Legislative bases for personal privacy policy specification

Yee, George; Korba, Larry; Song, Ronggong

Publisher's version / Version de l'éditeur:

Privacy Protection for E-Services, 2006

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC · CNRC

*Legislative Bases for Personal Privacy Policy Specification **

Yee, G., Korba, L., and Song, R.
2006

* published in Privacy Protection for E-Services, published by Idea Group Inc. 2006. NRC 48270. Yee, G. (Editor)

Canada

Legislative Bases for Personal Privacy Policy Specification[1]

George Yee

National Research Council Canada
Institute for Information Technology
1200 Montreal Road, Building M-50
Ottawa, Ontario, Canada K1A 0R6
Phone: 613-990-4284
Fax: 613 952-7151
Email: George.Yee@nrc.ca

Larry Korba

National Research Council Canada
Institute for Information Technology
1200 Montreal Road, Building M-50
Ottawa, Ontario, Canada K1A 0R6
Phone: 613- 998-3967
Fax: 613 952-7151
Email: Larry.Korba@nrc.ca

Ronggong Song

National Research Council Canada
Institute for Information Technology
1200 Montreal Road, Building M-50
Ottawa, Ontario, Canada K1A 0R6
Phone: 613-990-6869
Fax: 613 952-7151
Email: Ronggong.Song@nrc.ca

Legislative Bases for Personal Privacy Policy Specification[1]

ABSTRACT

The growth of the Internet has been accompanied by a proliferation of e-services, especially in the area of e-commerce (e.g. Amazon.com, eBay.com). However, consumers of these e-services are becoming more and more sensitive to the fact that they are giving up private information every time they use them. At the same time, legislative bodies in many jurisdictions have enacted legislation to protect the privacy of individuals when they need to interact with organizations. As a result, e-services can only be successful if there is adequate protection for user privacy. The use of personal privacy policies to express an individual's privacy preferences appears best-suited to manage privacy for e-commerce. We first motivate the reader with our E-Service Privacy Policy Model that explains how personal privacy policies can be used for e-services. We then derive the minimum content of a personal privacy policy by examining some key privacy legislation selected from Canada, the European Union, and the United States.

KEYWORDS: privacy, privacy policy, personal privacy policy, privacy legislation, privacy rules, specification

INTRODUCTION

The rapid growth of the Internet has been accompanied by a proliferation of e-services targeting consumers. E-services are available for banking, shopping, learning, healthcare, government services, and many other areas. However, each of these services requires a consumer's personal information in one form or another. This leads to consumer concerns over unwarranted leakage, storage, and/or exploitation of their private information. Indeed, consumer savvy regarding their rights to privacy is increasing. In Canada, recent federal privacy legislation known as the Personal Information Protection and Electronic Documents Act (PIPEDA) (Government of Canada) has forced businesses to seek consumer permission before collecting personal information. Similar legislation exists in the European Union (European Union, 1995) and in the United States for health care (U.S. Government). In this light, e-services must respect consumers' personal privacy if they are to be successful.

A promising solution for management of private information in e-services is to employ consumer personal privacy policies, i.e. a consumer expresses his/her privacy preferences in a personal privacy policy. Once the e-service provider agrees with this privacy policy, it is then the provider's responsibility to comply with it. These are the basic tenets of our E-Service Privacy Policy Model (explained below to motivate the need for personal privacy policies). However, what should go into the personal privacy policy? In this work, we answer this question by examining privacy legislation from Canada, the European Union, and the United States. (Although we could have looked at privacy legislation in other countries as well, we settled on these three because our

audience is expected to be mostly from these regions and thus be subject to privacy legislation from them.) The result is the minimum personal privacy policy, i.e. one that contains the necessary elements to satisfy privacy legislation, but one that can contain extra privacy provisions according to consumer wishes. We shall indicate what some of these "extra provisions" could be. Policy-based management approaches have been used effectively to manage and control large distributed systems. As in any distributed system, e-services may also use a policy-based framework to manage the security and privacy aspects of operations.

