Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 37 (2014) 143 – 152

Procedia Computer Science

The 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN-2014)

A Model for Privacy Compromisation Value

Kambiz Ghazinour[a]*, Amir H. Razavi[a], Ken Barker[b]

a School of Electrical Engineering and Computer Science, University of Ottawa, Ottawa, Canada
b Department of Computer Science, University of Calgary, Calgary, Canada

Abstract

Privacy concerns exist whenever sensitive data relating to people is collected. Finding a way to preserve and guarantee an individual's privacy has always been of high importance. Some may decide not to reveal their data to protect their privacy. It has become impossible to take advantage of many essential customized services without disclosing any identifying or sensitive data. The challenge is that each data item may have a different value for different individuals. These values can be defined by applying weights that describe the importance of data items for individuals if that particular private data item is exposed. We propose a generic framework to capture these weights from data providers, which can be considered as a mediator to quantify privacy compromisation. This framework also helps us to identify what portion of a targeted population is vulnerable to compromise their privacy in return for receiving certain incentives. Conversely, the model could assist researchers to offer appropriate incentives to a targeted population to facilitate collecting useful data.

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.

Keywords: Privacy; Concept lattice; Formal Concept; Compromisation.

1 Introduction

Privacy concerns are not new and have likely been with us since humans formed social groups. One early example of privacy law was set by the Justices of The Peace Act (England, 1361), which specified penalties for eavesdropping and peeping toms [9, 13]. Modern data collection methods have rendered these naïve early laws

* Corresponding author. *E-mail address:* kghazino@uottawa.ca

Peer-review under responsibility of the Program Chairs of EUSPN-2014 and ICTH 2014.
doi:10.1016/j.procs.2014.08.023

inadequately. With the emergence of social networks, online banking, and electronic health services, we are often required to provide personal information to receive services. There are several instances where providing personal information can benefit society such as: sending voting ballots to the eligible citizens, making economic and social strategic plans using census information items, and providing customized news or commercial ads. However, not all the people have the same privacy concerns about their Personal Identifiable Information (PII). For example, some people are not willing to disclose any information about themselves and refuse to use credit cards, while others willingly participate in activities that require full information about themselves, including posting their home address and phone number on their public social network profile.

It has been shown that some people are either naïve or unconcerned about their privacy and are willing to release such information without personal benefit [11,14]. However, nearly 25% place a very high value on their private information while 57% are pragmatic and willing to trade privacy for a returned value. Finding a way to value privacy in such a way that the provider can receive a return for giving their private information to a collector is the subject of on-going research. The collector can then receive a value for the collected data either in terms of increased utility within its own organization or by re-selling it in conformance with the criteria specified at the time of collection [2]. Banerjee *et al.* [1] introduce a privacy violation model that provides an operational framework to characterize and estimate privacy violations in a relational database system. However, their model is not tested with real data to demonstrate its effectiveness. In this paper we present a model that is not restricted to a specific database system and utilizes a conceptual hierarchy to capture the privacy compromise. We have also tested our model by capturing individual *comfort levels* and mapping these to the privacy policies of a financial organization.

We initially utilize formal concept analysis to represent privacy concepts and in the next step, we illustrate the level of privacy compromise through a comprehensible weighted concept lattice. Finally, we measure the extent of the compromised privacy for several applications: *a)* to estimate a proper compensation in case of unwilling privacy breaches (e.g. stolen devices containing personal information and information lost through malicious software); *b)* to provide enough incentive to data providers to collect required information to conduct research projects.

1.1 Data collectors' concerns

It is understandable that people are concerned about their privacy and are willing to take action to protect their private information. However, why should data collectors care about the privacy of their customers? There are three main reasons: data accuracy, legal issues, and trust.

Data accuracy: Data collectors want to have more accurate data because it has more utility. Williams and Barker [15] show that allowing data providers to select the level of specificity when providing data makes them more willing to reveal more accurate private data. In other words, when the data provider observes that the collector respects their privacy, they provide more accurate answers.

