NRC Publications Archive
Archives des publications du CNRC

Feature Interactions in Policy-Driven Privacy Management

Yee, George; Korba, Larry

This publication could be one of several versions: author’s original, accepted manuscript or the publisher’s version. / La version de cette publication peut être l’une des suivantes : la version prépublication de l’auteur, la version acceptée du manuscrit ou la version de l’éditeur.

Publisher’s version / Version de l'éditeur:

Proceedings from the Seventh International Workshop on Feature Interactions in Telecommunications and Software Systems (FIW'03), 2003

NRC Publications Archive Record / Notice des Archives des publications du CNRC :
https://nrc-publications.canada.ca/eng/view/object/?id=023467f1-ff1a-4383-86e8-afd3dda9e29e
https://publications-cnrc.canada.ca/fra/voir/objet/?id=023467f1-ff1a-4383-86e8-afd3dda9e29e

Access and use of this website and the material on it are subject to the Terms and Conditions set forth at
https://nrc-publications.canada.ca/eng/copyright
READ THESE TERMS AND CONDITIONS CAREFULLY BEFORE USING THIS WEBSITE.

L’accès à ce site Web et l’utilisation de son contenu sont assujettis aux conditions présentées dans le site
https://publications-cnrc.canada.ca/fra/droits
LISEZ CES CONDITIONS ATTENTIVEMENT AVANT D’UTILISER CE SITE WEB.

Questions? Contact the NRC Publications Archive team at PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca. If you wish to email the authors directly, please see the first page of the publication for their contact information.

Vous avez des questions? Nous pouvons vous aider. Pour communiquer directement avec un auteur, consultez la première page de la revue dans laquelle son article a été publié afin de trouver ses coordonnées. Si vous n’arrivez pas à les repérer, communiquez avec nous à PublicationsArchive-ArchivesPublications@nrc-cnrc.gc.ca.

National Research Council Canada
Conseil national de recherches Canada

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC-CNRC

*Feature Interactions in Policy-Driven Privacy Management**

Yee, G., and Korba, L.
June 2003

* published in Proceedings from the Seventh International Workshop on Feature Interactions in Telecommunications and Software Systems (FIW'03), June 11-13, 2003. Ottawa, Canada.

Copyright 2003 by
National Research Council of Canada

Permission is granted to quote short excerpts and to reproduce figures and tables from this report, provided that the source of such material is fully acknowledged.

Canada

Feature Interactions in Policy-Driven Privacy Management[1]

George YEE and Larry KORBA
Institute for Information Technology
National Research Council Canada
Montreal Road, Building M-50
Ottawa, Ontario, Canada K1A 0R6
Email: {George.Yee, Larry.Korba}@nrc-cnrc.gc.ca

Abstract. The growth of the Internet is increasing the deployment of e-services in such areas as e-business, e-learning, and e-health. In parallel, the providers and consumers of such services are realizing the need for privacy. The widespread use of P3P privacy policies for web sites is an example of this growing concern for privacy. However, while the privacy policy approach may seem to be a reasonable solution to privacy management, we show in this paper that it can lead to unexpected feature interaction outcomes such as unexpected costs, the lost of privacy, and even cause serious injury. We propose a negotiations approach for eliminating or mitigating the unexpected bad outcomes.

1 Introduction

The growth of the Internet has been accompanied by a growth in the number of e-services available to consumers. E-services for banking, shopping, learning, and even Government Online abound. Each of these services requires a consumer's personal information in one form or another. This leads to concerns over privacy. Indeed, the public's awareness of potential violations of privacy by online service providers has been growing. Evidence affirming this situation include a) the use of P3P privacy policies [1] by web server sites to disclose their treatment of users' private information, and b) the enactment of privacy legislation in the form of the Privacy Principles [2] as a sort of owners' "bill of rights" concerning their private information. We take a policy-based approach in privacy management. We believe this offers both effectiveness and flexibility. Both providers and consumers have privacy policies stating what private information they are willing to share, with whom it may be shared, and under what circumstances it may be shared. Privacy policies are attached to software agents that act as proxies for service consumers or providers. Prior to the activation of a particular service, the agents for the consumer and provider undergo a privacy policy exchange, in which the policies are examined for compatibility. The service is only activated if the policies are compatible (i.e. there are no conflicts). Figure 1 illustrates our policy exchange model. For the purposes of this paper, it is not necessary to consider the details of service operation.

Given the above scenarios, we show how the privacy policies of consumers and providers can interact with unexpected negative consequences. We then propose an approach

[1] NRC Paper Number: NRC 45785

to prevent or mitigate the occurrences of such consequences. Traditionally, feature interactions have been considered mainly in the telephony or communication services domains [3]. More recent papers, however, have focused on other domains such as the Internet, multimedia systems, mobile systems [4], and Internet personal appliances [5].

