



**HAL**  
open science

## A Model for Personalised Perception of Policies

Anirban Basu, Stephen Marsh, Mohammad Shahriar Rahman, Shinsaku Kiyomoto

► **To cite this version:**

Anirban Basu, Stephen Marsh, Mohammad Shahriar Rahman, Shinsaku Kiyomoto. A Model for Personalised Perception of Policies. 10th IFIP International Conference on Trust Management (TM), Jul 2016, Darmstadt, Germany. pp.52-62, 10.1007/978-3-319-41354-9\_4 . hal-01438348

**HAL Id: hal-01438348**

**<https://inria.hal.science/hal-01438348v1>**

Submitted on 17 Jan 2017

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution 4.0 International License

# A model for personalised perception of policies

Anirban Basu<sup>1</sup>, Stephen Marsh<sup>2</sup>, Mohammad Shahriar Rahman<sup>1</sup>, and  
Shinsaku Kiyomoto<sup>1</sup>

<sup>1</sup> KDDI R&D Laboratories, Japan

{basu, mohammad, kiyomoto}@kddilabs.jp

<sup>2</sup> University of Ontario Institute of Technology, Canada

stephen.marsh@uoit.ca

**Abstract.** We are often presented with policy terms that we agree with but are unable to gauge our personal perceptions (e.g., in terms of associated risks) of those terms. In some cases, although partial agreement is acceptable (e.g., allowing a mobile application to access specific resources), one is unable to quantify, even in relative terms, perceptions such as the risks to one’s privacy. There has been research done in the area of privacy risk quantification, especially around data release, which present macroscopic views of the risks of re-identification of an individual. In this position paper, we propose a novel model for the personalised perception, using privacy risk perception as an example, of policy terms from an individual’s viewpoint. In order to cater for inconsistencies of opinion, our model utilises the building blocks of the analytic hierarchy process and concordance correlation. The quantification of perception is idiosyncratic, hence can be seen as a measure for trust empowerment. It can also help a user compare and evaluate different policies as well as the impacts of partial agreement of terms. While we discuss the perception of risk in this paper, our model is applicable to perception of any other qualitative and emotive feature or thought associated with a policy.

**Keywords:** trust, perception, personalised, qualitative, privacy, risk, policy

## 1 Introduction

As pervasive computing devices – smart watches, smart phones, tablet and personal computers – increasingly become sources of personal data, many services require users to agree with terms and conditions of usage and data sharing including access to various device features, e.g., camera, microphone and location tracking. Some of these requested features and attributes may be optional while some others may not be. Users often opt for default settings and agree with the terms and conditions without having clear understandings of what such agreements constitute.

On the other hand, organisations collecting personal data (upon agreements with users) aim to quantify privacy guarantees from macroscopic perspectives. For instance, privacy guarantees are made about the re-identifiability of an individual from a collection of personal data that is either made public or shared

with other organisations. However, one user may be more sensitive to giving away certain personal information than another user, and thus feel uneasy with generalised privacy guarantees. Macroscopic privacy guarantees are unable to capture those nuances stemming from personalised perspectives.

In this position paper, we assume that a mapping exists that can transform a policy to a set of attributes that users can understand. This may be simply a breakdown of complex legal terms into user-friendly attributes. We propose a mechanism to help users make quantitative evaluations of a policies (e.g., in terms of risks) based on criteria that the users can define. These quantitative evaluations are also expected to help users compare policies from their own perspectives. These quantifications of subjective opinion aid the trust reasoning processes at the users' ends, by enabling personalised interpretations to each user. Though quantitative, the evaluations are highly subjective and therefore the interpretation of policies cannot be compared across users.

The remainder of the paper is organised as follows. In section 2, we present a brief description of related work followed by a background of the Analytic Hierarchy Process in section 3. We propose our model for personalised perception (of privacy risks) in section 4. We discuss the relation of this work with trust empowerment in section 5 before concluding with pointers to future work in section 6.

