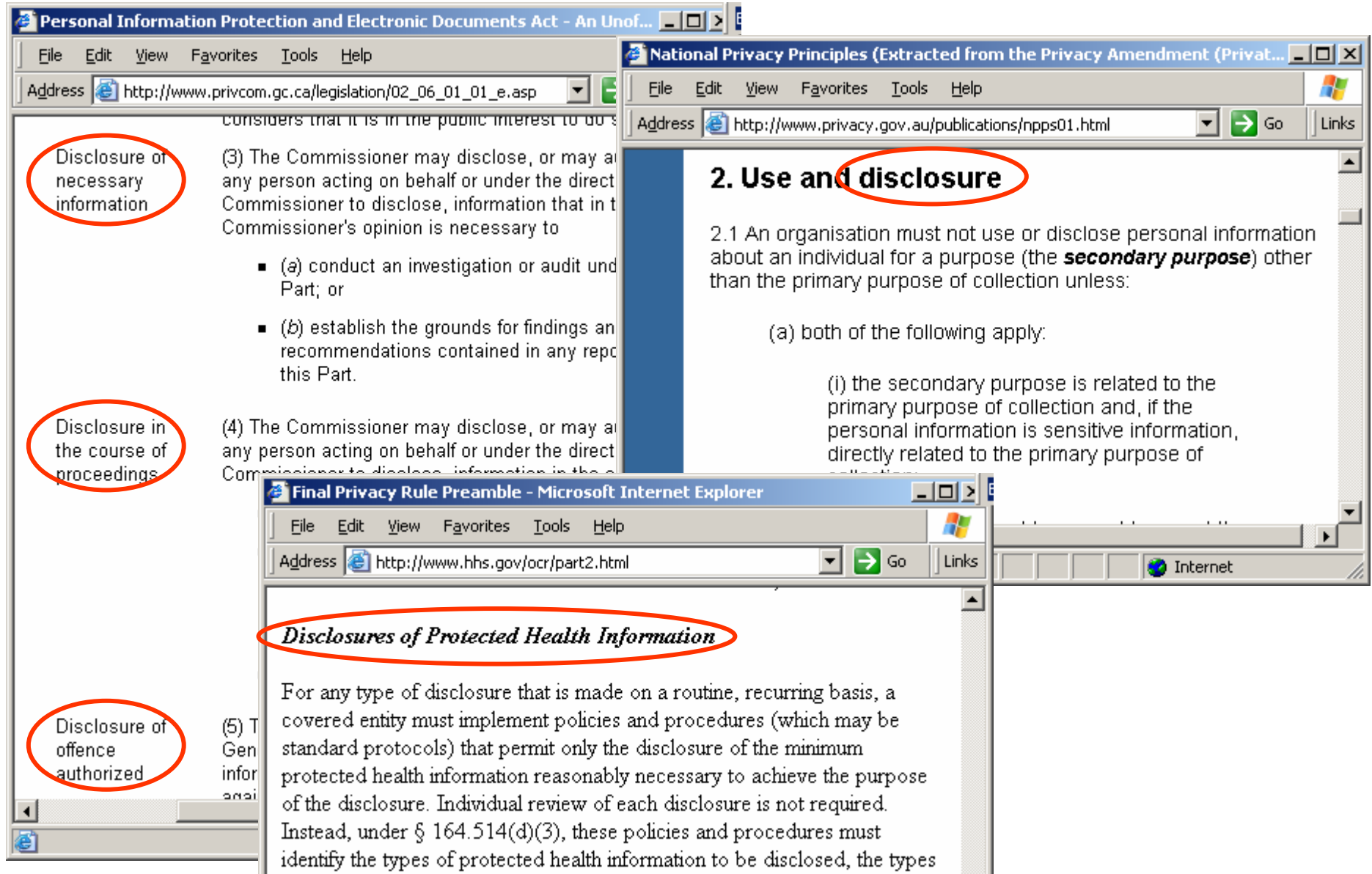
Article 10 Information in cases of collection of data from the data subject

Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

Disclosure (Recipients)



Personal Information Protection and Electronic Documents Act - An Unof...
Address: http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp

considers that it is in the public interest to do s

Disclosure of necessary information

(3) The Commissioner may disclose, or may allow any person acting on behalf or under the direct authority of the Commissioner to disclose, information that in the Commissioner's opinion is necessary to

- (a) conduct an investigation or audit under this Part; or
- (b) establish the grounds for findings and recommendations contained in any report under this Part.

Disclosure in the course of proceedings

(4) The Commissioner may disclose, or may allow any person acting on behalf or under the direct authority of the Commissioner to disclose, information in the course of proceedings.

Disclosure of offence authorized

(5) The Commissioner may disclose, or may allow any person acting on behalf or under the direct authority of the Commissioner to disclose, information in the course of proceedings.

National Privacy Principles (Extracted from the Privacy Amendment (Privat...
Address: <http://www.privacy.gov.au/publications/npps01.html>

2. Use and disclosure

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the **secondary purpose**) other than the primary purpose of collection unless:

(a) both of the following apply:

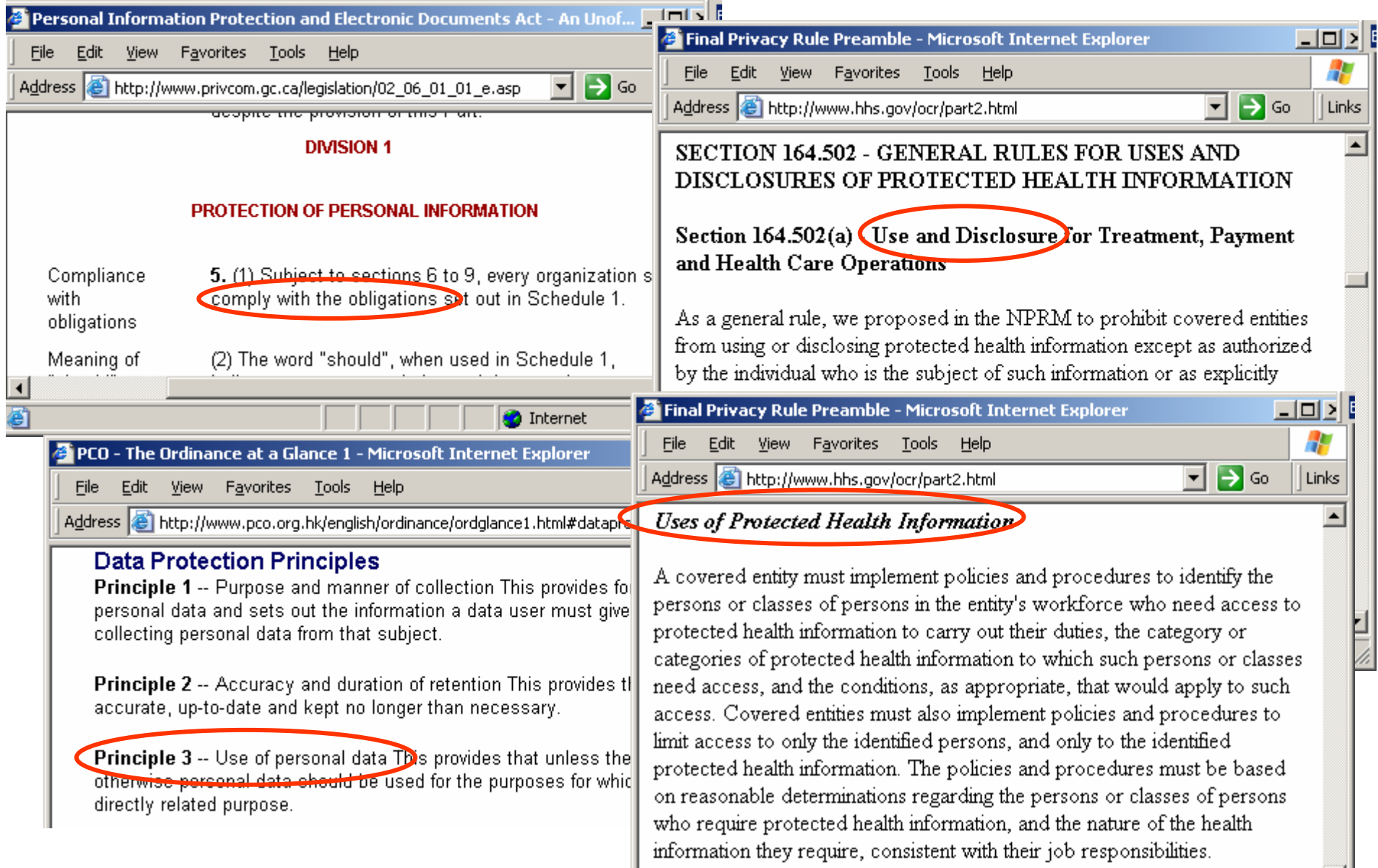
(i) the secondary purpose is related to the primary purpose of collection and, if the personal information is sensitive information, directly related to the primary purpose of collection.

Final Privacy Rule Preamble - Microsoft Internet Explorer
Address: <http://www.hhs.gov/ocr/part2.html>

Disclosures of Protected Health Information

For any type of disclosure that is made on a routine, recurring basis, a covered entity must implement policies and procedures (which may be standard protocols) that permit only the disclosure of the minimum protected health information reasonably necessary to achieve the purpose of the disclosure. Individual review of each disclosure is not required. Instead, under § 164.514(d)(3), these policies and procedures must identify the types of protected health information to be disclosed, the types