For privacy policies, there are related works such as P3P (W3C), APPEL (W3C, 2002), PSP (Carnegie Mellon University), and EPAL (IBM) which are languages for expressing privacy preferences in policies. Web sites use P3P to divulge their privacy policies to consumers. APPEL is a specification language used to describe a consumer's privacy preferences for comparison with the privacy policy of a web site. PSP is a protocol in the research stage that provides a basis for policy negotiation. EPAL is a markup language for privacy preferences. These works are not necessary for the purposes of this chapter. They only serve as illustrations of what has been done in the related area of capturing privacy preferences in a form amenable to machine processing. Our work differs from P3P, APPEL, PSP, and EPAL in that we look at privacy legislation and other regulations in order to derive a core set of privacy attributes that are required by law in the content of a consumer personal privacy policy, rather than be concerned with expressing preferences in machine processable form. In fact, the example personal privacy policies we give below are expressed in English. Therefore, we are not proposing another policy language but rather looking at what content must be in personal privacy

policies to satisfy privacy legislation. Our example privacy policies may well be expressed in P3P, APPEL, PSP, or EPAL. We are not aware of any other work that derives personal privacy policy content requirements from privacy legislation.

The rest of this chapter is organized as follows. Section "E-Service Privacy Policy Model" describes our model of using personal privacy policies to protect consumer privacy. This is followed by Section "Privacy Legislation" which examines privacy legislation from Canada, the European Union, and the United States and derives privacy attributes for inclusion in personal privacy policies. Section "Personal Privacy Policy Specification" integrates the privacy attribute findings from Section "Privacy Legislation" into the minimum personal privacy policy that satisfies privacy legislation. Finally, Section "Conclusions and Future Work" give our conclusions and ideas for future work.

E-SERVICE PRIVACY POLICY MODEL (EPPM)

Before explaining our E-Service Privacy Policy Model, it is useful to describe what we mean by an e-service. An e-service is a service that is offered by a provider to a consumer across a computer network. A stock quotation service is often used as an example of an e-service. Here a consumer would logon to the service from a computer, and after appropriate user authentication, would make use of the service to obtain stock quotes. Accessing one's bank account through online banking is another example of an e-service. Here the provider is the bank and the service consists of allowing the consumer to check the balance, transfer funds, or make bill payments. The network is usually the

Internet, but could also in principle be a private enterprise network. At any time, one provider may be serving many consumers and many providers may be serving one consumer. For the purposes of this chapter, the business relationship between provider and consumer is always one-to-one, i.e. the service is designed for one consumer and is provided by one provider (although this provider may make use of other providers to compose its e-service) and payment for the service is expected from one consumer. In addition, service providers may also be service consumers, and service consumers may also be service providers.

The E-Service Privacy Policy Model describes the origin and use of personal privacy policies to protect consumer privacy for e-services. This model consists of six phases as given in Table 1. These phases would occur in ascending numerical order. In this model, a provider of a particular e-service has a privacy policy for that e-service, stating what private information it requires from the consumer and how the information will be used. The consumer has a privacy policy stating his/her privacy preferences for using a particular e-service, e.g. what private information the consumer is willing to give to the provider and with whom the information may be shared. An entity that is both a provider and a consumer has separate privacy policies for these two roles.

Table 1. E-Service Privacy Policy Model Phases

Phase	Description	Reference
1. Formulate	Privacy policy creation; every e-service consumer needs to have his/her own personal privacy policy that expresses his/her privacy preferences for using a particular e-service; every provider also needs one or more privacy policies expressing what private information it needs for it's e-services	Yee and Korba (Jan. 2005) describes methods for creating personal privacy policies
2. Search	E-service consumer knows the type of e-service he/she needs (e.g. book seller) and searches the Internet (e.g. using Google) for such an e-service.	-
3. Match	Before an e-service is engaged, the service consumer and service provider exchange and compare their individual privacy policies for the e-service to see if there is a match. If there is a match, Phase 5 is entered next. Otherwise, Phase 4 is entered next.	Yee and Korba (May 2005)
4. Negotiate	Consumer and provider negotiate with each other to try to arrive at a mutually agreed privacy policy. If this negotiation is successful, Phase 5 is entered next. Otherwise, Phase 2 is entered next (consumer searches for another provider).	Yee and Korba (Jan. 2003, May 2003)
5. Engage	The consumer engages the e-service.	-
6. Comply	The provider must comply with the personal privacy policy of the consumer or comply with their mutually negotiated privacy policy.	Yee and Korba (July 2004, Mar. 2005)