## 2 Related work

When datasets containing sensitive information about individuals are released publicly or shared between organisations, the datasets go through what is known as privacy preserving data release (PPDP). Various anonymisation models, e.g.,  $k$ -anonymity [1],  $l$ -diversity [2], and  $t$ -closeness [3] can be employed to minimise the possibility of re-identification of an individual from the released data. Such a re-identification poses a privacy risk. The anonymisation models used to minimise this risk typically quantifies the probability of re-identification in the theoretical worst-case scenarios. There has been work [4, 5] on modelling the risk of re-identification from empirical analysis in comparison with theoretical guarantees.

In an approach somewhat different from the aforementioned PPDP, the idea of differential privacy [6] ensures that responses to queries on data models based on sensitive data do not give away any hint from which the presence or the absence of a particular data record, pertaining to an individual, can be inferred. Privacy-preserving data mining (PPDM) aims to build various machine learning models [7–14] to ensure the privacy of the sensitive data used in building those models. Typically, the privacy is preserved through operations in encrypted domain or through perturbation of the data. The former approach has a tradeoff with efficiency due to the use of computationally intensive homomorphic encryption while the latter approach presents a tradeoff with accuracy, and thus utility of the data. None of these models cater for any personal interpretation of privacy.

In a different research strand, Murayama et al's work [15] surveys the 'sense of security' (particularly within the context of Japanese society), which is a personal perspective. Winslett et. al's work [16,17] proposes a mechanism for trust negotiation based on interpretation of policies. Kiyomoto et. al's work on privacy policy manager [18] discusses a framework that enables interpreting privacy policies easier for users, which has been standardised by the oneM2M initiative [19]. Kosa et. al, [20] have attempted to measure privacy with a finite state machine representation. Li et. al's work [21] attempts to make users' privacy preferences more usable through modelling such preferences based on clustering techniques to identify user profiles.

Morton's work [22] suggests that besides understanding privacy from a generalised level, focus should be given to individual's privacy concern. As a first step to developing this paradigm, an exploratory study has been conducted to investigate the technology attributes and the environmental cues (e.g., friends' advice and experiences, media stories amongst others) that individuals take into consideration. Wu et. al's work [23] analyse users' behaviour towards personal information disclosure with relation to the order in which personal data attributes are requested.

Stemming from the concept of privacy personalisation, in this paper, we have embarked on the quantification of subjective personal perception (of risks, or any other factors) taking into account the inconsistencies that arise when quantifying such qualitative opinion. The objective of such quantification is to give users user-centric understandings of policies and their risks, so that such understanding may assist making decisions through the concept of trust empowerment [24].

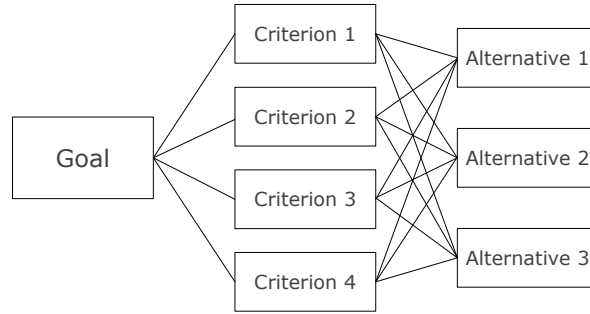
### 3 Background

#### 3.1 Analytic hierarchy process

The Analytic Hierarchy Process (AHP) due to [25] was developed in the 1970s. AHP helps with organising complex multi-criteria decision making processes. It can be used, for instance, in selecting a candidate for a vacancy based on multi-criteria evaluations in interviews. It can also be used in deciding a product to buy given various alternatives and multiple criteria for judging the alternatives. AHP can be visualised as a hierarchical structure between the goal, the selection criteria and the candidate alternatives. Figure 1 illustrates the hierarchies.

AHP assigns numeric values to the alternatives, thus facilitating a ranking. The ordering of the alternatives in such ranking is more important than the absolute numeric values associated with the alternatives. It is to be noted that in decision making problems where cost is a factor, the cost is generally not considered as a criterion in the AHP process so that each alternative ranked by the AHP can be evaluated in terms of utility-versus-cost. However, both qualitative and quantitative criteria can be used in AHP.