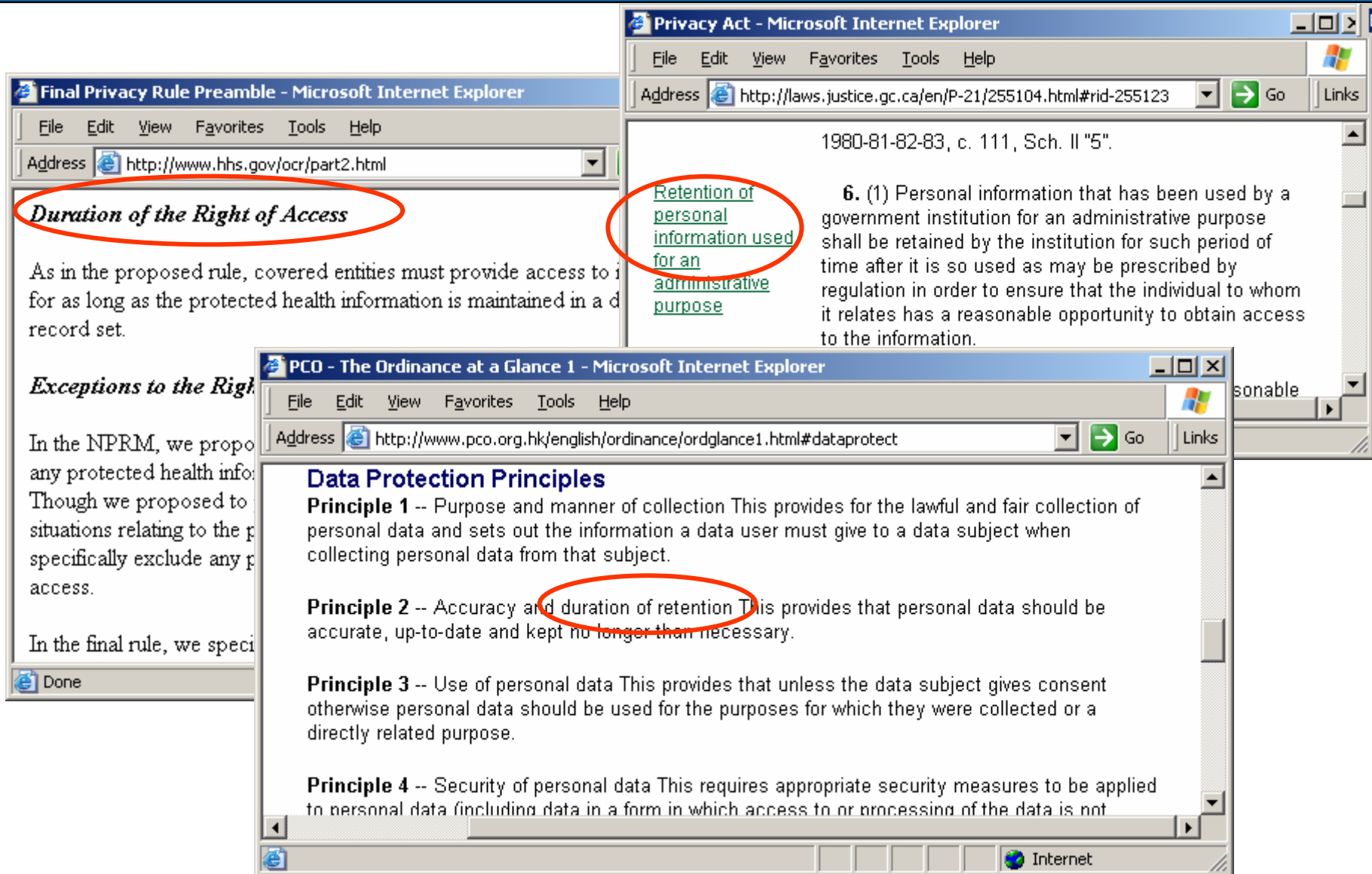
Use (Obligations in use)



The image displays four overlapping web browser windows, each showing a different document related to privacy and health information regulations.

- Top-left window:** "Personal Information Protection and Electronic Documents Act - An Unof...". The address bar shows http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp. The content includes "DIVISION 1" and "PROTECTION OF PERSONAL INFORMATION". A table lists "Compliance with obligations" and "Meaning of". The text for "Compliance with obligations" states: "5. (1) Subject to sections 6 to 9, every organization s comply with the obligations set out in Schedule 1." The text for "Meaning of" states: "(2) The word 'should', when used in Schedule 1,".
- Top-right window:** "Final Privacy Rule Preamble - Microsoft Internet Explorer". The address bar shows <http://www.hhs.gov/ocr/part2.html>. The content includes "SECTION 164.502 - GENERAL RULES FOR USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION". A sub-section is titled "Section 164.502(a) Use and Disclosure for Treatment, Payment and Health Care Operations". The text below states: "As a general rule, we proposed in the NPRM to prohibit covered entities from using or disclosing protected health information except as authorized by the individual who is the subject of such information or as explicitly".
- Bottom-left window:** "PCO - The Ordinance at a Glance 1 - Microsoft Internet Explorer". The address bar shows <http://www.pco.org.hk/english/ordinance/ordglance1.html#datapri>. The content includes "Data Protection Principles". "Principle 1" is about purpose and manner of collection. "Principle 2" is about accuracy and duration of retention. "Principle 3" is about use of personal data: "Principle 3 -- Use of personal data This provides that unless the otherwise personal data should be used for the purposes for which directly related purpose."
- Bottom-right window:** "Final Privacy Rule Preamble - Microsoft Internet Explorer". The address bar shows <http://www.hhs.gov/ocr/part2.html>. The content includes "Uses of Protected Health Information". The text states: "A covered entity must implement policies and procedures to identify the persons or classes of persons in the entity's workforce who need access to protected health information to carry out their duties, the category or categories of protected health information to which such persons or classes need access, and the conditions, as appropriate, that would apply to such access. Covered entities must also implement policies and procedures to limit access to only the identified persons, and only to the identified protected health information. The policies and procedures must be based on reasonable determinations regarding the persons or classes of persons who require protected health information, and the nature of the health information they require, consistent with their job responsibilities."

Retention



Final Privacy Rule Preamble - Microsoft Internet Explorer
Address: <http://www.hhs.gov/ocr/part2.html>
Duration of the Right of Access
As in the proposed rule, covered entities must provide access to information for as long as the protected health information is maintained in a data record set.

Privacy Act - Microsoft Internet Explorer
Address: <http://laws.justice.gc.ca/en/P-21/255104.html#rid-255123>
1980-81-82-83, c. 111, Sch. II "5".
[Retention of personal information used for an administrative purpose](#)
6. (1) Personal information that has been used by a government institution for an administrative purpose shall be retained by the institution for such period of time after it is so used as may be prescribed by regulation in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information.

PCO - The Ordinance at a Glance 1 - Microsoft Internet Explorer
Address: <http://www.pco.org.hk/english/ordinance/ordglance1.html#dataprotect>
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.
Principle 2 -- Accuracy and duration of retention This provides that personal data should be accurate, up-to-date and kept no longer than necessary.
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.
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

- Principle 1: Data-level security protection principle
- Principle 2: Communication-level security protection principle
- Principle 3: Consent requirement principle
 1. Limitation on Purpose of Collection
 2. Limitation on Data Disclosure
 3. Limitation on Use
 4. Limitation on Retention

Cheng, V. S. Y., and Hung, P. C. K. 2005.