Section 2 looks at the content of privacy policies by identifying some attributes of private information collection, using the Privacy Principles as a guide. Section 3 presents a categorization of privacy policy interactions with their outcomes. Section 4 proposes an approach to prevent or mitigate the occurrence of negative consequences from privacy policy interactions. Section 5 gives conclusions.

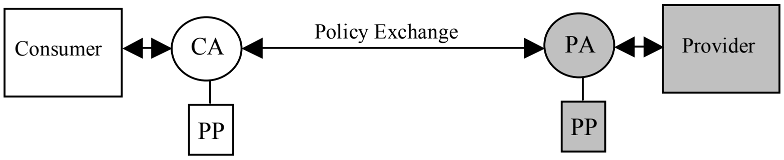

Figure 1. Exchange of Privacy Policies (PP) Between Consumer Agent (CA) and Provider Agent (PA)

2 Privacy Policies

We identify some attributes of private information collection using the Privacy Principles [2] as a guide. We will apply these attributes to the specification of privacy policy contents.

Table 1. The Ten Privacy Principles Used in Canada

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.

We interpret “organization” as “provider” and “individual” as “consumer”. Principle 2 implies that there could be different providers requesting the information, thus implying a *who*. Principle 4 implies that there is a *what*, i.e. what personal information is being collected. Principles 2, 4, and 5 state that there is a *purpose* for which the private information is being collected. Finally, Principle 5 implies a *time* element to the collection of personal information, i.e. the provider’s retention time of the private information. We thus arrive at 4 attributes of private information collection, namely *who*, *what*, *purpose*, and *time*.

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

Based on the above exploration, the contents of a privacy policy should, for each item of private information, identify a) who wishes to collect the information, b) the nature of the information, c) the purpose for which the information is being collected, and d) the retention time for the provider to keep the information. Figure 2 (top) gives examples of provider privacy policies from 3 types of providers: an e-learning provider, an e-commerce provider, and a nursing practitioner who uses the Internet to obtain referrals. Figure 2 (bottom) gives corresponding example consumer privacy policies. These policies need to be expressed in a

Privacy Policy: E-learning *Owner: E-learning Unlimited*	*Privacy Policy: Book Seller* *Owner: All Books Online*	*Privacy Policy: Medical Help* *Owner: Nursing Online*
Who: Any *What:* name, address, tel *Purpose:* identification *Time:* As long as needed	*Who:* Any *What:* name, address, tel *Purpose:* identification *Time:* As long as needed	*Who:* Any *What:* name, address, tel *Purpose:* contact *Time:* As long as needed
Who: Any *What:* Course Marks *Purpose:* Records *Time:* 1 year	*Who:* Any *What:* credit card *Purpose:* payment *Time:* until payment complete	*Who:* Any *What:* medical condition *Purpose:* treatment *Time:* 1 year

Privacy Policy: E-learning *Owner: Alice Consumer*	*Privacy Policy: Book Seller* *Owner: Alice Consumer*	*Privacy Policy: Medical Help* *Owner: Alice Consumer*
Who: Any *What:* name, address, tel *Purpose:* identification *Time:* As long as needed	*Who:* Any *What:* name, address, tel *Purpose:* identification *Time:* As long as needed	*Who:* Any *What:* name, address, tel *Purpose:* contact *Time:* As long as needed
Who: Any *What:* Course Marks *Purpose:* Records *Time:* 2 years		*Who:* Dr. Alexander Smith *What:* medical condition *Purpose:* treatment *Time:* As long as needed

Figure 2. Example Provider Privacy Policies (top) and Corresponding Consumer Privacy Policies (bottom)

machine-readable policy language such as APPEL [6] (XML implementation). The authors are presently experimenting with a prototype privacy policy creation system, which will be reported in a future paper.

3 Privacy Policy Interactions

Once consumer and provider agents exchange privacy policies, each agent examines the other's policy to determine if there is a match between the two policies. If each agent finds a match, the agents signal each other that a match has been found, and service is initiated. If either agent fails to find a match, that agent would signal a mismatch to the other agent and service would then not be initiated. In this case, the consumer (provider) is free to exchange policies with another provider (consumer). In our model, the provider always tries to obtain more private information from the consumer; the consumer, on the other hand, always tries to give up less private information. We say that there is a *match* between a consumer's privacy policy and the corresponding provider's policy where the consumer's policy is giving up less than or equal to the amount of private information required by the provider's policy. Otherwise, we say that there is a *mismatch*. Where time is involved, a private item held for less time is considered less private information. Thus in the policies above, there is a match for e-learning, since the time required by the provider (1 year) is less than the time the consumer is willing to give up (2 years), i.e. the provider requires less private information than the consumer is willing to give up. There is a mismatch for book seller (consumer not willing to provide credit card data) and a mismatch for medical help (consumer only willing to tell medical condition to Dr. Smith). A privacy policy is considered *upgraded* if the new version represents more privacy than the prior version. Similarly, a privacy policy is considered *downgraded* if the new version represents less privacy than the prior version.

