Integration of Situational and Reward Elements for Fair Privacy Principles and Preferences (F3P)

GEOFF SKINNER, SONG HAN & ELIZABETH CHANG
Centre for Extended Enterprises and Business Intelligence
Curtin University of Technology
Perth, WA
AUSTRALIA
Geoff.Skinner@newcastle.edu.au, Song.Han@cbs.curtin.edu.au & Elizabeth.Chang@cbs.curtin.edu.au

***Abstract*-It is widely acknowledged that Information Privacy is subjective in nature and contextually influenced. Individuals value their personal privacy differently with many willing to trade-off of privacy for some form of reward or personal gain. Many of the proposed privacy protection schemes do not give due consideration to the contextual, and more importantly situational influence on privacy. Rather privacy preferences for personal data are configurable for only a limited set of notions that include purpose, recipient, category, and condition. Current solutions offer no, or very limited, support for individual situational privacy preferences. This paper proposes a conceptual framework that allows entities to assign privacy preferences to their personal data items that incorporate situation and reward elements. The solution allows entities to assign trade-off values to their personal data based on the situation and context of the data request. In this manner the data owners set what they perceive as fair privacy practices and preferences for evaluating the worth of their personal data.**

I. INTRODUCTION

The need for better privacy protection is apparent to service providers and consumers alike and viewed as an important issue for the continued success of e-commerce [1]. What has seemed beyond reach is a solution or framework that is able to address all of the privacy concerns of each and every individual, while also incorporating at least a baseline set of privacy principles and regulations. With varying privacy policies, regulations and laws between not only organizations but also countries [2], universal privacy protection schemes are proving elusive. It has been accepted that no number of Privacy Enhancing Technologies are able to solve every privacy issue [3]. Additionally, solutions that incorporate elements from all four models of privacy protection [F4] can not guarantee perfect privacy that seems fair to every individual. The reason being is that the perception of personal privacy is different for every individual [5]. What seems fair to one person is not necessarily fair to another. Privacy is subjective and therefore privacy protection solutions must consider contextual and situational information. This is in addition to allowing individual perceptions on their perceived value of privacy to influence privacy preferences.

Privacy preferences need to cater for situation based privacy decisions. It has been shown that individuals are willing to provide personal information for some type of reward, personalization, or service [6]. For example, if an entity who in most circumstances is not willing to divulge personal data to other entities is placed in a situation where they are offered something they value for revealing their date of birth, sex, religion or other data element that they perceive as private information then the information systems that are managing this exchange should be able to accommodate this type of transaction. This example highlights two key issues that are currently not adequately considered in available solutions. Firstly, the situation influences an individual's decision on privacy. That is, given the right type of incentive in a given situation an entity may be willing to divulge personal data. Secondly, each person has a different perception of what is private information and when it can be revealed based on the situation and context of the data request. For example, if the situation is a medical emergency then they may be willing to provide their blood type or past medical history if it means it may save their life. Alternatively, even without a life or death situation some individuals may be willing to provide their blood type as may not perceive it as private.

This paper therefore proposes a conceptual framework that incorporates what we have termed Fair Privacy Practice's and Preferences. That is, privacy preferences are stored and configurable for each data element that includes situational and reward elements. The situational and reward elements reflect what an entity judges as a fair evaluation of the worth of that particular personal data item in a given situation. The proposal is detailed in Section 3 and explains what types of 'rewards' and situations an entity may reveal their personal data for. It is anticipated that this novel approach will address consumer privacy concerns that can impede e-business. Before this however background and related work is discussed in Section 2. After explaining the framework in Section 3, its practical implementation is covered in Section 4. A brief conclusion is provided in Section 5 that is followed by paper references.