For Phases 3 and 4, a privacy policy is attached to a software agent that acts on behalf of a consumer or a provider as the case may be. Prior to the activation of a particular service, the agent for the consumer and the agent for the provider undergo a privacy policy exchange, in which the policies are examined for compatibility. The service is only activated if the policies are compatible (see Yee and Korba, May 2005), in which case we say that there is a "match" between the two policies. In addition, *we assume that in general, the provider always asks for more private information from the*

consumer than the consumer is willing to give up. Figure 1 illustrates Phases 3 and 4. For the purposes of this work, it is not necessary to consider the details of service operation.

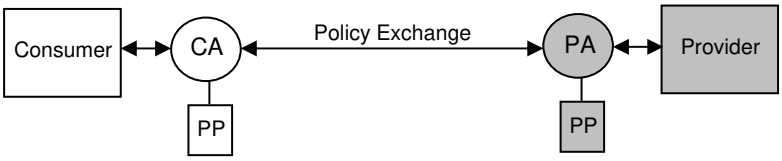

Figure 1. Exchange of Privacy Policies (PP) Between Consumer Agent (CA) and Provider Agent (PA)

Further detailed descriptions of how to carry out individual phases of this model is beyond the scope of this work; however, we include in Table 1 some references to Yee and Korba who have works describing how some of the phases may be carried out.

PRIVACY LEGISLATION

Canada

In Canada, federal privacy legislation is enacted in the *Personal Information Protection and Electronic Documents Act (PIPEDA)* (Government of Canada) and is based on the Canadian Standards Association's *Model Code for the Protection of Personal Information* (Department of Justice), recognized as a national standard in 1996. This Code consists of ten Privacy Principles that for convenience, we label as CSAPP (Table 2). Since the privacy provisions of PIPEDA are represented by CSAPP, we examine CSAPP rather than the more complicated text of PIPEDA itself.

To identify some attributes of private information collection using the CSAPP, we interpret "organization" as "provider" and "individual" as "consumer". In the following,

we use CSAPP.n to denote Principle n of CSAPP. Principle CSAPP.2 implies that there could be different providers requesting the information, thus implying a *collector* attribute. Principle CSAPP.4 implies that there is a *what* attribute, i.e. what private information is being collected. Principles CSAPP.2, CSAPP.4, and CSAPP.5 state that there are *purposes* for which the private information is being collected. Principle CSAPP.5 implies a *retention time* attribute for the retention of private information. Principles CSAPP.3, CSAPP.5 and CSAPP.9 imply that the private information can be disclosed to other parties, giving a *disclose-to* attribute. Thus, from the CSAPP we derive 5 attributes of private information collection, namely *collector*, *what*, *purposes*, *retention time, and disclose-to*.

The Privacy Principles also prescribe certain operational requirements that must be satisfied between provider and consumer, such as identifying purpose and acquiring consent. Our EPPM and the exchange of privacy policies automatically satisfy some of these requirements, namely Principles CSAPP.2, CSAPP.3, and CSAPP.8. The satisfaction of the remaining operational requirements depends on compliance mechanisms (Principles CSAPP.1, CSAPP.4, CSAPP.5, CSAPP.6, CSAPP.9, and CSAPP.10) and security mechanisms (Principle CSAPP.7).

Table 2 - CSAPP - The Ten Privacy Principles from (Canadian Standards Association)

Principle	Description
1. Accountability	An organization is responsible for personal information under its control and shall designate an individual or individuals accountable for the organization's compliance with the privacy principles.
2. Identifying Purposes	The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
3. Consent	The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except when inappropriate.

4. Limiting Collection	The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. Limiting Use, Disclosure, and Retention	Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for fulfillment of those purposes.
6. Accuracy	Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
7. Safeguards	Security safeguards appropriate to the sensitivity of the information shall be used to protect personal information.
8. Openness	An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.
9. Individual Access	Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. Challenging Compliance	An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

European Union (EU)

Privacy in the EU is defined as a human right under Article 8 of the 1950 European Convention of Human Rights and Fundamental Freedoms (ECHR). The implementation of this Article can be traced to The Directive (European Union Directive). Similar legislation and enforcement structures as the European model exist in Canada, Australia, Norway, Switzerland and Hong Kong.