*Privacy Principles for Developing Multi-legislation Compliant E-healthcare Web Services Applications
In the Proceeding of the Fourth Workshop on e-Business (WeB2005)*

- ■ In general, privacy policies describe an organization's data practices what information they collect from individuals/ organizations and what (e.g., purposes) they do with it.

- ■ Need a *Privacy Policy* for Web services:

- ■ A document that expresses clearly and concisely what the data protection mechanisms are to achieve.

- ■ A statement of the privacy the requestor expect the Web services to enforce.

- ■ Privacy policies must be implemented in the Web Services Architecture (WSA).

Web Services Architecture

- ❑ **AC020** enables privacy protection for the consumer of a Web service across multiple domains and services.
 - ❑ **AR020.1** the WSA must enable privacy policy statements to be expressed about Web services.
 - ❑ **AR020.2** advertised Web service privacy policies must be expressed in P3P.
 - ❑ **AR020.3** the WSA must enable a consumer to access a Web service's advertised privacy policy statement.
 - ❑ **AR020.5** the WSA must enable delegation and propagation of privacy policy.
 - ❑ **AR020.6** Web Services must not be precluded from supporting interactions where one or more parties of the interaction are anonymous.

Web Services Architecture Requirements: W3C Working Group Note 11 February 2004

Online: www.w3.org/TR/2002/WD-wsa-reqs-20021114
www.w3.org/TR/2004/NOTE-wsa-reqs-20040211

Web Services Architecture

A permissive policy concerns those actions and accesses that entities are permitted to perform and an obligation policy concerns those actions and states that entities are required to perform.

...

The two kinds of policies have different enforcement mechanisms: a permission guard is a mechanism that can be used to verify that a requested action or access is permitted; an audit guard can only verify after the fact that an obligation has not been met.

...

Web Services Architecture: W3C Working Group Note 11 February 2004

Online: <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>

Web Services Architecture

...

A permission guard acts as a guard enabling or disabling action to a resource or action. In the context of SOAP, for example, one important role of SOAP intermediaries is that of permission guards: the intermediary may not, in fact, forward a message if some security policy is violated.

...

An audit guard acts as a monitor; watching resources and agents, validating that obligations that have been established are respected and/or discharged. Due to the nature of obligations it is often not possible to prevent obligations; instead the focus is on observing that obligations are respected. If an audit guard detects a policy violation, then it normally cannot prevent the violation; instead some form of retribution or remediation must be enacted. The precise forms of this are, of course, beyond the scope of this architecture.

...

Web Services Architecture: W3C Working Group Note 11 February 2004

Online: <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>

3.6.5 Privacy Considerations

Issue (privacy_needs_more_work):

The relationship between privacy and Web services technology needs clarification.

There is considerably more complexity to privacy than treated in this section.

Resolution:

None recorded.

Privacy policies are typically much more of the obligatory form than access control policies. A policy that requires a provider agent to properly propagate P3P tags, for example, represents an obligation on the provider entity. However, it is not possible to prevent a rogue provider agent from leaking private information. Thus, it should be possible to monitor the public actions of the Web service to verify that the P3P tags are propagated appropriately.

Web Services Architecture: W3C Working Group Note 11 February 2004

Online: <http://www.w3.org/TR/2004/NOTE-ws-arch-20040211/>

Platform for Privacy Preferences Project (P3P)

- **Developed by the World Wide Web Consortium (W3C)**
 - ★ Final P3P1.0 Recommendation issued 16 April 2002
- **Allows web sites to communicate about their privacy policies in a standard computer-readable format**
 - ★ Does not require web sites to change their server software
- **Enables the development of tools (built into browsers or separate applications) that**
 - ★ Summarize privacy policies
 - ★ Compare privacy policies with user preferences
 - ★ Alert and advise users
- **P3P helps users understand privacy policies**
 - ★ P3P increases transparency, but it does not set baseline standards or enforce policies
- **P3P user agent software available (as of July 2002)**
 - ★ Microsoft Internet Explorer 6
 - ★ Netscape Navigator 7
 - ★ AT&T Privacy Bird
<http://privacybird.com/>
- **For more information**
 - ★ <http://www.w3.org/P3P/>
 - ★ <http://p3ptoolbox.org/>
 - ★ *Web Privacy with P3P*
by Lorrie Faith Cranor
<http://p3pbook.com/>

Web Services Privacy (cont.)