II. BACKGROUND AND RELATED WORK

The idea of extending current privacy preferences was derived from previous work done with P3P [7], EPAL [8]. The 'container' element used in EPAL is similar to the situation

1-4244-0726-5/06/$20.00 '2006 IEEE

and reward elements we are proposing for our extensions. However, the ‘container’ element in EPAL does not cater for the diversity of entity privacy perceptions based on their situations and personal evaluation preferences. The storing of those preferences rather than just the organizational privacy policy in a database follows a similar line of thought proposed by Hippocratic Databases [9]. P3P, EPAL and Hippocratic Database are part of a much larger field of privacy protections, commonly referred to as Privacy Enhancing Technologies (PETs). There are currently numerous PETs being developed and new proposals are constantly being put forward for consideration [10, 11]. As has been stated above PET’s are currently unable to address all privacy protection needs. Rather a combination of solutions from the four models of privacy protection is needed [4]. That is, solutions are needed that encompass comprehensive laws, sectoral laws, self regulation, and technologies of privacy.

Our conceptual framework is best classified as a PET than integrates individual user privacy values based on available ‘rewards’ and influenced by the contextual and situational factors. The idea of individual privacy contracts is discussed in [12], in our framework represents one form of reward an entity may request before revealing personal data. Privacy and the interdependence with context is covered in detail in [13, 14, 15], in particular the work by Nissenbaum in [13] is very useful in the way it is able to clarify many privacy ideas from a legal and contextual integrity standpoint. Privacy as viewed from and economical and financial perspective is the focus of [16]. The evaluation and attempts to place values on information privacy is discussed in [17], while a more focused discussion on user trade-offs of privacy for various benefits is covered in [6].

An important element that must be considered with any work related to P3P is the fact that P3P has had only had limited success to date. P3P has not proven to be very popular as has resulted in few people and organizations making any practical use of it. It is generally perceived that the added over head to a user of managing their privacy preferences is enough to deter them from the using P3P. We hope that our work will provide additional incentives and support for P3P implementation and usage. Users would have the option of increasing their return or ‘reward’ in our framework to offset and compensate the additional work required in setting and maintaining their privacy preferences. Further, some contexts and situations may justify the small cognitive costs associated with handling ones own privacy preferences. The costs associated may be further diminished through selective configuration of only those P3P elements important to each individual user.

An additional factor that must be considered in all systems that would enable automatic disclosure of personal information is its limited use in some countries and regions. For example, member states governed by EU privacy legislation are governed by a directive that does not allow automatic disclosure of special sensitive data, such as in health related contexts. Our framework aims to address these issues by allowing our privacy preference elements of situation and reward to accommodate such restrictions. For example, when dealing with health related data in such regulated environments each setting would be set to the default of restricted. The specifics of each element’s settings are discussed in the following section. However, a setting of restricted basically means that the data is not revealed no matter the situation or reward on offer.

III. Context and Situation Dependant Fair Privacy Practices

Determining if a transaction is fair is subjective to an entity’s perception and values. It involves the consideration of any possible ‘reward’ or benefit resulting from that transaction. An entity’s process of transaction evaluation is influenced by the context and situation of the transactional environment it is taking place in. Therefore, when we discuss the meaning of Fair Privacy Preferences and Principles it should encompass an individual entity’s perception of privacy and their privacy preferences for different situational settings. Additionally the owner of the personal data or privacy that is under evaluation should be able to determine to some extent the type of reward or ‘benefit’ they are trading off for. With these concepts in mind we have formulated a conceptual framework that extends current privacy preference representations to include the key elements of Reward and Situation.

The privacy preferences are configured and stored with each personal data item an entity provides or stores in a database. These preferences can be encoded in either P3P or other XML compatible formats that have been modified to include our additional two elements or notions of reward and situation. This approach allows organizations that need to collect and store all forms of data to also store the data owner’s privacy preferences with the data. This approach is similar to use of privacy meta-data in the Hippocratic Database solution for enforcement and filtering of queries. The main improvement however is the addition of the two elements of reward and situation to better capture an entity’s true valuation of their personal data and privacy.

Definition 1: The Reward element included in Privacy Preferences represents an expandable list of predefined categories that are perceived to be of value and/or benefit to an entity when trading off their privacy in return for one or more of these rewards.