Legal issues: Data collectors want to avoid potential legal repercussions arising from unauthorized use or disclosure of customer's private information that is costly and damages their reputation.

Trust: Protecting customer's privacy increases their loyalty and demonstrates that the service provider/data collector values individual's privacy. Organizations that do not protect the privacy of their customers will gradually lose their customers due to lack of trust. Note that this is true even for the most powerful companies such as Facebook. A comparison[†] between Facebook's data use policy from 2005 to 2012 and their introduction of several new privacy setting features for the users shows that they have sensed the public's privacy concern and try to address it. Customers are getting more concerned about shopping online from websites that do not have a secure and trustable service. Hence, they tend to use sites that have this protection service in which they can trust (e.g. the VeriSign Authentication Services[‡]). Also, by enforcing privacy laws one can be assured that such companies must follow privacy guidelines and protect the privacy of the customers if the proper tools are provided to them.

To fulfil the three above conditions it is beneficial for the data collectors to negotiate with the data providers upon obtaining their information and offer them a value compensating them for compromised privacy if it is acceptable by the data provider. Furthermore, each data provider must be allowed to value their privacy uniquely because people may have different privacy preferences around different pieces of data so there is no single solution [11].

[†] http://www.statista.com/statistics/157452/development-of-privacy-on-facebook-since-2005/
[‡] http://www.verisign.com/

1.2 Motivation and terminology

Our model benefits data providers and collectors: this model can be used to assist data providers understanding the extent to which their data can be used. It also supplies data collectors with a measure of data usage. Furthermore, it guides the data collectors to provide proper incentives thereby increasing data applicability for the data collected.
To achieve these goals we tailored formal concept analysis [16] and weighted lattices. To apply these methods we initially introduce and customize the following terms:

Privacy elements: are the components of data privacy including purpose, visibility, granularity and retention of the data which are used to construct a privacy policy. These elements will be discussed in Section 3.

Formal concept analysis: is a mathematical modeling schema to represent concepts as sets of objects and their corresponding attributes. We apply this method to analyze privacy elements and the relationships among them. This is discussed in Section 4.

Conceptual lattice: is a lattice structure derived from the relationships among the concepts depicted in the formal concept analysis schema.

Privacy lattice: is a conceptual lattice that illustrates the privacy elements in a lattice structure. It is discussed in more detail in Section 3.

Privacy compromisation *value (pcv)*: is a value determined by the data providers to represent how comfortable they are with their data being used by the collectors. Section 3 will discuss this in more detail.

To assess the feasibility and practicality of the model, we conducted an experiment on real data (see Appendix A).

2 Background

2.1 Data privacy

Since the terminology found in the literature is often ambiguous, we start by providing some privacy nomenclature and its relationship to this work. Based on the Barker *et al.* [3] definition, the data provider is an individual or organization providing data to be stored or used for particular purposes. Data providers share personal information if they trust the organization and perceive benefits in return. The data provider may or may not be the owner of the data. The data collector is an individual, enterprise or organization that collects data from the data providers to provide service to them. A third-party is any individual, enterprise or organization that acquires the provided data from the collector. Barker *et al.* [3] introduce a data privacy taxonomy that captures purpose, visibility, granularity, and retention as privacy elements that should be addressed in any privacy-aware model.

2.2 Capturing Privacy in a Lattice Structure

Each privacy predicate of purpose, visibility, granularity and retention can be represented in a lattice format [7]. Capturing these privacy predicates in lattice structures has its own challenges and benefits [6]. The lattice-based privacy aware model [7] facilitates negotiation between data providers and collectors. The lattice structure allows the data provider to specify stronger and more detailed reasons for the collector to access the provided data.
In brief, the following steps have to be taken: First, the data collector according to its policies constructs privacy lattices (e.g. the task is performed by the Chief Privacy Officer (CPO)). Second, depending on the flexibility of the data collector and privacy legislation in place, a subset of the lattice is described for the data provider to choose from. The nodes in this subset are considered legitimate for the data collector to access. However, the nodes located on the path from the selected nodes to the least upper bound (root) node of the lattice are not legitimate to access. A privacy violation occurs if the data collector wants to access the data for an illegitimate node [7].