The Directive applies to all sectors of EU public life, with some exceptions. It specifies the data protection rights afforded to “data subjects”, plus the requirements and responsibilities obligated for “data controllers” and by association “data processors” (Deitz, 1998). This triad structure of entities balances data subject fundamental rights against the legitimate interests of data controllers (see Figure 2). The Directive places an obligation on member states to ratify national laws implementing its requirements.

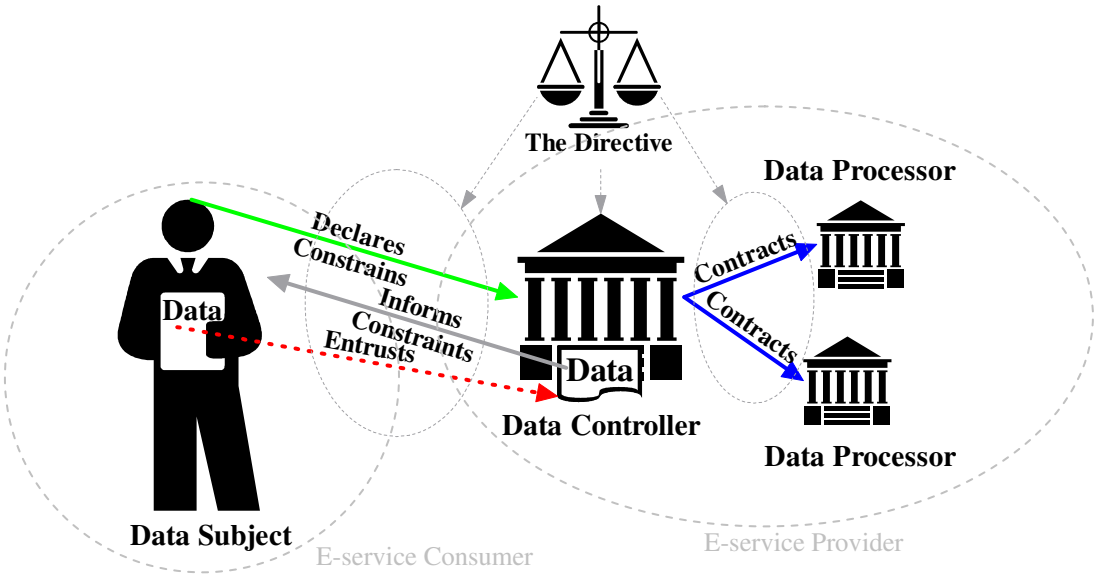

Figure 2. A schematic representation of the roles of the three entities defined in the Directive.

The data subject is a person who can be identified by one or more pieces of data related to his physical, physiological, mental, economic, cultural or social identities. Even data associated with an individual in ambiguous ways may be deemed reasonable personally identifiable information. Following Article 1 of the ECHR, the fundamental right to data protection falls not to the nationality of the data subject, but as an obligation to a party that relies on the data subject (Council of Europe Convention 108). The parties that rely on the data subject are the data controller and, by association, the data processor.

The data controller is an entity that determines the purpose and means of processing personal data, and is defined as the holder of ultimate accountability as it relates to the correct processing and handling of the information from the data subject. The data processor is an entity that processes personal data on behalf of the data controller.

For e-services in this work, the data subject maps to the e-service consumer and the data controller and data processors together map to the e-service provider, as depicted using gray in Figure 2.

EU privacy principles (Table 3) abstracted from the complexities of legislation have been developed to simplify compliance with privacy regulations. Analyzing an approach using the principles as a guide, offers a fruitful means for determining the effectiveness and pitfalls of the approach. We thus use these principles to derive privacy attributes based on EU privacy legislation. For convenience, we label these Principles as EUPP, with EUPP.n meaning Principle n of EUPP.

