Trust your Social Network According to Satisfaction, Reputation and Privacy

Yann Busnel, Patricia Serrano-Alvarado, Philippe Lamarre

Trust your Social Network According to Satisfaction, Reputation and Privacy

Yann Busnel
LINA / University of Nantes
2, rue de la Houssinière
BP 92208
44322 Nantes, France
Yann.Busnel@univ-nantes.fr

Patricia
Serrano-Alvarado
LINA / University of Nantes
2, rue de la Houssinière
BP 92208
44322 Nantes, France
Patricia.Serrano-Alvarado@univ-nantes.fr

Philippe Lamarre
LINA / University of Nantes
2, rue de la Houssinière
BP 92208
44322 Nantes, France
Philippe.Lamarre@univ-nantes.fr

ABSTRACT

Nowadays we are witnessing a massive usage of social networking sites (Facebook, MySpace, *etc.*). Those systems facilitate user interaction; however, they disregard users' wellbeing because users are forced to trust the network and to use the system without any guarantees. We consider that this is little satisfactory for systems where the users make the network successful thanks to their interactions.

In this work, we propose to study how to improve users' trust towards the system in terms of reputation, privacy and satisfaction. Despite former separate studies, we argue that these notions are strongly linked and must be analyzed in a correlated way.

Categories and Subject Descriptors

H.4 [**Information Systems Applications**]: Miscellaneous; C.2.4 [**Computer-communication networks**]: Distributed systems

General Terms

Privacy, Reputation, Satisfaction, Trust

1. INTRODUCTION

Recently, several sites, built on social networks, are web-based applications that allow users worldwide to publish potentially any kind of information (personal, professional, *etc.*), and interact with each other through services provided by the applications. Current examples of famous social networking applications include Facebook, MySpace, Twitter, Delicious and LinkedIn. In those large-scale networks, the more users are numerous and the amount of shared information is larger, the more the system is interesting and at-

tractive[1]. Users then make the network successful thanks to their interactions. However, actual systems disregard users' wellbeing. In fact, specific individual needs are generally not taken into account. Users are forced to *trust the system*, without any guarantees. Current systems aim to be considered as trustworthy in terms of efficiency and reliability, but ignore other subjective aspects like users' expectation or privacy of used data and resources. In general, they neglect users' satisfaction in favor of cost saving.

On the other hand, network size endlessly increases. Most of current social networks mainly rely on a client-server communication paradigm through which users (clients) connect to a web site (server, possibly geographically distributed for performance purposes) in order to make use of a wide set of available services. Those kind of systems are good for simplicity of use, deployment and maintenance but data privacy is completely ignored. As this approach currently reaches their bounds, numerous fully distributed solutions are designed and recent outcomes argue for their feasibility [6, 10, 21]. Peer-to-peer (P2P) paradigm facilitates scalability but also brings up some problems. Since peers are heterogeneous, some might be faulty or malicious, and cannot ensure services that provide enough quality. In order to restrain those behaviors, several systems attempt to increase user's trust toward the system by using reputation mechanisms [13, 20, 24]. Those mechanism can be used to help peers to distinguish *good* from *bad* partners which eventually enhances the users' satisfaction.

Reputation mechanisms require a size-able degree of sensitive information which can be personal, professional, behavioral, *etc.* Unfortunately, this goes against the privacy rights of individuals. In fact, the Organization for Economic Co-operation and Development (OECD) provides some guidelines that systems should consider in data privacy management (*cf.* Section 2.3) [16].

The aim of this position paper is to put down some milestones of a complementary 3-facet analysis (satisfaction, reputation and privacy) to allow users to trust the system. Our

---

[1]This attraction can be viewed from different points of view, *e.g.,* users who want to communicate with their friends, or commercial entities who are interested in data for business issues.

objective is to allow the deployment of fully decentralized architectures, which can define different degrees of users' trust towards the system in terms of, mainly, privacy, reputation and satisfaction (global and individual), according to different applicative contexts. Nevertheless, it is obvious that user's trust is not only linked to reputation, satisfaction and privacy, but our work consists in a first step and we have make the choice to start with this focus.

This paper is organized as follows. Section 2 introduces the three dimensions of our current work. Then, Section 3 presents the links that we identify between these dimensions. Section 4 presents the objectives of our proposition. We finally conclude and raise some open issues in Section 5.

2. SOME CONCEPTS TO TRUST THE SYSTEM

In this section, we briefly introduce the three dimensions used in this work. In the literature, they have been studied separately but we argue that they are intrinsically connected when trusting the system is a main challenge.

2.1 Satisfaction

Studying user satisfaction is generally motivated by an attempt to improve information systems. A full satisfaction requires a system which both provides results of good quality and is also usable accordingly to the user needs. For example, in the field of information retrieval, per-query answers relevance measures [8, 22, 19] provide standardized, repeatable measurements of search result quality while usability studies [5, 11] try to measure the user experience in a more direct way. Recently, in the context of query allocation and routing services, users' satisfaction – with respect to the system comportment – has been studied [3, 17]. It is defined as a long run notion evaluating the capacity of the system to follow the intentions of each participant. For instance, a data provider can be satisfied even if sometimes the system imposes queries he does not intend to treat, or a data consumer is satisfied because "in general" she receives answers from the providers she prefers. Here, quality of results is a private notion that is assumed to be used by a data consumer to decide which providers she prefers.