Before addressing the privacy compromisation value, we briefly explain the way lattices are constructed from a conceptual perspective as it helps to understand privacy compromisation effects on the lattice hierarchy.

2.3 Formal Concept Analysis

Formal concept analysis is a mathematization of the philosophical understanding of a concept. It is a human-centric method that structures and analyzes data. A concept can be defined as a set of objects and attributes. A simple example is the concept of a "bank account". What drives us to call a financial object a "bank account"? Every object with certain attributes is called "bank account"; e.g., a bank account has account holder's name, account number, balance, *etc*. Hence, the objects that have these attributes are called "bank accounts" including a saving account, a chequing account, a business account, *etc*.
A formal context [16] in general consists of a set of objects A, a set of unary attributes B, and an indication of which objects have which attributes. A (formal) specific concept of a generic context is defined to be a pair (A_i, B_i) such that:

- $A_i \subseteq A$ and $B_i \subseteq B$
- every object in A_i has corresponding attributes in B_i
- for every object in A that does not exist in A_i, there is at least one attribute in $(B|B_i)$
- for every attribute in B that does not exist in B_i, there is at least one object in $(A|A_i)$

A is called the *concept's extension* and B is the *concept's intension*. The sets of concepts are embedded in the context set. Those sets and their relationships are the basis for all conclusions. Any concept we recognize and any implication deduced is based on the context. In short, the context is the universe of discourse. Changing the context will change the concepts and their structures.
A group (G, M, I) of objects G, attributes M and a relationship I is called a formal context. Wormuth and Becker [16] introduce the derivation operator $'$ to define formal concepts of a given context in a mathematical way. Applying the derivation operator on a set of objects A and set of attributes B, results in sets A' and B':

A' = all attributes of M shared by the objects of A
B' = all objects in G that have all attributes of B

Formal concepts are pairs of sets (A, B) of objects and attributes that fulfil the two conditions of $A' = B$ and $B' = A$. To generate formal concepts the following steps should be taken:

1. Pick a set of objects A.
2. Derive the attributes A'.
3. Derive $(A')'$ also denoted as A''.

For example, according to the above definitions (A'', A') is a formal concept.
Table 1 illustrates a list of attributes and objects in the context of "banking". A sample formal concept can be generated as follows:

A_1 = {verification}
A_1' = $\{a_1, a_2, a_4\}$
$(A_1')' = A_1''$ = {mortgage, insurance, verification}
(A_1'', A_1')= ({mortgage, insurance, verification}, $\{a_1, a_2, a_4\}$)

2.4 The Conceptual hierarchy

There are certain concepts that contain all the attributes of other concepts in addition to their own attributes. Putting those concepts in an ordered (partially or totally ordered) set will result in a lattice in which the nodes are organized by means of their attributes, which are abstract representations of the different concepts and their relationships.
For instance, Table 1's set of attributes and objects have formal concepts that can be derived as follows:
(A_2'', A_2') = ({line of credit}, $\{a_1, a_3, a_4, a_5, a_6, a_7\}$)
(A_3'', A_3') = ({service enhancement}, $\{a_1, a_3, a_4\}$)
According to Wormuth and Becker [16], the formal concept (A_3'', A_3') is called the super-concept of (A_2'', A_2') and by definition (A_2'', A_2') is the sub-concept of (A_3'', A_3').
Fig. 1 illustrates the hierarchy of the concepts. For example since line of credit is sub-concept of service

enhancement, it is drawn below it and connected with lines and so on. Several methods (e.g., Ganter's [5] or Lindig's algorithms [12]) can be used to derive all formal concepts from a set of attributes and objects. Describing the methodology of these algorithms is beyond this paper's scope however it exploits the hierarchical structure, which is the outcome of these algorithms.