Table 3. European Union Privacy Principles

Principle	Description
1. Reporting the processing	All non-exempt processing must be reported in advance to the National Data Protection Authority.
2. Transparent processing	The data subject must be able to see who is processing his personal data and for what purpose. The data controller must keep track of all processing it performs and the data processors and must make it available to the user.
3. Finality & Purpose Limitation	Personal data may only be collected for specific, explicit, legitimate purposes and not further processed in a way that is incompatible with those purposes.
4. Lawful basis for data processing	Personal data processing must be based on what is legally specified for the type of data involved, which varies depending on the type of personal data.
5. Data quality	Personal data must be as correct and as accurate as possible. The data controller must allow the citizen to examine and modify all data attributable to that person.
6. Rights	The data subject has the right to improve his or her data as well as the right to raise certain objections regarding the execution of these principles by the data controller.
7. Data traffic outside EU	Exchange of personal data to a country outside the EU is permitted only if that country offers adequate protection. The data controller assures appropriate measures are taken in that locality if possible.
8. Data processor processing	If data processing is outsourced from data controller to processor, controllability must be arranged.
9. Security	Measures are taken to assure secure processing of personal data.

Looking at Table 3, we note that the EUPP has much in common with the CSAPP. We see that EUPP.2 has "who is processing his personal data and for what purpose" implying the privacy attributes *collector* (for "who"), *what* (for "personal data"), and *purpose*. Purpose is also confirmed by EUPP.3. EUPP.7 talks about exchanging personal data implying the *disclosed-to* attribute. While retention time is not mentioned explicitly, EUPP.3 mentions "not further processed in a way that is incompatible with those purposes" which can be partly enforced using retention time. In addition, EUPP.8 talks about arranging for controllability which is supported by retention time. In any case, retention time as a privacy attribute can only help the cause of privacy protection. The remaining aspects of the EUPP refer to operational requirements (e.g. EUPP.1, EUPP.9). We thus conclude that the privacy attributes *collector*, *what*, *purposes*, *retention time,* and *disclose-to* are also supported by the EUPP, and moreover, that the EUPP does not introduce any additional attributes.

United States

In the United States, privacy protection is achieved through a patchwork of legislation at the federal and state levels. Privacy legislation is largely sector-based (Banisar, 1999). At the Federal level there are presently more than a dozen privacy laws. Some of these laws are: Privacy Act of 1974 as amended (5 USC 552a), Electronic Communications Privacy Act of 1986, and Right to Financial Privacy Act of 1986. Laws applicable to the private sector include: Family Educational Rights and Privacy Act of 1978, Privacy Protection Act of 1980, and Video Privacy Protection Act of 1988. As can be seen, the laws typically apply to specific technologies or privacy threats to, for

example, bank records, government databases, or video rental history. The laws serve as operational boundaries rather than requirements and there is no national all encompassing code for privacy protection. As such, the US laws are less effective at protecting personal privacy than either the legislations of the European Union or Canada. The United States is not the leader in privacy protection (Hurley, 1999; Milberg et al, 1995; Banisar, 1999). However, there is one very hot area where privacy is treated very seriously and that is the area of personal health information privacy, as exemplified by the Health Insurance Portability and Accountability Act (HIPAA) (U.S. Government). We therefore examine the privacy provisions of HIPAA for privacy attributes.

The following three paragraphs are quoted from U.S. Government-1 give a good background on HIPAA privacy provisions:

> "The following overview provides answers to general questions regarding the *Standards for Privacy of Individually Identifiable Health Information* (the Privacy Rule), promulgated by the Department of Health and Human Services (HHS).
>
> To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act (HIPAA) of 1996, Public Law 104-191, included "Administrative Simplification" provisions that required HHS to adopt national standards for electronic health care transactions. At the same time, Congress recognized that advances in electronic technology could erode the privacy of health information. Consequently, Congress incorporated into HIPAA provisions that mandated the adoption of Federal privacy protections for individually identifiable health information.

> In response to the HIPAA mandate, HHS published a final regulation in the form of the Privacy Rule in December 2000, which became effective on April 14, 2001. This Rule set national standards for the protection of health information, as applied to the three types of covered entities: health plans, health care clearinghouses, and health care providers who conduct certain health care transactions electronically. By the compliance date of April 14, 2003 (April 14, 2004, for small health plans), covered entities must implement standards to protect and guard against the misuse of individually identifiable health information. Failure to timely implement these standards may, under certain circumstances, trigger the imposition of civil or criminal penalties."