The relative importance of each criterion is determined at first using pairwise comparison. The integer scale [1 9] is used. For criterion X compared to Y, 1



**Fig. 1.** The Analytic Hierarchy Process in a diagram.

signifies that X and Y are *equally* important, 3 signifies that X is *moderately* more important than Y; 5 signifies X is *strongly* more important than Y; 7 signifies that X is *very strongly* more important than Y while 9 implies that X is *extremely* important in comparison with Y. The even values 2, 4, 6 and 8 can be used to specify the intermediate values. The inverse relation is multiplicative, i.e., if  $X : Y = 9$  (i.e., X is extremely important in comparison with Y) then  $Y : X = \frac{1}{9}$ .

This pairwise comparison is described as a matrix. Thus, for a  $k$  criteria comparison, we can have a comparison matrix  $\mathbf{C}$  of  $k \times k$  elements where the leading diagonal contains elements that are all 1 (i.e., every criterion compared with itself) and the upper triangular contains elements that are the multiplicative inverses of their corresponding elements in the lower triangular, i.e., any element  $C_{i,j} = \frac{1}{C_{j,i}}$  (even for  $i = j$ ). Saty showed in [25] that the principal eigenvector of the matrix  $\mathbf{C}\mathbf{c} = \lambda\mathbf{c}$  is a  $k$ -length vector  $\mathbf{c}$ , which contains the relative importances of the  $k$  elements of the criteria, which means that the criteria can now be ordered.

Having obtained a relative ordering of the criteria, each alternative is compared pairwise with each other for each criteria generating  $k$   $m \times m$  matrices given that there are  $m$  alternatives. Computing the eigenvectors of each such matrix produces a  $m \times k$  matrix of relative importances of the alternatives. Multiplying this matrix with the  $k$ -length criteria ranking vector will produce a  $m$ -length vector of weighted importances of each alternatives. This helps in ranking the alternatives and thereby making a decision. To keep things simple in this explanation, we have omitted the normalisation processes and the consistency ratio, which may arise from large inconsistencies in the way pairwise comparisons are made. In our proposed scheme, we only need to make use of the relative ordering of criteria.

## 4 Modelling perception

In this section, we propose a model to help users quantify, from their personal perspectives, the risks to their privacy associated with policy agreements. As

mentioned earlier, we use risks as an example but the model can be applied to any other factors too. These policies could be of different types, e.g., computer application terms of use, data release license, and so on. The key challenge in quantifying such personal perspectives is that they are highly qualitative and often inconsistent. We propose to make use of the well-known *analytic hierarchy process* to obtain quantification of subjective opinion. The quantifications are, however, indicative figures. When comparing the different policies, more importance should be attached to the relative ordering of policies than to the absolute quantitative values. The perspectives being personal, none of those quantitative figures are comparable between different users.

**Running example:** To help the reader conceptualise our proposal, let us assume, as a running example without loss of generality, that the user wishes to quantify her perceptions of two applications, X and Y, on her smart phone with respect to the policy of each application defines regarding the resources it wants to access.

#### 4.1 AHP based ranking of preferences

To quantify (risk) perception of a policy, we assume that the policy has been mapped into easy-to-understand constituent parts, such that the user is able to associate some or all the parts of the policy with corresponding preferences she has in her mind. The user is required to associate free-text labels to categorise the constituent parts of the policy. Consider, for instance, a mobile phone app requesting access to the back camera, the contacts list and the microphone. One user, Alice, may have a mental model whereby she labels the access to contacts list as *contacts-access*, and views a policy asking for permission to access this as not particularly intrusive. A different user, Bob, could group the access to both the camera and the microphone with his label, e.g., *av-recording-access*, and views access to these as intrusive. Such labels are personal requiring no consistency to be preserved between labels used by different users.

Let us assume that a specific user has defined labels as a set  $\mathbf{L}$  containing  $k$  elements:  $\{L_i\}_{i=1}^k$ . The constituent parts of a policy may be a superset of those labels. In other words, the labels defined by the user may not be exhaustive enough to exclusively tag all the corresponding elements of a policy. This is okay because the quantification of perception would be based on what can be tagged while the rest will be ignored (although, the user will be notified of this exclusion). Having constructed some labels, the user needs an importance ranking of those labels. The importance measure can either communicate a factor (e.g., risk) directly or it may communicate the inverse. For instance, in case of the inverse of the risk, the user is least concerned if the policy asks for something that matches a particular label, thus, the importance ranking will be inverse of the risk ranking.