The sub-concept–super-concept relationship defines an order for the set B of all formal concepts of a formal context. For each set B, there exists a unique greatest sub-concept (meet) and a unique smallest super-concept (join). The ordered set B with this property forms a mathematical structure called *concept lattice*.

Table 1. A sample list of attributes and objects in the context of banking.

		mortgage	insurance	line of credit	remote services	service enhancement	verification	safety & security
a_1	personal information	X	X	X	X	X	X	X
a_2	family information	X	X				X	
a_3	Income	X	X	X		X		
a_4	credit information	X	X	X	X	X	X	
a_5	debt	X	X	X				
a_6	property information	X	X	X				
a_7	stocks and investments	X	X	X				
a_8	health information	X	X					
a_9	travel information		X		X			X

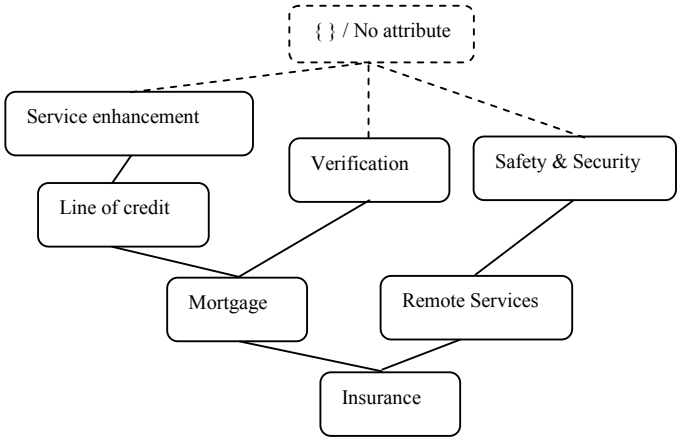

Fig. 1. Concept hierarchy structure

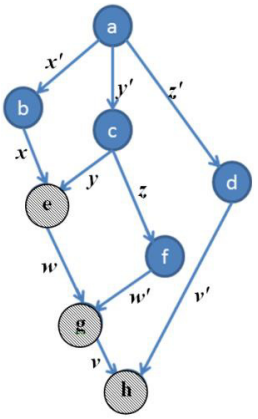

Fig. 2. A weighted lattice

3 Weighted Conceptual Lattice

3.1 Concept lattice

As Fig. 1 illustrates, the greatest super-concept has zero attributes but it contains all of the objects. For a better understanding, we can assume the super-concept as a super-class in object oriented school of thought. On the other hand, the smallest sub-concept, insurance, has all the attributes from a_1 to a_9. If there are no objects that can have (or be related to) all the attributes, we can define a node that has all the attributes and is the sub-concept of all the nodes. We assume that the CPO constructs the lattices from privacy elements. For instance, we put *verification* as super-

concept of *mortgage* in the purpose hierarchy since *mortgage* implicitly contains objects and attributes corresponding to *verification*. The concept of *mortgaging* can be defined as a set of attributes (i.e. workflow of the business model [10], actions that need to be performed for giving mortgage or even data items that are used for this concept).

Considering a concept lattice for privacy elements, we define a privacy violation as follows.

***Definition 1 (Privacy Violation)*:** When the data is intended to be used for a concept with a set of attributes A, and instead is used for another concept with the set of attributes B, a privacy violation occurs if $B \not\subset A$.

An example of privacy violation would be that the customer provides a data to be used for *service enhancement* purpose and instead it is used for *line of credit* or *verification* purposes. In contrast, if the customer provided data for giving *line of credit* purpose and instead it is used for *service enhancement*, since the attributes of *services enhancement* are the subset of those of *line of credit*, no privacy violation occurs.

3.2 Weighted lattice

Section 3.1 describes the hierarchical concepts and explains that when moving from a concept to its super-concept, a privacy compromisation may occur since the super-concept does not have the same set of attributes. Hence, each edge must be assigned values showing the amount of privacy compromisation if it occurs. In other words, by referring to the values of the edges in a path between two concepts one can calculate the compromised privacy.