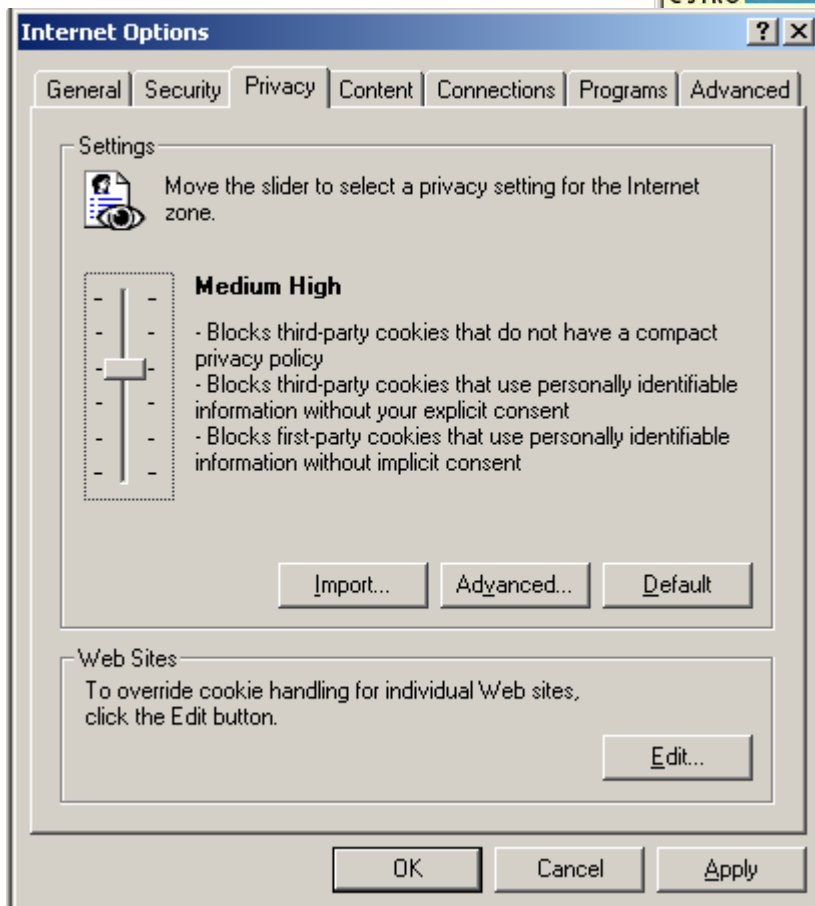
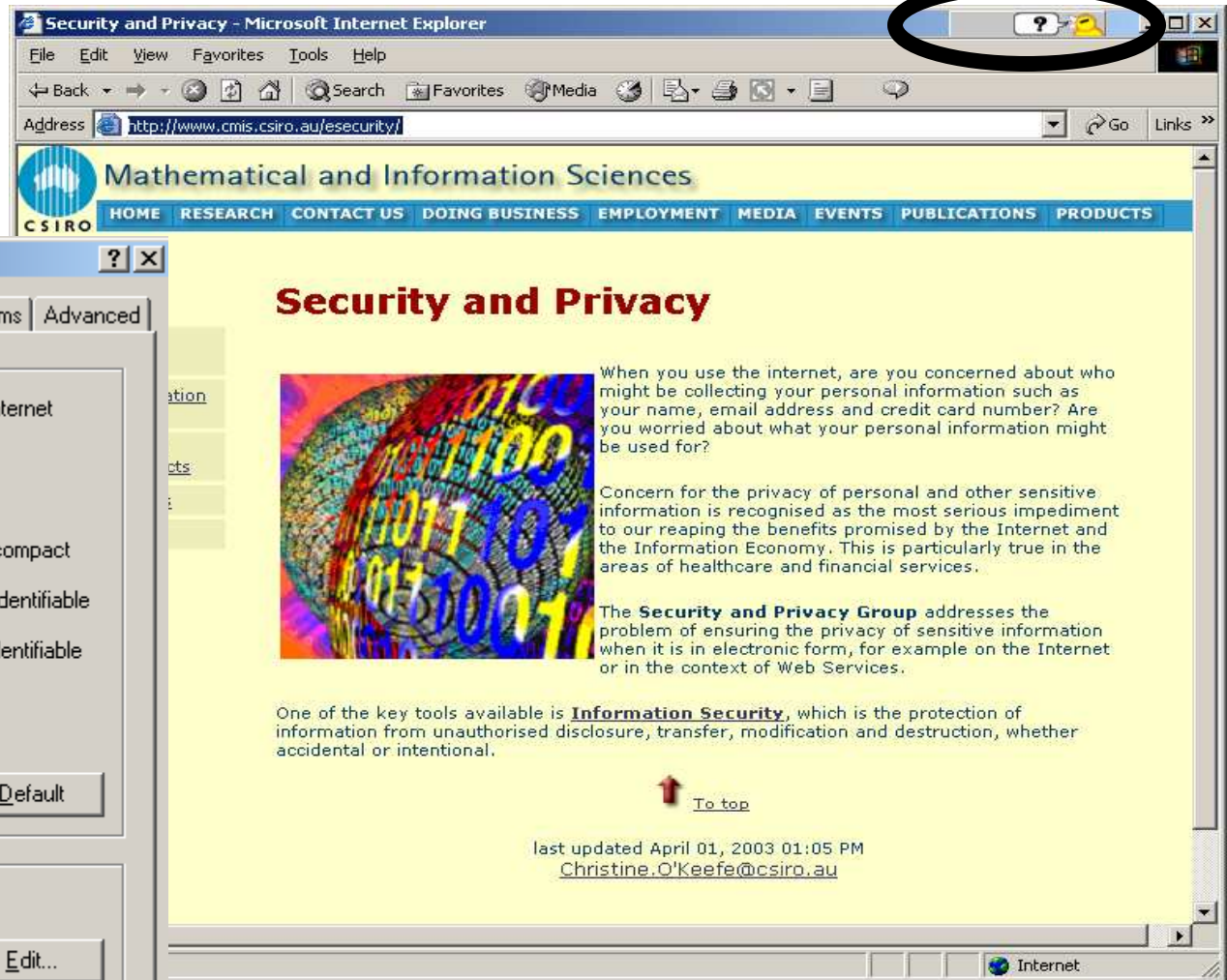
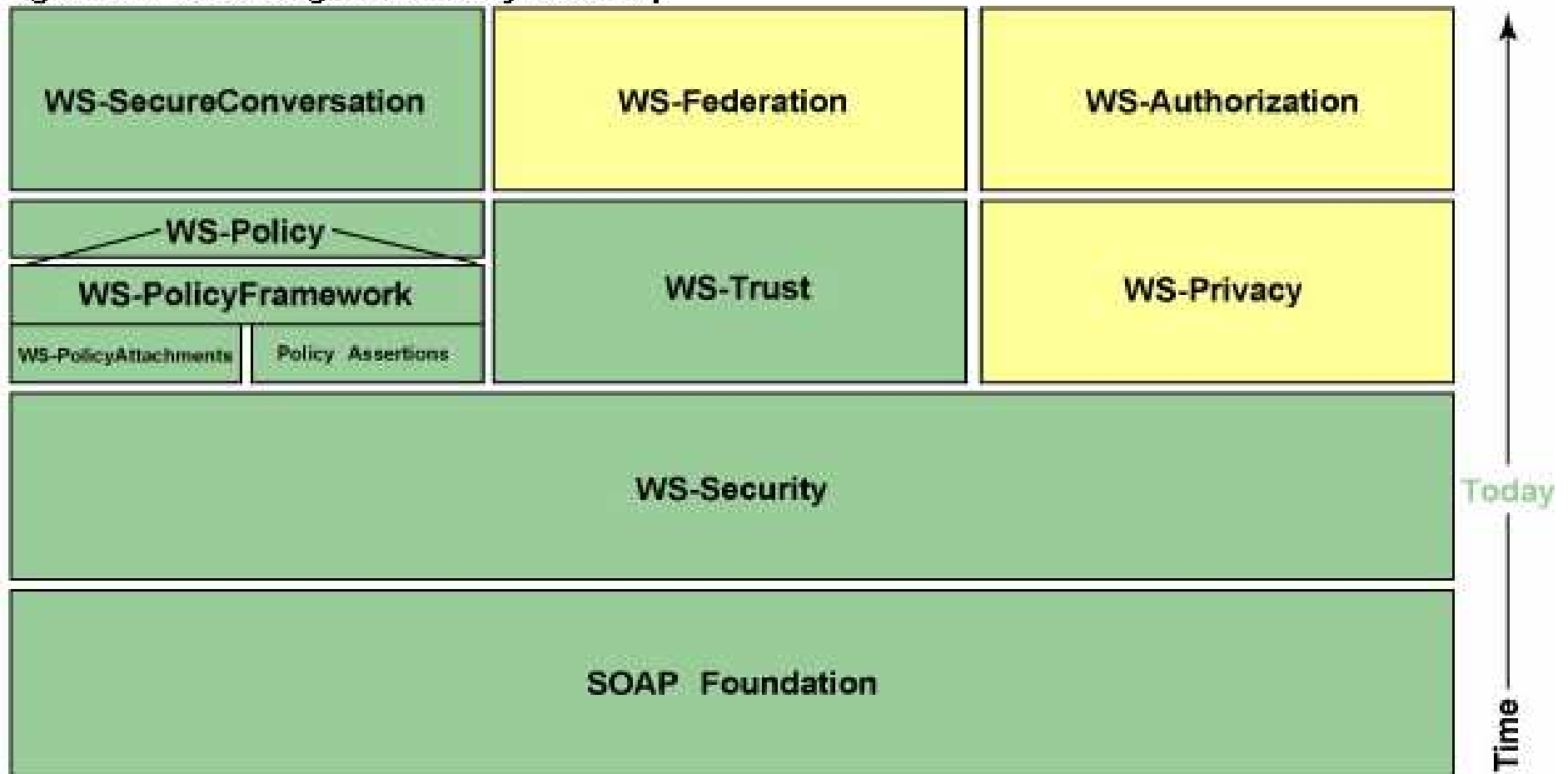