To develop this internal model for ranking labels, we use pairwise comparisons in the analytic hierarchy process described in section 3. For simplicity yet without loss of generality, we do not take into consideration the situation where each

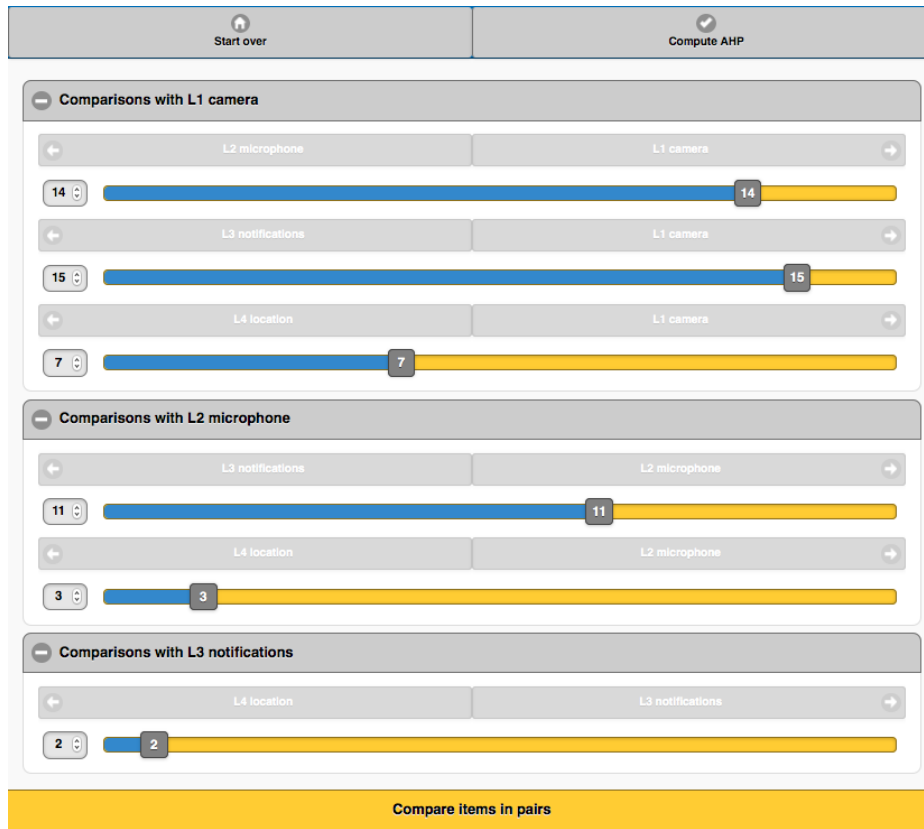
label may be further broken down into multiple labels, from a semantic point-of-view although we may consider this in future work. Thus, for  $k$  labels, we will need  $k(k-1)/2$  or, order  $\mathcal{O}(k^2)$  pairwise comparisons. If the set of labels is changed then a re-comparison is required to rebuild the label ranking. We assume that changing the label set is a relatively infrequent process. Assuming that the pairwise comparisons generate a ranking within the 10% acceptance level of the consistency ratio, the output of the AHP is a  $k$ -length preferences vector,  $\mathbf{v} = \{v_i\}_{i=1}^k$ , where each element  $L_i$  consists of a value  $v_i$ . These values can be used to determine the ranking of the labels.