For our framework we have initially defined a straightforward list of rewards that have been refined to cover the most anticipated types of benefits an entity may wish to trade-off personal data for. This list is modifiable in that additional categories may be added, removed or modified upon system configuration. The Reward element provides a number of additional ‘rewards’ besides those of a financial type. One of the main reasons for this is to account for the different cultural perceptions and value of personal privacy. Additionally our proposal caters for the very subjective nature of privacy and individual evaluation. Therefore the categories that will hence forth be termed Reward Categories within the Reward Element of Fair Privacy Policies and Preferences are:

- None: An entity is willing to divulge a personal data item in return for nothing. That is, the data is given freely governed by default privacy rules.
- Monetary: An entity is willing to divulge personal data for an amount of money. The actual amount value is defined as a sub element of the Reward parent element. It is inferred to be in the currency of country of data origin.
- Service: An entity is willing to divulge personal data in exchange for some service or product. For example: a user may provide additional personal details to a web site in exchange for free support or services from the site.
- Identification: An entity is willing to divulge personal data in exchange for a Verifiable or Authenticated Identification of the data requestor. It should be noted that in certain countries, such as those within the EU, such a setting will always be true as it is governed by a legislative directive.
- Information: An entity is willing to divulge personal data in exchange for additional information or sharing of knowledge. For example two entities may simply swap personal details of the same nature and content.
- Contract: An entity is willing to divulge personal data in exchange for a binding contract or agreement between themselves and the data requestor. For example an entity may wish to bind a data requestor to the national privacy laws of the country or organization of the entity providing the personal data.
- Restricted: This is basically the default case and means that the personal data item will not be divulged no matter the reward.

Definition 2: The Situation element included in Privacy Preferences represents an expandable list of predefined categories that represent a number of situations in which a personal data request may be presented to an entity.

For our framework we have initially defined a straightforward list of situations that have been refined to cover the most anticipated types of settings an entity may receive a request for access to and use of their personal data. This list is modifiable in that additional categories may be added, removed or modified upon system configuration. They included the following categories that will hence forth be termed Situation Categories within the Situation Element of Fair Privacy Policies and Preferences:

- Any: This indicates that entity is willing to divulge a personal data item in any situation.
- Social: This indicates that entity is willing to divulge a personal data item in a social situation. That is, between known friends, family and other people. For example, if an electronic personal organizer was requesting contact details.
- Commercial: An entity is willing to divulge personal data in situation where the data is to be used for marketing and/or survey type uses.
- Professional: An entity is willing to divulge personal data in situation where it is require in an employee or working capacity. For example an entity may need to provide personal details to the Human Resources department of the organization they are employed with.
- Services: An entity is willing to divulge personal data in a situation in which there is a clear indication of an exchange for service. For example some websites provide additional services if an entity provides their email address.
- Emergency: An entity is willing to divulge personal data if they are in an emergency type situation. For example an entity may provide their blood type and medical history if they require urgent medical attention that is dependent on such data.
- Restricted: This is basically the default case and means that the personal data item will not be divulged no matter the situation.

Privacy Preference Element	**Element Classification**
REWARD	None
	Monetary
	Service
	Identification
	Information
	Contract
	Restricted
SITUATION	Any
	Social
	Commercial
	Professional
	Services
	Emergency
	Restricted

Table 1: Summary of Reward and Situation Classifications.

IV. Practical Implementation and Application

Using a similar implementation approach to Hippocratic databases, a standard XPath engine is used to match privacy policies with personal privacy preferences. For the protection of personal data stored in a database other entities wishing to access the data need to generate a data request in the form of an XPath-based preference language such as XPref [18]. Within the submitted XML document the requestor specifies the values for the Reward and Situation elements, as well as any other P3P or EPAL notions if they needed. The XML Requestor document is passed to the servers XPath engine which runs the matching process against the stored data privacy preferences. The return result set are the records that have matching Reward and Situation element conditions and any other notions that have been set by requestors XML form.

In the situation where data is being requested on the semantic web, such as a web-site registration, then a process that works the same in principle to standard P3P policy and preference matching is initiated. The main differences are the extensions to the basic privacy preferences, in which the matching must be performed on the additional two elements of Reward and Situation. The actual process of matching is similar for both data at rest and data provided at the time of request. The idea of preferences matching and the specific details are not covered due to space limitations. However there are a number of implementations that operate on similar principles. The novel contribution of our proposal is the integration of the situation and reward elements into the preferences. Figure 1 provides a graphical representation of the preference and data request matching for data at rest in a database.