Weighted graph is a well-studied structure that appears as a model for numerous problems, i.e. where nodes (cities, computers, *etc*.) are linked with different weights (distance, cost, *etc*.) [8]. Let (G,w) be a weighted graph and P be a path between two arbitrary nodes of G. $w(P)$, called the length of P, is the summation of all the weights of the edges on the path P. The distance between two vertices u and v, denoted by $distG,w(u, v)$, is the length of the shortest (with minimum length) (u, v)-path which is derived using Dijkstra's Algorithm [4].

Fig. 2 illustrates a weighted concept lattice where the grey nodes (concept) correspond to the legitimate nodes and the weights represent the amount of privacy compromisation that occurs from the data provider's point of view. Thus, using the data item with nodes *a, b, c, d* and *f* is a privacy violation. However, the level of privacy violation is different. The following scenarios show different privacy violations and their corresponding quantifications for the intended node *e*:

- the data is used for node *b* so the level of privacy violation is: $pcv(e,b) = dist_{G,w}(e,b) = x$.
- the data is used for node *c* so the level of privacy violation is: $pcv(e,c) = dist_{G,w}(e,c) = y$.

Based on this lattice, if data is intended to be used for node *e* and instead is used for node *a*, there are two possible paths where the violation may have occurred: 1) the data might be leaked from node *e* to node *b* and then from node *b* to node *a* which means $x+x'$ units of privacy violation; or 2) the data might be leaked from node *e* to node *c* and then from node *c* to node *a*, which means $y+y'$ units of privacy violation. Although the privacy violation has occurred from node *e* to node *a*, it does not necessarily mean that $x+x' = y+y'$. In other words, the path through which the privacy has been violated does matter. The impact of the privacy violations differs depending on, for example in the visibility lattice, who (a third party or government) reveals an individual's personal information.

To calculate the privacy compromisation value from node *e* to node *a,* we select the minimum distance from node *a* to node *e* based on the summations of the weights which is $min(x+x',y+y')$. Although we used the minimum function (shortest path) to estimate the privacy compromisation, depending on different real life scenarios the compensation could be also calculated through average or maximum *pcv* or its corresponding *incv*.

Deriving this privacy compromisation value for the illegitimate nodes located on the path between the intended node(s) to the root concept (i.e. node *b* in Fig. 2) is straightforward as discussed earlier. However, calculating the privacy compromisation value for the illegitimate nodes not located on the path (i.e. node *d* in Fig. 2) can be more difficult and is done using a different method. For instance, assume that *e* is the intended node for a data item and instead the data is used for node *f*. Assume that the data collector wanted to access node *e* and in the best-case scenario, he might have permission to use node *g* as well. Hence, the real privacy violation occurs from node *g* to *f* and the $pcv(g, f) = dist_{G,w}(g, f) = w'$. The following formalization explains how *pcv* is calculated.

Assume node *a* is the intended concept for the provided data and *b* is the node for which the data item is used:

if *b* is sub-concept of *a*:	$pcv(a,b) = 0$
elseif *b* is super-concept of *a*:	$pcv(a,b) = distG,w(a, b)$
else:	$pcv(a,b) = distG,w(\text{meet}(a,b), b)$

Knowing the *pcv* suggests how much incentive should be given to the data providers. The higher the *pcv* is, the more incentives should be offered. An incentive *incv*, can be represented as a function of *pcv*. The ratio of *incv* and *pcv* are application dependent. In this research, we consider *incv=f(pcv)* and leave it to the data collector to decide what incentive should be proposed to compensate for the compromised privacy. Finding a proper function (*f*) could be an interesting research topic in economics, sociology or psychology but is not considered further here.

3.3 Weighting process

Since each data provider might have different privacy preferences, they specify the weights for the lattice that represent the privacy violations that may occur to them. It is assumed that the range in which the providers specify their privacy compromisation level is set to be [*0*, *m*] where *0* represents no concern and *m* is the maximum privacy concern they could have. The range of *m* is application dependent and also related to the classifications of potential privacy violations that may occur.
The data providers are then given the chance to express their concerns and weight the edges of the lattice through a questionnaire and can be done in the data collection phase or afterwards. This will be illustrated in Section 4.
After the data collectors gather all the privacy compromisation values from the *n* data providers[§], they calculate the median[**] of the *n* values for each edge of the lattice to have an understanding of providers' privacy values.