Figure 1. The evolving WS-Security Roadmap



Adapted from: IBM CORPORATION. 2002. Security in a Web Services World: A Proposed Architecture and Roadmap, White Paper, Version 1.0.

<http://www-106.ibm.com/developerworks/library/ws-secroad/>

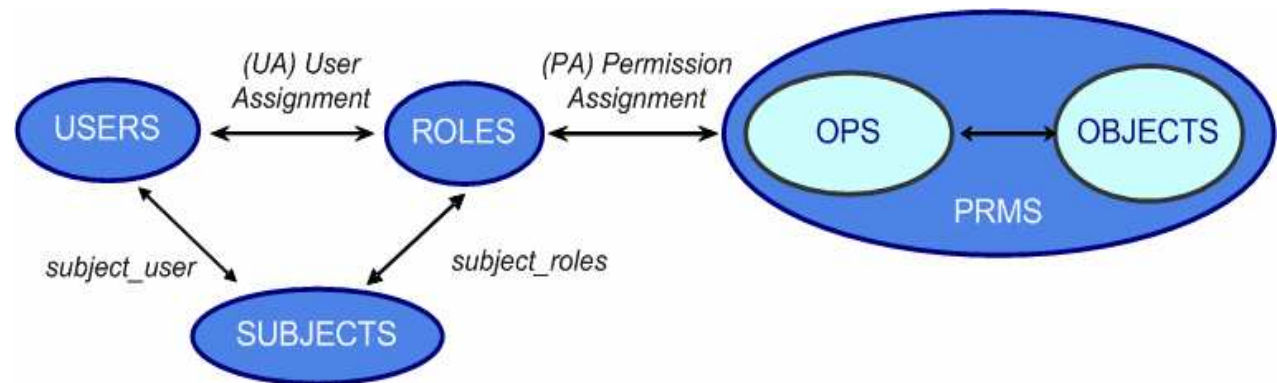
Access control is used to monitor whether or not a user has proper permission to access a particular object (e.g. a file), or to perform a particular operation assuming that the user is successfully authenticated.

A typical access control model involves querying for membership in a particular user group, possession of a particular clearance, or looking for that user on a resource's approved access control list.

