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/