4 The pcv-lattice applications

The resulting weighted lattice can be used for the following cases: a) To estimate a proper compensation in case of unwilling privacy breaches and b) To provide enough incentive to data providers in order to collect required information to conduct crucial research projects.

Assume matrix $L = [l]q \times n$ is constructed where:

1) Each element *lij* in matrix *L* shows the summation of all the *pcvs* on path *i* for the provider *j*, and 2) *q* is the number of path exits between the intended node and the provided node and *n* is the number of data providers. Finding *q* for each pair of nodes is a classic problem called *all simple paths*. A simple path in a graph does not have repeating vertices. The number of paths, *q*, is found using the classis depth first search algorithm[††].

This is formalized as: $lij = wpath(i,j) = \sum_{k=1}^{e(i)} \mathrm{pcv}_{ik}^{j}$ where:

1) *e(i)* is the number of edges that exist in path *i* and
2) pcv_{ik}^{j} is the *pcv* for the data provider *j* on the edge *k* on path *i*.

In other words, each element *lij* in matrix *L*, represents how sensitive the privacy of each data provider is which implies how much *incv* should be offered to them by the collector to componsate their privacy breaches for the data.
Based on the relationship *incv=f(pcv)*, the data collector has a *pcv* in hand that can be measured against the rows of matrix *L*. For comparison, each row of matrix *L* will be sorted in ascending format. $L' = \mathrm{sort}(L)$.
For each row in *L'*, all the elements that are less than or equal to the desired *pcv* of the data collector are counted and added to a list. The maximum value of the list then reveals how many providers could be componsated in return for getting the incentives that match the *pcv*. In case a) we need to know the *pcv* to componsate the entire community (100% of population) whose privacy is breached, whereas in case b), the collector may want to find enough *incv* that must be offered, m*incv*, to have at least *x*% of the community to provide their information.
For each row *i* of the matrix, a pointer will be set to the position where the number of elements on the left side is equal to *x*% of the row size. For instance, if *x* is equal to 50%, then the middle element that has the pointer will be

§ Collecting, storing and managing this privacy metadata can be accomplished in a number of standard ways used for other metadata. These methods are being compared to determine the most efficient mechanisms for such highly accessed data but the details are beyond the scope of this paper.
** Selecting other statistical operations such as average or mode is orthogonal to this process. In this work, we use median in order to capture the opinion of the *majority* of the providers.
†† Suggested by (NIST). http://xlinux.nist.gov/dads//HTML/allSimplePaths.html

appended to the list. If *x* is greater than 50%, then while there exists an element on the right side of the pointer, the percentage of the number of elements on the left side of the pointer is calculated. If it is greater than or equal to *x*%, the *pcv* referred by the pointer is added to the list, otherwise the pointer refers to the next element on the right. If *x* is less than 50%, then while there exists an element on the left side of the pointer, the percentage of the elements existing on the left side of the pointer is calculated. If it is less than or equal to x%, the *pcv* on the right side of the pointer is added to the list, otherwise the pointer refers to the next element on the left.
This process is repeated for every single row of the matrix. Eventually, the minimum value of the list is the *pcv*. Appendix A describes a real world study that we performed based on the proposed algorithm.

5 Conclusion and Future work

In this paper, we presented a model to capture possible privacy violations that may occur. We also defined a privacy compromisation value by using the notion of formal concept analysis and weighted concept lattice structure.
We further contribute by using the concept lattice structure to introduce a mechanism to evaluate the privacy compromisation value (*pcv*). This mechanism answered questions such as: How important is the data for the data providers? How much privacy is violated if the data is revealed or used in a manner that was not intended?
This paper demonstrates another advantage of capturing privacy elements in the lattice format which is the main message for the data privacy research community. Furthermore, the derived results will help the privacy community to adopt this model for privacy negotiations between the two parties (i.e. data providers and data collectors).
It is fruitful to extend the work done for capturing privacy compromisation value in the following directions: Performing experiments to measure the effectiveness of such model in commercial and online business platforms. This may involve experts from Social Studies to evaluate the outcome of such privacy compromisation values. Designing a recommendation system that suggests the data providers how they should set their privacy compromisation value based on their privacy preferences.