**Running example:** Let us assume that the user labels four different resources as *camera* ( $L_1$ ), *microphone* ( $L_2$ ), *notifications* ( $L_3$ ) and *location* ( $L_4$ ). We use the web-based tool at <http://goo.gl/XAuleF> to compute the ranking of our labels through AHP. The tool allows for ranking a number of items through pairwise comparisons. Each pairwise comparison is done through a sliding scale where moving the slider to one side implies preferring the item on that side of the slider to the other. The left-most point in the scale is 1 and the right-most point is 17 with 9 being neutral. In terms of AHP comparisons, the slider value of 9 signifies neutrality, i.e., neither item is preferred to the other. This corresponds to the AHP comparisons representation of  $L_1 : L_2 = 1$ . Moving the slider towards  $L_1$  allows expressing the values of  $L_1 : L_2$  from 2 through 9, while moving the slider towards  $L_2$  allows representing the values of  $L_1 : L_2$  from  $\frac{1}{2}$  through  $\frac{1}{9}$  (or inversely, of  $L_2 : L_1$  from 2 through 9). The final result shows the ranked list of items, including the individual elements of the eigenvector (resulting from the AHP). The tool also helps scaling the importances of the ranks, which is beyond the scope of this paper.

Using this AHP computation tool, we express the quantification of importance in terms of risks in pairwise comparisons. Assume that the user inputs comparisons are as follows.

- $L_1 : L_2 = 6$  (14 on the slider of the AHP computation tool where 9 is in the middle signifying neutral).
- $L_1 : L_3 = 7$  (15 on the slider).
- $L_1 : L_4 = \frac{1}{3}$  (7 on the slider).
- $L_2 : L_3 = 3$  (11 on the slider).
- $L_2 : L_4 = \frac{1}{7}$  (3 on the slider).
- $L_3 : L_4 = \frac{1}{8}$  (2 on the slider).

Figure 2 shows our comparisons as done through the AHP computation tool. This sort of comparison translates to the fact that the user perceives the access to the camera 6 times as important as that to the microphone in terms of risk, while access to the location is seen as 3 times as important as that to the camera. AHP over that data generates ranking values of  $L_4 = 0.5690$ ,  $L_1 = 0.3054$ ,  $L_2 = 0.0817$  and  $L_3 = 0.0439$  with a consistency ratio of 0.086, or under 9%. Thus, we have the vector  $\mathbf{v} = \{0.3054, 0.0817, 0.0439, 0.5690\}$  corresponding to location ( $L_1$ ),



**Fig. 2.** The pairwise comparisons in the AHP tool showing our example comparisons.

camera ( $L_2$ ), microphone ( $L_3$ ) and notification ( $L_4$ ), respectively. This is consistent with the fact that the user views access to the location more important, with respect to privacy risk, than that to the camera and so on. Even though that conclusion may seem obvious at this point, AHP can smoothen out inconsistencies arising from the comparisons.

#### 4.2 Optimism or pessimism: negative, neutral or positive perception

When a new policy is encountered, some or all of its mapped terms are exclusively tagged with existing labels that the user has defined. The label-to-policy-term mapping is essentially one-to-one. Thereafter, the user is required to assign a numeric score,  $s_{t_i}$ , in a fixed positive numeric range, e.g.,  $[1 \ 10]$ . The range can be fixed once for all policies by the user. Such scores for all such policies are recorded by the local device, which can compute a centrality measure (e.g., median) for all those scores. Let us call this  $\bar{s}$ . A policy term  $t_i$  is considered to infer negative, neutral or positive perception,  $p_i$ , depending on if  $t_i < \bar{s}$ ,  $t_i = \bar{s}$  or  $t_i > \bar{s}$  respectively. Perception of negative, neutral or positive bias is inspired



by Marsh’s work on optimism and pessimism in trust [26]. Estimating individual term scores based on a central value  $\bar{s}$ , our model takes into account unintended biases that users have when they are asked to assign numeric scores. This process of determining perception evaluated against a  $k$ -element set of labels outputs a  $k$ -length vector of perceptions,  $\mathbf{p} = \{p_i|_{i=1}^k\}$ , where each label  $L_i$  corresponds to a perception  $p_i$  for a particular policy.