In telecom, the individual features work as designed, but the combination of features working together interact and produce unexpected outcomes. In the case of consumers and providers, each privacy policy is a statement of how private information is to be handled, much like how a telecom feature is a statement of how telecom traffic is to be handled. A privacy policy is therefore analogous to a telecom feature. Given any consumer-provider pair, the execution of their privacy policies is analogous to the simultaneous execution of two or more telecom features, and can also produce unexpected outcomes. Here, "execution" includes the examination by the respective agents to determine if there is a match. As for telecom, each privacy policy or feature is correct by itself (in the sense that it reflects the wishes of its owner), but can produce unexpected outcomes when executed in combination.

There are also differences with telecom feature interactions. Firstly, telecom feature interactions are regarded as side effects of the features. Policy interactions, on the other hand, are part of the normal workings of privacy management, i.e. consumer and provider privacy policies must interact or work together. There is thus no special mechanism needed to detect policy interactions – they occur normally. Secondly, there is a difference in the degree of certainty of unexpected outcomes. In telecom interactions, the unexpected outcomes are the results of physics, and are certain outcomes. In policy interactions, some unexpected outcomes are less certain to occur because they are based on predictions of social behaviour, which can be far more difficult to predict than the outcome of physical laws.

We categorize privacy policy interactions according to how many providers and consumers are exchanging policies at the same time and give examples of outcomes under each category. These policy interactions represent what we consider would be typical occurrences. Example outcomes for simpler exchange structures may also apply for more complex structures. This is determined by the degree to which the simpler structure is part of the more complex structure. We will indicate when this is the case. Our categorization follows:

A. One Consumer to One Provider Interactions

This is the case depicted in Figure 1, with one consumer exchanging policy with one provider.

Case 1: Policies match. Provider may begin service. Possible outcomes:

a) If this match occurred after a series of mismatches with other providers, then the newly found provider is probably less attractive according to criteria such as reputation and cost (this consumer probably started with more attractive providers).
b) If this match occurred after the provider or the consumer downgraded their privacy policies, the provider or consumer may not realize the extra costs that may result from not having access to the private information item or items that were eliminated through downgrading. For example, leaving out the social insurance number may lead to more costly means of consumer identification for the provider. As another example, suppose All Books Online in section 2 downgraded its privacy policy by eliminating the credit card requirement. This would lead to a match with Alice's privacy policy, but may cost Alice longer waiting time to get her order, as she may be forced into an alternate slower means of making payment (e.g. mail a cheque), if payment is required prior to shipping.
c) The provider now has the responsibility to safeguard the consumer's private data (Privacy Principle 7). The provider may not realize that the cost of the safeguard may be very high.
d) Unexpected outcomes that derive from the specifics of the privacy policies. For example, suppose the Nursing Online provider above modifies its policy to match Alice's policy because Dr. Smith is on staff. Alice is able to subscribe to Nursing Online. Then if Dr. Smith becomes unavailable due to an accident, just at the time Alice needs medical attention, Nursing Online would not be able to help Alice – an unexpected outcome.

Case 2: Policies mismatch. Provider may not begin service. Possible outcomes:

a) Consumer may decide to downgrade his privacy policy to try to get a match.
b) Provider may decide to downgrade its privacy policy to try to get a match.
c) The mismatch may result in a denial of service that has serious consequences, where the service is one that is required for safety reasons. For example, if the sought after provider is a health services provider, the consumer may suffer serious injury. In the example policies for medical help above, there is a mismatch due to Alice's requirement to only reveal her medical condition to Dr. Smith. However, if Dr. Smith is not available, a nursing service might still be better than no service.

B. One Consumer to Many Providers Interactions

This is the case shown in Figure 3, where agents for the same consumer exchange the same policy with many provider agents at the same time, with each provider agent representing a different provider that provides the same service.