Appendix A

To demonstrate the proposed model in capturing the data provider's privacy compromisation and make it more concrete, the following experiment was performed.

As a sample, 100 graduate and undergraduate students were chosen randomly from different Faculties at the University of Calgary to answer 4 groups of questions regarding their sensitivity about disclosing data, such as date of birth, phone number, mailing address, and account balance. The students were not asked to provide their private information; but instead answered questions regarding their sensitivity about revealing their data to a data collector, third parties, and other organizations. The data providers were asked to express to whom and how precisely they would prefer their data to be revealed. For example, the data providers were asked whether they would authorize a financial institute to utilize their data. If the data providers agreed, according to the lattice construction definition [7], the financial institute and other descendant nodes would be the only entities that have access to the provider's data. Trivially, for any further data utilities, such as disclosure of data to a third party, the participants must be asked how comfortable they are about the data usage.

The questionnaire asked the providers to specify their data sensitivity and the privacy compromisation value using a discrete scale from 0 to 10. There was no context associated with each number and it was subject to the data providers' interpretation of what 4, for example, in the range 0 to 10 meant. The participants were told that 0 represents being not concerned at all and 10 represents being extremely concerned.

The questionnaire was designed in a way that answering the questions resulted in adding weights to the three lattices of purpose, visibility and granularity for each data item. The lattices were derived as simpler versions of the lattices introduced earlier [6] where a use case of the Royal Bank of Canada was discussed. After collecting the privacy compromisation values for all *n* participants, methods described in Section 4 were applied to the collected data. (Figures 3 and 4 show the corresponding lattices). The following example shows how the use case data can be utilized.

Example: The data collector wants to know how much proper incentive *incv* correspond to *pcv* should be offered to the data providers to have information of 60% of community size (e.g. their mailing address can be used for

protecting the personal safety of employees purposes). Using the method described in Section 4 reveals that if the data collector gives enough incentives that match the *pcv* of 6, there are 62% of people whose data will be available for the requested purpose. (Table 2 shows the sample of collected *pcvs* of each edge of the purpose lattice on mailing list).