The Privacy Rule is too long to use here (even the summary of the Privacy Rule takes 25 pages). We instead present a summary of HIPAA health information privacy rights from U.S. Government-2 (Table 4). For convenience, we label Table 3 as HIPR and use HIPR.n to mean the n^{th} right of the HIPR, which has 8 rights.

Looking at the HIPR, we note that the HIPR has much in common with the CSAPP and the EUPP. We see that HIPR.3 states "you can learn how your health information is used and shared by your provider or health insurer". This implies a *collector* ("by your provider") and a *what* ("your health information"). HIPR.4 contains

Table 4. HIPAA consumer privacy rights

	Your Health Information Privacy Rights: Providers and health insurers who are required to follow this law must comply with your rights to…
1	**Ask to see and get a copy of your health records** You can ask to see and get a copy of your medical record and other health information. You may not be able to get all of your information in a few special cases. For example, if your doctor decides something in your file might endanger you or someone else, the doctor may not have to give this information to you. • In most cases, your copies must be given to you within 30 days, but this can be extended for another 30 days if you are given a reason. • You may have to pay for the cost of copying and mailing if you request copies and mailing.
2	**Have corrections added to your health information** You can ask to change any wrong information in your file or add information to your file if it is incomplete. For example, if you and your hospital agree that your file has the wrong result for a test, the hospital must change it. Even if the hospital believes the test result is correct, you still have the right to have your disagreement noted in your file. • In most cases the file should be changed within 60 days, but the hospital can take an extra 30 days if you are given a reason.
3	**Receive a notice that tells you how your health information is used and shared** You can learn how your health information is used and shared by your provider or health insurer. They must give you a notice that tells you how they may use and share your health information and how you can exercise your rights. In most cases, you should get this notice on your first visit to a provider or in the mail from your health insurer, and you can ask for a copy at any time.
4	**Decide whether to give your permission before your information can be used or shared for certain purposes** In general, your health information cannot be given to your employer, used or shared for things like sales calls or advertising, or used or shared for many other purposes unless you give your permission by signing an authorization form. This authorization form must tell you who will get your information and what your information will be used for.
5	**Get a report on when and why your health information was shared** Under the law, your health information may be used and shared for particular reasons, like making sure doctors give good care, making sure nursing homes are clean and safe, reporting when the flu is in your area, or making required reports to the police, such as reporting gunshot wounds. In many cases, you can ask for and get a list of who your health information has been shared with for these reasons. • You can get this report for free once a year. • In most cases you should get the report within 60 days, but it can take an extra 30 days if you are given a reason.
6	**Ask to be reached somewhere other than home** You can make reasonable requests to be contacted at different places or in a different way. For example, you can have the nurse call you at your office instead of your home, or send mail to you in an envelope instead of on a postcard. If sending information to you at home might put you in danger, your health insurer must talk, call, or write to you where you ask and in the way you ask, if the request is reasonable.
7	**Ask that your information not be shared** You can ask your provider or health insurer not to share your health information with certain people, groups, or companies. For example, if you go to a clinic, you could ask the doctor not to share your medical record with other doctors or nurses in the clinic. However, they do not have to agree to do what you ask.
8	**File complaints** If you believe your information was used or shared in a way that is not allowed under the privacy law, or if you were not able to exercise your rights, you can file a complaint with your provider or health insurer. The privacy notice you receive from them will tell you who to talk to and how to file a complaint. You can also file a complaint with the U.S. Government.

"used or shared for many other purposes" implying a *purpose* attribute. HIPR.7 talks about sharing your health information with other entities, implying a *disclose-to*. The HIPR does not mention *retention time* but the much more detailed Privacy Rule of the HIPAA (see above) mentions "retention of records". The remaining aspects of the HIPR refer to operational requirements (e.g. HIPR.1, HIPR.2) some of which are similar to the CSAPP and EUPP (e.g. HIPR.1 and HIPR.2 relate well with EUPP.6, CSAPP.6, and CSAPP.9). We thus conclude that the privacy attributes *collector*, *what*, *purposes*, *retention time,* and *disclose-to* are also supported by the HIPR and HIPAA. Moreover, the HIPR does not introduce any additional private information attributes.