The flexibility offered by this framework allows entities to establish complex matrices of relationships between their perceived value of personal data elements and the situations in which they are requested. For example an entity E1 may specify a Monetary category with value $X for the Reward element on their home telephone number. This may be paired with a situation element setting of Commercial. Then when ever third party organizations request home telephone numbers for commercial use and offer a reward of $X or greater for that data E1's home telephone number will always be included in the data set divulged to the organizations. In turn E1 can expect a reward of $X or greater for each instance their home telephone number is revealed. This is of course dependent on the legal measures and enforcement procedures used by the initial data custodians to ensure remuneration is received.

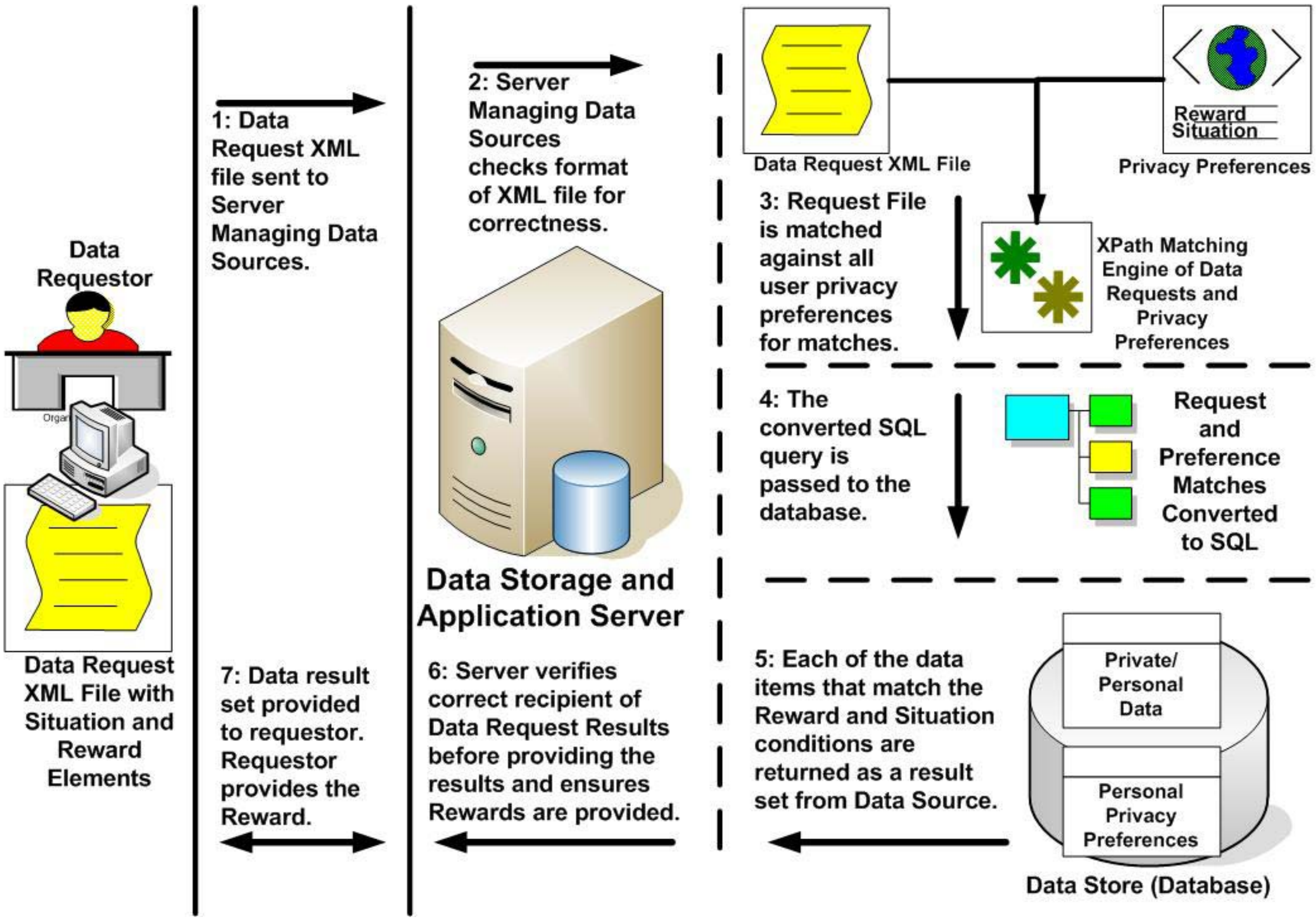
Data Requestor
Data Request XML File with Situation and Reward Elements
1: Data Request XML file sent to Server Managing Data Sources.
7: Data result set provided to requestor. Requestor provides the Reward.
2: Server Managing Data Sources checks format of XML file for correctness.
Data Storage and Application Server
6: Server verifies correct recipient of Data Request Results before providing the results and ensures Rewards are provided.
Data Request XML File
Reward
Situation
Privacy Preferences
3: Request File is matched against all user privacy preferences for matches.
XPath Matching Engine of Data Requests and Privacy Preferences
4: The converted SQL query is passed to the database.
Request and Preference Matches Converted to SQL
5: Each of the data items that match the Reward and Situation conditions are returned as a result set from Data Source.
Private/ Personal Data
Personal Privacy Preferences
Data Store (Database)