**Running example:** Let us assume that both applications X and Y have policy terms that can be mapped exactly to the user-defined labels, i.e., *camera*, *microphone*, *notifications* and *location*. In other words, each app requires access to each of the labelled resources and each such access is specified in a policy term. Let us also assume that the user rates each such policy term using a positive numeric scale [1–10]. Suppose the user attaches the following numeric scores to terms of X:  $s_{X_{t_1}} = 6$ ,  $s_{X_{t_2}} = 7$ ,  $s_{X_{t_3}} = 9$ ,  $s_{X_{t_4}} = 9$  where each  $t_i$  corresponds to  $L_i$ . Thus, the median is  $\bar{s}_X = 8$  and the equivalent perception vector is  $\mathbf{p}_X = \{-1, -1, 1, 1\}$ . Similarly, suppose the user attaches the following numeric scores to terms of Y:  $s_{Y_{t_1}} = 8$ ,  $s_{Y_{t_2}} = 7$ ,  $s_{Y_{t_3}} = 8$ ,  $s_{Y_{t_4}} = 9$ . The median is  $\bar{s}_Y = 7.5$  and the equivalent perception vector is  $\mathbf{p}_Y = \{1, -1, 1, 1\}$ .

### 4.3 Weighted score for policies

The perceptions of individual terms weighted by the preferences is obtained by computing a Hadamard or Schur product of the AHP-ranked preferences vector and the perceptions vector:  $\mathbf{v} \circ \mathbf{p}$ . An aggregate score for a policy is generated, in order to define a basis for comparison, by computing the average of the elements in the product  $\mathbf{v} \circ \mathbf{p} = \{v_i p_i|_{i=1}^k\}$ , i.e., a policy score  $r = \frac{1}{k} \sum_{i=1}^k v_i p_i$ . The closer to zero this score is, the implication is that both the positive and the negative perceptions of the policy balance out. Similarly, the more negative it is, the more negative perceptions rule; while the more positive it is; the policy contains mostly terms that the user has positive perception about.

**Running example:** Based on the previously computed perception vectors, we can now define the perception score for X as follows from the Hadamard or Schur product:  $r_X = ((-1) \times 0.3054 + (-1) \times 0.0817 + (1) \times 0.0439 + (1) \times 0.5690)/4 = 0.05645$ . Similarly, the score for Y will be:  $r_Y = (0.3054 - 0.0817 + 0.0439 + 0.5690)/4 = 0.20915$ . This means that user has a more positive view of the policy terms specified by Y than those specified by X, which is in accord with the perception vectors for the policies. In both cases, positive perceptions outweigh the negative ones but X loses out to Y. The quantitative values can help the user develop an idea of how much more favourable one policy is compared to another.

### 4.4 (Dis)similarity between two policies

A label-by-label comparison can also be done between any two policies, assuming that they correspond to the same set of labels exactly, or there exists a subset

of labels that are common to both policies. In this case, we assume that the user has a defined set of labels,  $\mathbf{L} = \{L_i|_{i=1}^k\}$ , but the user does not need the comparison of labels themselves, i.e., no need to construct the preferences vector. Assuming that two policies,  $P_1$  and  $P_2$  correspond completely and exhaustively to the same set of labels  $\mathbf{L}$ , the user assigns two sets of numeric scores for each label for each policy, represented by  $\{s_{1_{t_i}}\}$  and  $\{s_{2_{t_i}}\}$  respectively. As before, the centrality measures of these sets are computed separately as  $\bar{s}_1$  and  $\bar{s}_2$ . The two policies are considered to be concordant over a term  $t_i$  if  $s_{1_{t_i}} > \bar{s}_1$  and  $s_{2_{t_i}} > \bar{s}_2$  or  $s_{1_{t_i}} < \bar{s}_1$  and  $s_{2_{t_i}} < \bar{s}_2$ . They are said to be discordant over the same term if  $s_{1_{t_i}} > \bar{s}_1$  and  $s_{2_{t_i}} < \bar{s}_2$  or  $s_{1_{t_i}} < \bar{s}_1$  and  $s_{2_{t_i}} > \bar{s}_2$ . They are tied for that term if  $s_{1_{t_i}} = \bar{s}_1$  and  $s_{2_{t_i}} = \bar{s}_2$ .