PERSONAL PRIVACY POLICY SPECIFICATION

Based on the above exploration, the contents of a personal privacy policy should, for each item of private information, identify a) *collector* - who wishes to collect the information, b) *what* - the nature of the information, c) *purposes* - the purposes for which the information is being collected, d) *retention time* – the amount of time for the provider to keep the information, and e) *disclose-to* – the parties to whom the information will be disclosed. Privacy policies across different types of e-services (e.g. e-business, e-learning, e-health) are specified using these attributes (see examples below) and principally differ from one another according to the values of the attributes *what* and *purposes*. For example, an e-commerce privacy policy might specify credit card number as *what* and payment as *purposes* whereas an e-learning privacy policy might specify marks as *what* and student assessment as *purposes*.

Figure 3 gives 3 examples of consumer personal privacy policies for use with an e-learning provider, an online bookseller, and an online medical help clinic. The first item in a policy indicates the type of online service for which the policy will be used. Since a privacy policy may change over time, we have a *valid* field to hold the time period during which the policy is valid. The proxy field holds the name of the proxy if a proxy is employed to provide the information. Otherwise, this field has the default value of "no". The address and telephone contact of the proxy may be specified as an informational item in the privacy policy itself. These policies need to be expressed in a machine-readable policy language such as APPEL (W3C, 2002) (XML implementation).

A personal privacy policy thus consists of "header" information (policy use, owner, proxy, valid) together with 5-tuples or privacy rules

<collector, what, purposes, retention time, disclose-to>

where each 5-tuple or rule represents an item of private information and the conditions under which the information may be shared. A personal privacy policy therefore consists of a header plus one or more privacy rules.

As we mentioned in the Introduction, this is a minimum personal privacy policy that satisfies the privacy legislation of Canada, the European Union, and the United States (for personal health information), since it can contain additional privacy provisions. Additional provisions could include, for example, a) elaborated retention time using conditions such as "6 months unless I call to have it deleted right away", b) negative purposes such as "not for purposes A or B", c) negative disclose-to such as "not

to be disclosed to persons C or D", and d) operational items such as requesting a report as in HIPR.5 or requesting different means of contact as in HIPR.6.

Policy Use: E-learning *Owner*: Alice Consumer *Proxy*: No *Valid*: unlimited	*Policy Use*: Bookseller *Owner:* Alice Consumer *Proxy*: No *Valid:* June 2005	*Policy Use*: Medical Help *Owner:* Alice Consumer *Proxy*: No *Valid*: July 2005
Collector: Any *What:* name, address, tel *Purposes:* identification *Retention Time:* unlimited *Disclose-To*: none *Collector:* Any *What:* Course Marks *Purposes:* Records *Retention Time:* 2 years *Disclose-To*: none	*Collector:* Any *What:* name, address, tel *Purposes:* identification *Retention Time:* unlimited *Disclose-To*: none	*Collector:* Any *What:* name, address, tel *Purposes:* contact *Retention Time:* unlimited *Disclose-To*: pharmacy *Collector:* Dr. A. Smith *What:* medical condition *Purposes:* treatment *Retention Time:* unlimited *Disclose-To*: pharmacy

Figure 3. Example Consumer Personal Privacy Policies

CONCLUSIONS AND FUTURE RESEARCH

We began by introducing our E-Services Privacy Policy Model that describes how personal privacy policies can be used to protect personal privacy in an e-services environment. We then examined privacy principles and rights representative of privacy legislation from Canada, the European Union, and the United States and derived 5 attributes of private information collection for use in specifying personal privacy policies, namely *collector, what*, *purposes*, *retention time*, and *disclose-to*. We showed that these attributes are supported by the privacy legislation of all 3 geographic regions. Moreover, these attributes are complete in the sense that no other privacy attributes are required by the legislation, although one could add additional modifiers to the attributes and include operational items in the policy. In addition, we believe that the 5 attributes lead to a

policy that is very understandable and manageable by the average e-service consumer which is important if the EPPM is to succeed. In this sense, the possible additional privacy provisions mentioned above would only complicate matters and may not be used by most consumers.