Figure 1: Process flow of matching Reward and Situation Privacy Preferences against those offered for access to an entity's personal data. Personal data elements matching preferences are accessible to the data requestor.

Information privacy and data security are very important in the area of health informatics. Health informatics involves the acquisition, storage, retrieval and use of information in health. Much of the information is composed of personal data including patient records, treatments, and medical history. Data of this type requires stringent privacy protection. Entities such as patients are often required to provide personal information for health purposes and therefore require tools to manage their privacy. The reasons for the collection and use of personal medical information are diverse, as are the situations in which data is acquired and processed. The integration of situation and reward elements into privacy preferences and policies facilitates the optimizing of health information management. Additionally, health privacy laws are equally diverse and in countries like the United States vary greatly from state to state. The laws are in thousands of statutes, regulations, common law principles and advisories with lack of uniformity across the country. Associating privacy preferences with health data ensures consistency of privacy protection across all domains.

For example, a patient may set a privacy preference situation element to 'Emergency', with a corresponding reward element to 'none'. This configuration of preferences would allow the entity's personal data to be automatically accessible to medical staff in the event of a medical emergency. The same entity may also have another configuration setting of 'Commercial' for situation and a number of options for reward such as 'Monetary', 'Service', or 'Information'. In this scenario then a health organization may request access to the entity's personal health records for research purposes and offers the entity some reward in return. This may be money, free health tests, or access to useful medical knowledge respectively. In all a cases the integration of situational and reward elements has facilitated better health informatics practices.

V. Conclusion

The conceptual framework proposed facilitates individual user perceptions on the evaluation of their privacy and personal data as it is affected by different contextual and situational conditions. Formally termed Fair Privacy Principles and Preferences (F3P), it integrates the subjective nature of privacy and its effect on privacy protection mechanisms and configuration. The solution incorporates the principles that entities are willing to trade-off their privacy for some form of reward and/or based on the situation and context of the personal data request. The rewards can include anything from monetary compensation, entering a formal binding contractual agreement, reciprocation of data exchange, or the Identification and Authentication of the entity requesting the data. Like the reward elements, the situational elements are also represented as extensions to privacy preferences defined by the user and stored along with their personal data. Defined categories within the framework for the situational element include: Any; Social; Commercial; Professional; Services; Emergency; Restricted. While implementation is not complete initial testing indicates that integration into current systems working with privacy preferences languages is an achievable objective for future work.

References

[1] IBM Research Division: Views of Privacy: Business Drivers, Strategy and Directions. IBM Research Report (2003)

[2] Clarke, R.: Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Xamax Consultancy Pty. Ltd. (1999)

[3] Cranor, L.F.: The Role of Privacy Enhancing Technologies. The Center for Democracy & Technology (2005)

[4] Laurant, C.: Privacy and Human Rights 2003. Electronic Privacy Information Center (2003)

[5] van Blarkom, G.W., Borking,J.J., Olk,J.G.E.: Handbook of Privacy and Privacy Enhancing Technologies. PISA (2003)

[6] Silvana, F.: Privacy in e-commerce: understanding user trade-offs. Issues in Information Systems (2005), Vol. VI, No.2, pp.83-89.