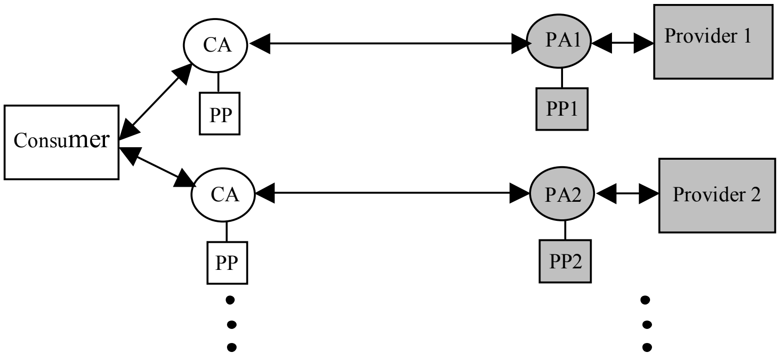

Figure 3. Exchange of Privacy Policies Between One Consumer and Many Providers

Case 1: Policies match for at least one provider. Provider may begin service. Possible outcomes:

a) Same outcomes as in A, Case 1.
b) Where more than one match is found, the consumer has the opportunity to select the best provider based on other criteria such as reputation and cost.

Case 2: Policies mismatch. Provider may not begin service. Possible outcomes:

a) Same outcomes as in A, Case 2.
b) The consumer may be influenced by the many provider policies he has seen to adjust his privacy policy to get a match with the provider that requests the least amount of private information.

C. Many Consumers to One Provider Interactions

This is the case shown in Figure 4, where agents for different consumers exchange different policies at the same time with agents for the same provider.

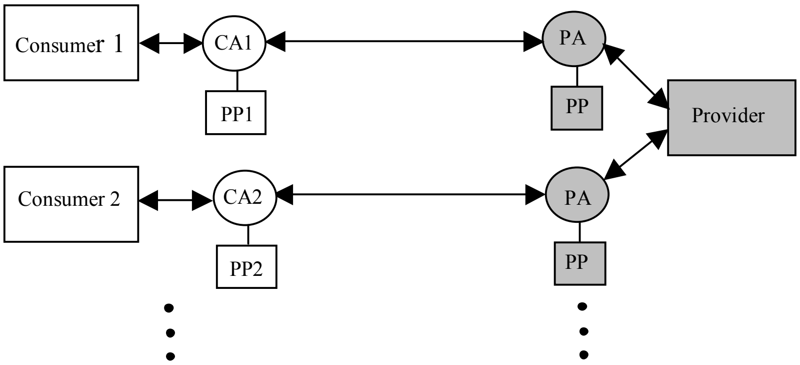

Figure 4. Exchange of Privacy Policies Between Many Consumers and One Provider

Case 1: Policies match for at least one consumer. Provider may begin service to that consumer. Possible outcomes:

a) Same outcomes as in A, Case 1.
b) Where more than one match is found, the provider has the opportunity to select the best consumer based on other criteria such as reputation and credit history.

Case 2: Policies mismatch. Provider may not begin service. Possible outcomes:

a) Same outcomes as in A, Case 2.

b) The provider may be influenced by the many consumer polices it has seen to adjust its privacy policy to get a match with the consumer that offers the most amount of private information.

D. Many Consumers to Many Providers Interactions
This situation is a combination of A, B, and C with the same outcomes.

4 Preventing Unexpected Bad Outcomes

The problem at hand is how to detect and prevent the unexpected outcomes that are bad or dangerous. Not all the possible outcomes in section 3 are unexpected or bad. Solutions to telecom feature interaction problems are varied, ranging from formal analysis [7] to negotiating agents [8] and architectural approaches [9]. In this work, we propose the use of privacy policy negotiation between consumer and provider agents to mitigate or eliminate the unexpected outcomes that are bad. Consider section 3, category A. In case 1, part a) would be less serious since negotiation would reduce the number of mismatches. Case 1, parts b), c), and d) may also be less likely to happen since negotiation may force the provider or consumer to consider all implications. Case 2 c) would likely not occur since negotiations would reveal that Alice's policy is overly restrictive (see example negotiation below). The new outcomes in categories B and C are ones that favour either the consumer or the provider, based on the possibility of several matches, or the examination of many policies. These additional outcomes are neither good nor bad. It suffices to observe that they are still possible with negotiation, i.e. by negotiating several matches or examining many policies concurrently. We have proposed methods for agent-based privacy policy negotiation in [10,11]. In these papers, we provide formal descriptions of the negotiations process and methods for negotiating in cases where there is uncertainty of what offers and counter-offers to make. Table 2 illustrates how negotiation can detect and prevent the unexpected bad outcome of having no access to medical service when it is needed (read from left to right and down):