Ideas for future research include: a) expressing our personal privacy policy using a policy language such as APPEL (W3C, 2002) to investigate ease and practicality of use, b) have consumer volunteers express their privacy preferences using our privacy policy to gauge how well consumers adapt to it and whether or not it meets the requirements for a variety of e-services in different domains. The latter work would explore how personal privacy policies may be used with Web Services via their implementation protocols (e.g. UDDI, WSDL, and SOAP).

REFERENCES

Banisar, D. (1999). Privacy and Data Protection Around the World. *21st International Conference on Privacy and Personal Data Protection*, September 13.

Carnegie Mellon University. *Privacy Server Protocol Project*. Internet Systems Laboratory, Robotics Institute and eCommerce Institute, School of Computer Science. Retrieved August 13, 2002 from: http://yuan.ecom.cmu.edu/psp/

Council of Europe Convention 108. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Available at: http://conventions.coe.int/treaty/EN/Treaties/Html/108.htm

Deitz, L. (1998). Privacy and Security – EC's privacy directive: protecting personal data and ensuring its free movement. *Computers and Security Journal*, V. 17, N. 4, pp. 25-46.

Department of Justice. *Privacy Provisions Highlights*. Retrieved July 3, 2002 from: http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

European Union Directive (1995). *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*. Unofficial text retrieved Sept. 5, 2003 from: http://aspe.hhs.gov/datacncl/eudirect.htm

Government of Canada. *Personal Information Protection and Electronic Documents Act*. Available as of February 28, 2005 at: http://www.privcom.gc.ca/legislation/index_e.asp

IBM. Enterprise Privacy Architecture Language (EPAL). Accessed March 9, 2005 at:

Milberg, S.J., Burke, S.J., Smith, H.J., Kallman, E.A. (1995). Values, Personal Information, Privacy, and Regulatory Approaches. *Communications of the ACM*, December, Vol. 38, No. 12.

U.S. Government. Office for Civil Rights – HIPAA: Medical Privacy - National Standards to Protect the Privacy of Personal Health Information. Available as of Feb. 28, 2005 at: http://www.hhs.gov/ocr/hipaa/

U.S. Government-1. General Overview of Standards for Privacy of Individually Identifiable Health Information. Available as of Feb. 28, 2005 at: http://www.hhs.gov/ocr/hipaa/guidelines/overview.pdf

U.S. Government-2. Your Health Information Privacy Rights. Available as of Feb. 28, 2005 at: http://www.hhs.gov/ocr/hipaa/consumer_rights.pdf

W3C. *The Platform for Privacy Preferences*. Retrieved August 12, 2002 from: http://www.w3.org/P3P/

W3C (2002). A P3P Preference Exchange Language 1.0 (APPEL1.0). *W3C Working Draft 15 April 2002*. Retrieved August 12, 2002 from: http://www.w3.org/TR/P3P-preferences/

Yee, G. & Korba, L. (Jan. 2003). Bilateral E-services Negotiation Under Uncertainty. Proceedings, *The 2003 International Symposium on Applications and the Internet (SAINT2003)*, Orlando, Florida, USA.

Yee, G. & Korba, L. (May 2003). The Negotiation of Privacy Policies in Distance Education. In *Proceedings of the Information Resources Management Association International Conference 2003 (IRMA 2003)*, Philadelphia, Pennsylvania, USA.

Yee, G. & Korba, L. (July 2004). Privacy Policy Compliance for Web Services. In *Proceedings, IEEE International Conference on Web Services (ICWS 2004)*, San Diego, California, USA.

Yee, G. & Korba, L. (Jan. 2005). Semi-Automatic Derivation and Use of Personal Privacy Policies in E-Business. *International Journal of E-Business Research*, *Vol. 1, No. 1*, Idea Group Publishing.

Yee, G. & Korba, L. (Mar. 2005). An Agent Architecture for E-Services Privacy Policy Compliance. Proceedings, *The IEEE 19th International Conference on Advanced*

Information Networking and Applications (AINA 2005), Tamkang University, Taiwan.

Yee, G. & Korba, L. (May 2005). Comparing and Matching Privacy Policies Using Community Consensus. In *Proceedings of the Information Resources Management Association International Conference 2005 (IRMA 2005)*, San Diego, California, USA.

[1] NRC Paper Number: NRC 48270