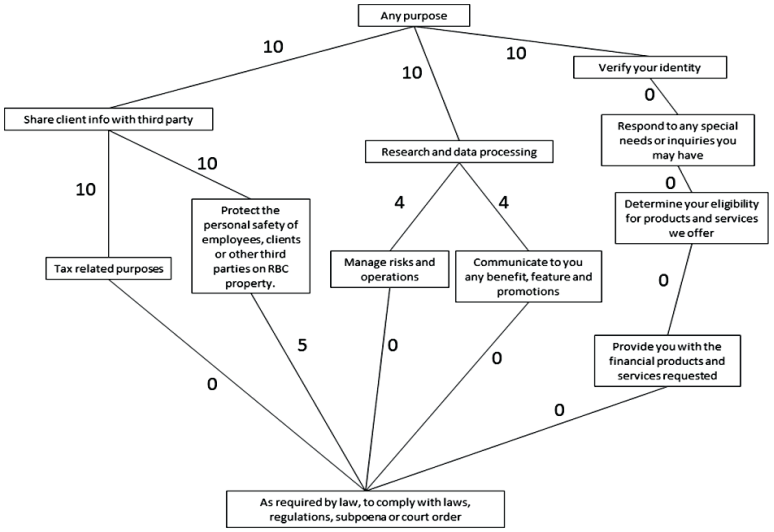

Fig. 3. Purpose lattice with the median *pcv* collected in the use case

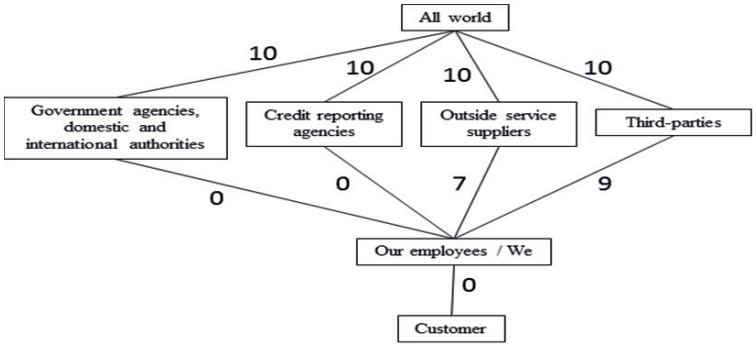

Fig. 4. Visibility lattice with the median *pcv* collected in the use case

Table 2. A sample of collected *pcvs* of each edge of the purpose lattice on mailing list

Any purpose	Sharing client info with third party	Research and data processing	Verifying your identity	Tax related purposes	Protecting the personal safety	Managing risks and operations	Communicating to you any benefit, …
7	5	3	0	0	4	0	5
10	7	0	0	0	0	0	0
10	10	10	0	0	10	10	10
10	10	8	0	0	10	9	4
10	10	6	0	0	0	0	0
0	6	0	0	0	0	0	0
:	:	:	:	:	:	:	:

References

1. Banerjee M., Karimi Adl R., Wu L. and Barker K. Quantifying Privacy Violations. SDM 2011, LNCS 6933, pp. 1–17, 2011.
2. Barker K. "Valuing" Privacy While Exposing Data Utility. LNCS, 2012, Volume 6121/2012, 1-2.
3. Barker K., Askari M., Banerjee M., Ghazinour K., Mackas B., Majedi M., Pun S. and Williams A. A data privacy taxonomy. In BNCOD 26: Proceedings of the 26th BNCOD, pages 42–54, Berlin, Heidelberg, July 2009. Springer-Verlag.
4. Cormen T.H., Leiserson C.E. and Rivest R.L. “Introduction to algorithms”. Prentice-hall,2002.
5. Ganter B. and Wille R. Formal Concept Analysis, Mathematical Foundations. Springer-VerlagBerlin 1998.
6. Ghazinour K. and Barker K. Capturing P3P Semantics Using an Enforceable Lattice-based Structure. Proceedings of the 2011 EDBT/ICDT Workshops, Sweden. 2011.
7. Ghazinour K. and Barker K.: A privacy preserving model bridging data provider and collector preferences. EDBT/ICDT Workshops 2013: 174-178.
8. Gross J. and Yellen J. 1999. Graph theory and its applications. CRC Press, Florida, USA.
9. Hondius, F.W. Data Law in Europe. Stanford journal of Int. Law, 16, 1980, pp. 87-111.
10. Jafari M., Safavi-Naini R., and Sheppard N. P. Enforcing purpose of use via workflows. In Workshop on Privacy in the Electronic Society, Chicago, IL, November 2009.
11. Kumaraguru P. and Cranor L.F. Privacy indexes: A survey of westin’s studies. Technical Report CMU-ISRI-5-138, Carnegie Mellon University, CMU, PA, USA, December 2005.
12. Lindig C. Fast concept analysis. In:Stumme G.: Working with Conceptual Structures Contributions to ICCS 2000. Shaker Verlag, Aachen, 2000, 152–161.
13. Soma, J. and Rynerson, S. 2008. Privacy Law in a Nutshell. West Publishing.
14. Westin A., 1967, Privacy and Freedom, New York: Atheneum
15. Williams, A. and Barker, K.: Controling inference: Avoiding p-level reduction during analysis. Journal of Research and Practice in Information Technology 40(3), 163–185 (2008).
16. Wormuth B. and Becker P.; Introduction to formal concept analysis, in: 2nd International Conference of Formal Concept Analysis. (2004), Sydney, Australia.