A comparison of these two policies can be achieved by computing a non-parametric statistic, Somer's d, as  $d = \frac{C-D}{k-T}$  where  $C$  and  $D$  are the numbers of concordant and discordant terms and  $T$  is the number of terms tied between the two policies (while  $k$  is the total number of comparable terms). The Somer's d signifies the degree of similarity of the users' perception between the two policies. Similar to the policy score, this similarity measure is not comparable across users.

**Running example:** Given the perception vectors  $\mathbf{p}_X = \{-1, -1, 1, 1\}$  and  $\mathbf{p}_Y = \{1, -1, 1, 1\}$  both of which map to the exact same set of policy terms, we see that X and Y are concordant over terms  $t_2, t_3$  and  $t_4$ ; and discordant over term  $t_1$ . To compute the Somer's d, as  $d = \frac{C-D}{k-T}$ , we have  $C = 3, D = 1, k = 4, T = 0$ . Thus,  $d = \frac{3-1}{4-0} = 0.5$ . A positive Somer's d indicates *similarity* between the two policies while a negative d would have implied *dissimilarity*. The Somer's d has a range of  $[-1, 1]$ ; a value of  $-1$  means *most dissimilar* while 1 implies *most similar*. The value of 0.5 in this case implies that the policies are somewhat similar, while the previously obtained score of each policy offers an insight into how much favourable (or not) is one policy compared to the other.

## 5 Trust empowerment

We envisage that personalised perception of features, such as risk, enables users to have freedom and consistency in their thought process without having any clear idea about the policy terms. Trust is an inherently subjective phenomenon. Whilst this is often stated, it makes sense to repeat it occasionally. As we have noted before [25, 24] the systems that we and others build that 'use' trust should be seen in the light of empowerment through trust reasoning, not enforcement through mandating trust decisions. In accord with this position, we conjecture that there is a great deal to be gained from making as many parameters of the trust reasoning process as subjective and tailored to the specific user as possible. The use of subjective viewpoints of policies and the risks associated with them is a step in this direction. The hypothesis, then, is that subjective parameters increase the efficacy, tailorability and understandability of the computational trust reasoning process and its alignment to human users. An additional hypothesis

is that trust models built with such subjective notions tied to them are likely to be more robust against attacks that exploit homogeneity.

It goes without saying, of course, that intuitively there is sense here, whilst practically, much still needs to be done to confirm the intuition. Future work is planned that will work toward confirming our hypotheses, including user studies and simulations.

## 6 Conclusions and future work

In this position paper, we have introduced a novel idea for personalised quantification of emotive perceptions, such as privacy risks, associated with policies that, we believe, could assist users in making decisions through trust empowerment. The evaluation of the proposed scheme using the technology acceptance testing (TAM) and the consideration of semantic dependencies of policy terms, amongst others, are avenues of future work.

## References

1. Sweeney, L.: *k*-anonymity: a model for protecting privacy. *International Journal on Uncertainty Fuzziness Knowledge-Based Systems* **10**(5) (2002) 557–570
2. Machanavajjhala, A., Kifer, D., Gehrke, J., Venkatasubramanian, M.: *l*-diversity: Privacy beyond *k*-anonymity. *ACM Transactions on Knowledge Discovery from Data (TKDD)* **1**(1) (2007) 3–es
3. Li, N., Li, T., Venkatasubramanian, S.: *t*-closeness: Privacy beyond *k*-anonymity and *l*-diversity. In: *Data Engineering, 2007. ICDE 2007. IEEE 23rd International Conference on, IEEE* (2007) 106–115
4. Basu, A., Monreale, A., Trasarti, R., Corena, J.C., Giannotti, F., Pedreschi, D., Kiyomoto, S., Miyake, Y., Yanagihara, T.: A risk model for privacy in trajectory data. *Journal of Trust Management* **2**(1) (2015) 1–23
5. Basu, A., Nakamura, T., Hidano, S., Kiyomoto, S.: *k*-anonymity: Risks and the reality. In: *Trustcom/BigDataSE/ISPA, 2015 IEEE. Volume 1., IEEE* (2015) 983–989
6. Dwork, C.: Differential privacy. In: *Automata, languages and programming. Springer* (2006) 1–12
7. Vaidya, J., Clifton, C.: Privacy preserving association rule mining in vertically partitioned data. In: *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM* (2002) 639–644
8. Vaidya, J., Clifton, C.: Privacy-preserving *k*-means clustering over vertically partitioned data. In: *Proceedings of the ninth ACM SIGKDD international conference on Knowledge discovery and data mining, ACM* (2003) 206–215
9. Evfimievski, A., Srikant, R., Agrawal, R., Gehrke, J.: Privacy preserving mining of association rules. *Information Systems* **29**(4) (2004) 343–364
10. Polat, H., Du, W.: Privacy-preserving collaborative filtering on vertically partitioned data. *Knowledge Discovery in Databases: PKDD 2005* (2005) 651–658
11. Yu, H., Jiang, X., Vaidya, J.: Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data. In: *Proceedings of the 2006 ACM symposium on Applied computing, ACM* (2006) 603–610