[7] IBM Tivoli Privacy Manager. http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus/

[8] Cranor, L., Langheinrich, M., Machiori, M., Presler-Marshall, M., and Reagle, J.: The Platform for Privacy Preferences 1.0 (P3P 1.1) Specification. W3CRecommendation, April (2002)

[9] Ashley, P., Hada, S., Karjoth, G., Powers, C., and Schunter, M.: Enterprise Privacy Authorization Language 1.2 (EPAL 1.2). W3C Member Submission, November (2003)

[10] PrivacyBird at http://www.privacybird.com

[11] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y.: Hippocratic Databases. In Proceedings of the 28th Int'l Conference on Very Large Databases, Hong Kong, China, August (2002)

[12] Directorate for Science, Technology and Industry: Inventory of Privacy Enhancing Technologies (PETs). Organization for Economic Cooperation and Development (2002)

[13] Goldberg, I.: Privacy Enhancing Technologies for the Internet, II: Five Years Later. PET2002, San Francisco, USA (2002)

[14] Oberholzer, H.J.G. and Olivier, M.S.: Privacy Contracts as an Extension of Privacy Policies. Privacy Data Management 2005, Tokyo, Japan (2005)

[15] Nissenbaum, H.: Privacy as Contextual Integrity. Washington Law Review, Vol. 79:119, (2004)

[16] Osbakk, P. and Ryan, N.: Context, CC/PP, and P3P. UbiComp 2002 Ubiquitous Computing International Conference, Göteborg, Sweden (2002)

[17] Wishart, R., Henricksen, K., and Indulska, J.: An Access Control Scheme for Ubiquitous Computing Environments Based on Context Dependent Privacy Preferences. ACISP 2005, Brisbane, Australia, 4-6 July (2005)

[18] Hann, I., Hui, K.L., Lee, T.S., and Png, I.P.L.: The Value of Online Information Privacy: An Empirical Investigation. SSRN: http://ssrn.com/abstract=391993, March, (2003).

[19] Jaisingh, J., Barron, J., Chaturvedi, A., and Mehta, S.: Privacy on the Internet: An Economic Analysis. Proceedings of the Americas Conference on Information Systems (AMCIS 2002), Dallas, Texas, August (2002)

[20] Yingxin (Sheila) He, Dawn N. Jutla, "Contextual e-Negotiation for the Handling of Private Data in e-Commerce on a Semantic Web," HICSS, p. 62a, Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06) Track 3 (2006)

[21] The CUSP Project. E-Privacy Research. http://cusp.smu.ca/default.htm

[22] Skinner, G. & Chang, E.: 'Dynamic user reconfigurable privacy and trust settings for industrial collaborative environments', Proceedings of IEEE's 3rd International Conference on Industrial Informatics (INDIN), Perth, Australia, 10-12 August (2005)

[23] Traore, I. and Khan, S: A Protection Scheme for Collaborative Environments. ACM 1-58113-624-2 (2003)

[24] Agarwal, D., Jackson, K., and Thompson, M.: Securing Collaborative Environments. ACE Working Group Grid Forum. SciDAC Security Panel - June 21 (2002)

[25] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y.: Implementing P3P Using Database Technology. 19th International Conference on Data Engineering, Bangalore, India (2003)

[26] Ceravolo, P., Damiani, E., Capitani di Vimercati, S., Fugazza, C., and Samarati, P.: Advanced Metadata for Privacy Aware Representation of Credentials. International Workshop on Privacy Data Management, National Center of Sciences, Tokyo, Japan, April 9 (2005)

[27] Agrawal, R., Kiernan, J., Srikant, R., and Xu, Y.: An XPath based Preferences Language for P3P. In WWW2003, Budapest, Hungary, May (2003)

[28] Cranor, L., Langheinrich, M., and Marchiori, M.: A P3P Preference Exchange Language 1.0 (APPEL1.0). W3C Working Draft, February (2001)