Beside all, privacy level determination in access control is also based on:

- ▣ Regulations
 - ▣ User privacy preferences
-

Role-Based Access Control (RBAC)



Core RBAC Model



American National Standard 359-2004 is the Information Technology industry consensus standard for RBAC

Adapted from: David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn and Ramaswamy Chandramouli, "Proposed NIST Standard for Role-Based Access Control, *ACM Transactions on Information and Systems Security (TISSEC)*," Volume 4, Number 3, August 2001.

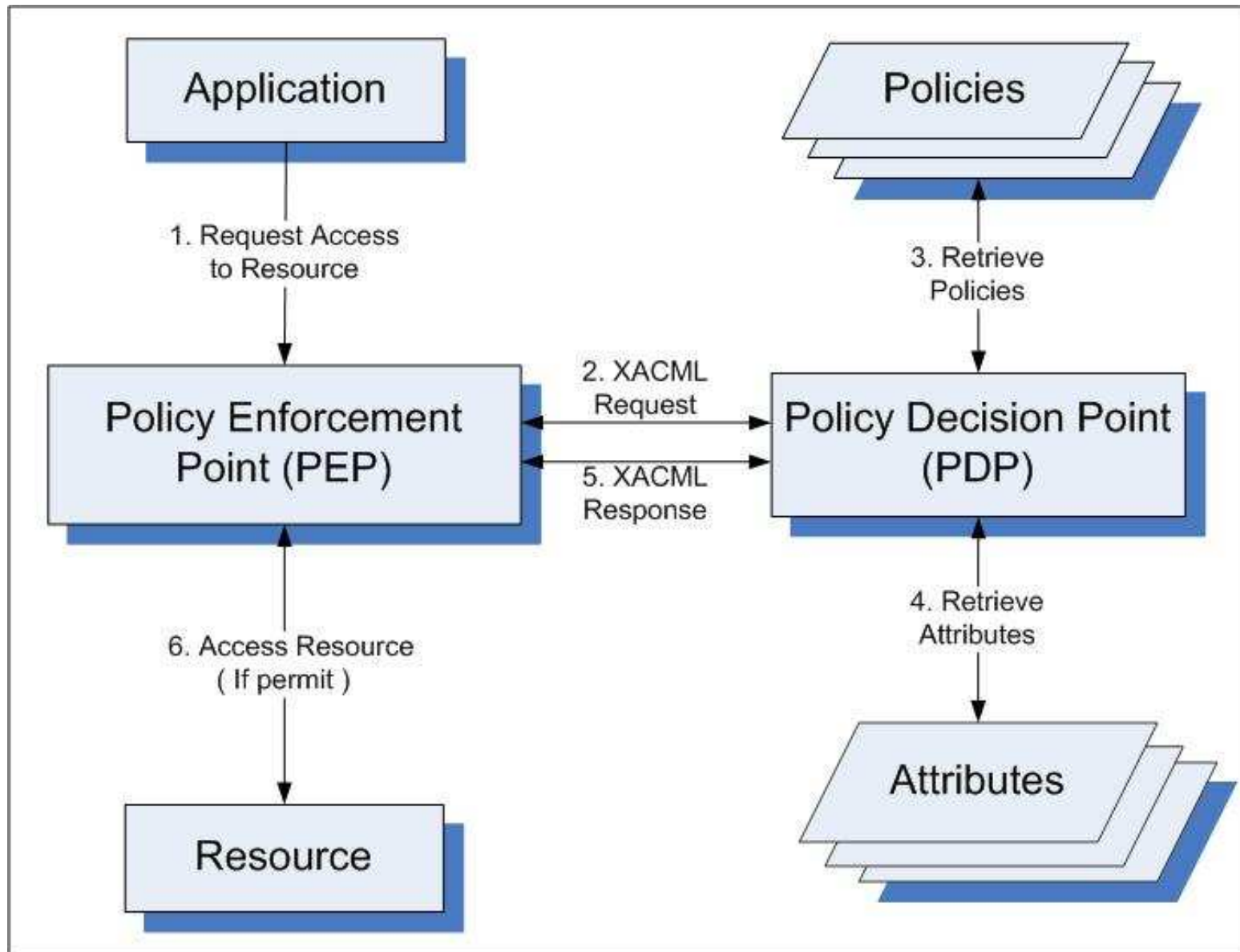
■ ■ eXtensible Access Control Markup Language (XACML) is a general-purpose access control policy language used to describe policy and access control decision requests/responses.

■ ■ The XACML is designed to support both centralized and decentralized policy management.