Table 2. Preventing Unexpected Bad Outcomes

Nursing Online (Provider)	*Alice (Consumer)*
OK if a nurse on our staff sees your medical condition?	*No, only Dr. Alexander Smith can see my medical condition.*
We cannot provide you with any nursing service unless we know your medical condition.	*OK, I'll see Dr. Smith instead.*
You are putting yourself at risk. What if you need emergency medical help for your condition and Dr. Smith is not available?	*You are right. Do you have any doctors on staff?*
Yes, we always have doctors on call. OK to allow them to know your medical condition?	*That is acceptable.*

The result of this negotiation is that Nursing Online will be able to provide Alice with nursing service whenever Alice requires it. If this negotiation had failed (Alice did not agree), Alice will at least be alerted to the possibility of a bad outcome, and may take other measures to avoid it. We have assumed that the provider will want to inform the consumer about bad policy implications that it knows about. We believe this is a reasonable assumption given that it is in their mutual interest to avoid unexpected bad outcomes.

5 Conclusions

The Privacy Principles impose legislative conditions on the rights of individuals (consumers) to privacy. They imply that the collection of private information may be done under the headings of *who*, *what*, *purpose*, and *time*. Privacy policies may be constructed using these headings to specify each private informational item to be shared. In an online community, consumers and providers of electronic services specify their privacy preferences using privacy policies. Agent proxies for consumers and providers exchange and compare these polices in an attempt to match up a consumer of an electronic service with the provider of that service. However, such exchanges can lead to unexpected feature interaction outcomes that have serious negative consequences. Rather than a simple matching process, privacy policies should be negotiated between consumer and provider to develop a mutually agreed upon policy for operation [12]. Such negotiation reduces or eliminates the harmful feature interaction outcomes. It does, however, lead to questions regarding revisiting mutually agreed policies, as consumer or provider policies change over time. As future work, we plan to continue experimenting with a prototype we have built for agent-based privacy negotiation, to identify issues and their resolution. We also plan to investigate ways of avoiding harmful outcomes that may be used in conjunction with negotiation, forming a multi-pronged approach to preventing unexpected bad outcomes.

6 References

[1] W3C, “The Platform for Privacy Preferences”, http://www.w3.org/P3P/

[2] Department of Justice, Privacy Provisions Highlights, http://canada.justice.gc.ca/en/news/nr/1998/attback2.html

[3] D. Keck and P. Kuehn, “The Feature and Service Interaction Problem in Telecommunications Systems: A Survey”, IEEE Transactions on Software Engineering, Vol. 24, No. 10, October 1998.

[4] L. Blair, J. Pang, “Feature Interactions – Life Beyond Traditional Telephony”, Distributed Multimedia Research Group, Computing Dept., Lancaster University, UK.

[5] M. Kolberg et al, “Feature Interactions in Services for Internet Personal Appliances”, University of Stirling, UK, Telcordia Technologies, USA.

[6] W3C, “A P3P Preference Exchange Language 1.0 (APPEL1.0)”, W3C Working Draft 15 April 2002, http://www.w3.org/TR/P3P-preferences/

[7] Amyot, D., Charfi, L., Gorse, N., Gray, T., Logrippo, L., Sincennes, J., Stepien, B. and Ware T, “Feature Description and Feature Interaction Analysis with Use Case Maps and LOTOS”, Sixth International Workshop on Feature Interactions in Telecommunications and Software Systems (FIW'00), Glasgow, Scotland, UK, May 2000.

[8] N. D. Griffeth and H. Velthuijsen, “The Negotiating Agents Approach to Runtime Feature Interaction Resolution”, Proc. of 2nd Int. Workshop on Feature Interactions in Telecommunications Systems, pp. 217-235, IOS Press, 1994.

[9] P. Zave, “Architectural Solutions to Feature-Interaction Problems in Telecommunications”, Proc. 5th. Feature Interactions in Telecommunications and Software Systems, pages 10-22, IOS Press, Amsterdam, Netherlands, Sept. 1998.

[10] G. Yee, L. Korba, “Bilateral E-services Negotiation Under Uncertainty”, accepted for publication, The 2003 International Symposium on Applications and the Internet (SAINT2003), Orlando, Florida, Jan. 27-31, 2003.

[11] G. Yee, L. Korba, “The Negotiation of Privacy Policies in Distance Education”, accepted for publication, 14th IRMA International Conference, Philadelphia, Pennsylvania, May 18-21, 2003.

[12] L. Korba, “Privacy in Distributed Electronic Commerce”, Proc. of the 35th Hawaii International Conference on System Science (HICSS), Hawaii, January 7-11, 2002.