12. Laur, S., Lipmaa, H., Mielikäinen, T.: Cryptographically private support vector machines. In: Proceedings of the 12th ACM SIGKDD international conference on Knowledge discovery and data mining, ACM (2006) 618–624
13. Amirbekyan, A., Estivill-Castro, V.: Privacy preserving DBSCAN for vertically partitioned data. In: Intelligence and Security Informatics. Springer (2006) 141–153
14. Basu, A., Vaidya, J., Kikuchi, H., Dimitrakos, T., Nair, S.K.: Privacy preserving collaborative filtering for SaaS enabling PaaS clouds. *Journal of Cloud Computing* **1**(1) (2012) 1–14
15. Murayama, Y., Hikage, N., Hauser, C., Chakraborty, B., Segawa, N.: An Anshin Model for the Evaluation of the Sense of Security. In: System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. Volume 8., IEEE (2006) 205a–205a
16. Winslett, M., Yu, T., Seamons, K.E., Hess, A., Jacobson, J., Jarvis, R., Smith, B., Yu, L.: Negotiating trust in the web. *Internet Computing, IEEE* **6**(6) (2002) 30–37
17. Lee, A.J., Winslett, M., Perano, K.J.: Trustbuilder2: A reconfigurable framework for trust negotiation. In: Trust Management III. Springer (2009) 176–195
18. Kiyomoto, S., Nakamura, T., Takasaki, H., Watanabe, R., Miyake, Y.: PPM: Privacy policy manager for personalized services. In: Security Engineering and Intelligence Informatics. Springer (2013) 377–392
19. Datta, S.K., Gyrard, A., Bonnet, C., Boudaoud, K.: oneM2M architecture based user centric IoT application development. In: Future Internet of Things and Cloud (FiCloud), 2015 3rd International Conference on, IEEE (2015) 100–107
20. Kosa, T.A., El-Khatib, K., Marsh, S.: Measuring privacy. *Journal of Internet Services and Information Security (JISIS)* **1**(4) (2011) 60–73
21. Lin, J., Liu, B., Sadeh, N., Hong, J.I.: Modeling users mobile app privacy preferences: Restoring usability in a sea of permission settings. In: Symposium On Usable Privacy and Security (SOUPS 2014). (2014) 199–212
22. Morton, A.: “all my mates have got it, so it must be okay”: Constructing a richer understanding of privacy concernsan exploratory focus group study. In: Reloading Data Protection. Springer (2014) 259–298
23. Wu, H., Knijnenburg, B.P., Kobsa, A.: Improving the prediction of users disclosure behavior by making them disclose more predictably? In: Symposium on Usable Privacy and Security (SOUPS). (2014)
24. Dwyer, N., Basu, A., Marsh, S.: Reflections on measuring the trust empowerment potential of a digital environment. In: Proceedings of the IFIP WG11.11 International Conference on Trust Management (IFIPTM), Malaga, Spain. (2013)
25. Saaty, T.L.: The analytic hierarchy process: planning, priority setting, resources allocation. McGraw-Hill (1980)
26. Marsh, S.: Optimism and pessimism in trust. In: Proceedings of the Ibero-American Conference on Artificial Intelligence (IBERAMIA94). (1994)