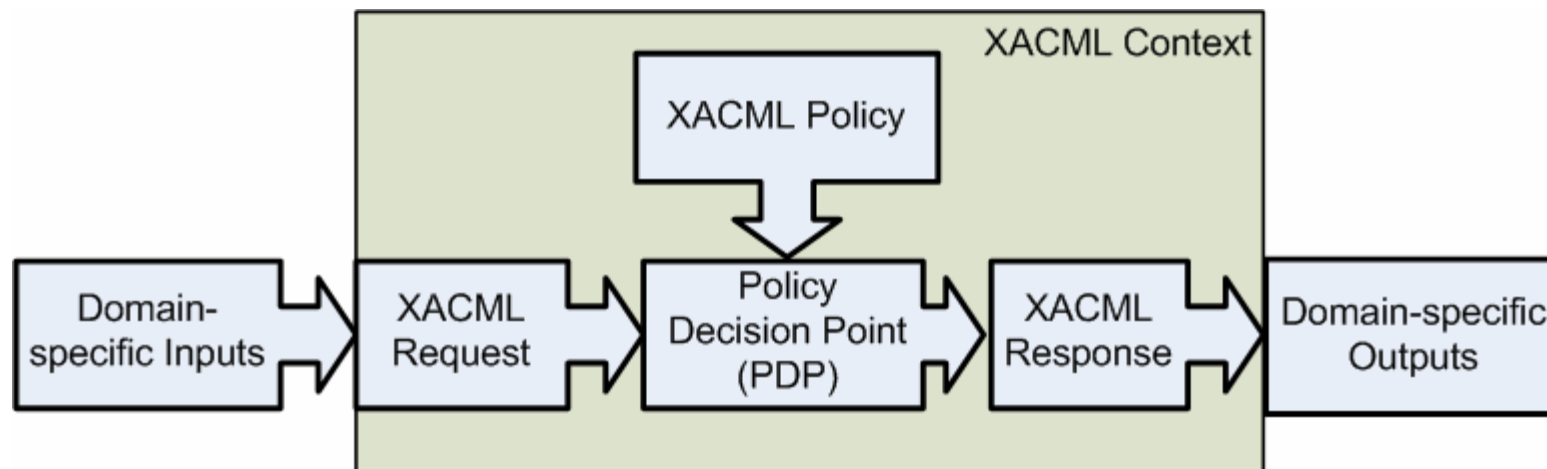
■ ■ With the support of policy assertions, XACML can be extended into a more comprehensive solution for expressing the policies.

- ■ The Internet Engineering Task Force (IETF) defines an abstract model for policy enforcement which is applied by eXtensible Access Control Markup Language (XACML):
 - ■ *Policy Decision Point (PDP)*: The point where policy decisions are made.
 - ■ *Policy Enforcement Point (PEP)*: It is the logical entity or place on a server that enforces policies for admission control and policy decisions in response to a request wanting to access a resource on a computer or network server.
 - ■ *Resource*: Something of value in a network infrastructure to which rules or policy criteria are first applied, before access is granted.
 - ■ *Policies*: The combination of rules and services where rules define the criteria for resource access and usage.
-

The IETF Policy Enforcement Model

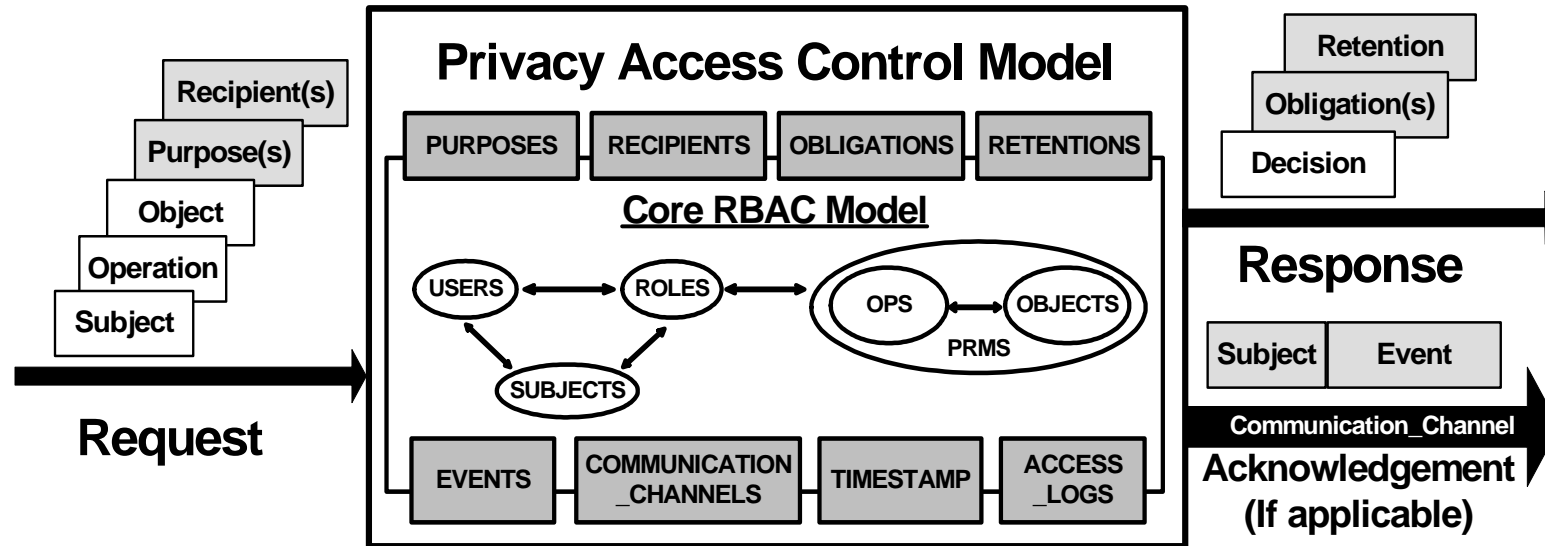


XACML and RBAC entities



Core RBAC Entities	XACML Implementation
USERS	<Subjects>
ROLES	<Subject Attributes>
OBJECTS	<Resources>
OPS	<Actions>
PRMS	<PolicySet> <Policy>

RBAC Entities with Extensions



Core RBAC Entities	XACML Implementation
USERS	<Subjects>
ROLES	<Subject Attributes>
OBJECTS	<Resources>
OPS	<Actions>
PRMS	<PolicySet>, <Policy>

Extended RBAC Entities	XACML Implementation
PURPOSES	<resource:purpose> <action:purpose>
RECIPIENTS	<Subjects>
OBLIGATIONS	<Obligations>
RETENTIONS	<Retentions>

Conclusions



- ■ *“On the Internet, nobody knows you’re a dog.”*
- ■ The New Yorker Collection 1993



The End

Thank you for your time!