Intuitively, a participant is satisfied by the system process if the latter meets its *intentions* in the long term (*i.e.* matching users' expectations as a way to figure satisfaction). The *satisfaction* of participants may have a deep impact on the system, because they may decide whether to stay or to leave the system based on it. In [17], a complete model is proposed that characterizes autonomous participants by formally defining the adequacy, satisfaction, and allocation satisfaction of a participant.

Whatever the system (information retrieval, query or ressource allocation, social network, etc.), in order to define her intentions and strategy, a participant needs information about the system itself and its participants. Similarly, the system needs information about the participants to adapt himself to individual intentions and to evaluate participants' satisfaction. So, on one hand, there are needs of information about participants while on the other hand, the principles of privacy require sensitive information not to be disclosed.

As a consequence, a solution has to be built on the core idea of compromize, equilibrium of which may differ from one participant to the other.

2.2 Reputation

It is expected that systems remain reliable, efficient and secure even if they evolve or increase. Reputation systems contribute to this goal in systems based on a large-scale network composed by numerous autonomous and potentially untrusted participants. As proposed in [15], a reputation system design can be divided in three main basic blocks: *information gathering*, *scoring and ranking*, and *response*. Depending on the application context, these blocks can take various states. Application context includes expected user behavior (*e.g.,* churn, reliability, privacy, anonymity) as well as adversarial goals and power (*e.g.,* selfish peers, malicious peers, traitors, whitewashers) or environment limitation (*e.g.,* centralized vs decentralized).

Several decentralized solutions [4, 7, 13, 18, 20] have been recently proposed. For instance, among the most cited ones, Eigentrust [13] presents a PageRank-like algorithm that computes a global reputation rating by using transaction reports and the rating of the reporting peer. TrustMe [20] imposes that a transaction certificate be pairwise established before any transaction between involved peers takes place. PowerTrust [24] constructs a trust overlay network to model the trust relationships among peers.
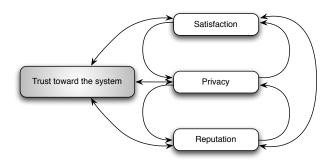
All these approaches need potentially sensitive information which can be personal, professional, behavioral, *etc.* that lead to privacy breaches. Recently, some studies have been proposed in order to ensure efficient reputation mechanisms, under classical anonymous assumption [2, 4]. These approaches permit to reach an interesting but challenging trade-off between reputation and privacy purposes. The latter are presented below.

2.3 Privacy

Data privacy is the right of individuals to determine for themselves *when*, *how* and *to what extent* information about them is communicated to others [23]. It has been treated by many organizations and legislations which have defined well accepted principles. According to the OECD guidelines [16], data privacy should consider:

- collection limitation;
- purpose specification;
- use limitation;
- data quality
- security safeguards;
- openness
- individual participation;
- accountability.

Privacy concerns individual choices of human beings, it is thus important to allow each individual to determine and

Figure 1: Relationship among the identified dimensions.

modify her privacy preferences freely. In general, those preferences are defined in "privacy policies" (PP). Inspired form P3P [9], we consider that PPs should consider *authorized users*, allowed *operations*, *access purposes*, *access conditions*, *retention time*, *obligations* and the *minimal trust level* necessary to allow data access.

Efforts are being realized to offer solutions to personal distributed data privacy. In [1], authors propose a privacy-enhanced social networking site oriented to satisfy privacy awareness and customization, data minimization and data sovereignty. PriServ [12], is a privacy service for P2P systems that proposes functions to publish and request private data by taking into account the PPs of data owners (in particular, access purpose, operations and authorized users). Hello World [14], is a distributed social network that focus on authentication, decentralization and security. Their objective is to give the control of their data to data owners by letting them to manage their data privacy. [10] proposes a social networking based on P2P systems. It uses and propose techniques to trust users in the system, anonymization of traffic, pseudonyms, *etc.* to offer privacy protection to users.

3. CONCEPT INTERACTIONS

Interactions and dependencies of the three concepts that we are concerned on, can be taken from different points of view. This paper analyzes a first point of view which surely may evolve.

We consider that different levels of users' satisfaction, reputation and privacy have direct repercussion on the trust towards the system. Figure 1 shows some links among those concepts. The center box corresponds to the trust towards the system as it is a main issue. We consider that each user of the system can have her own perception of the level of trust she can have in the system. But also, the system can be considered globally as trusted or not.

The satisfaction notion depends on the objectives/intentions/motivations of each user when using the system. Then, a user can have a satisfaction perception that can be influenced only by its local vision of the system, or by a global one. The global vision means that each user can perceive the interaction of other users in the system even if she is not concerned.

Reputation is constructed from the interaction and feedback of users. The reputation system is supposed to calculate individually the trustworthy level of users and the set of those levels may indicate the trustworthy of the global system.

Privacy concerns the respect of individual PPs. A system may in general respect the user' privacy but eventually some users may be unhappy because they consider that their personal privacy is not respected[2]. Guaranteeing PPs' respect has an important influence on the system. Reputation and satisfaction mechanisms may need more or less private information to work efficiently.
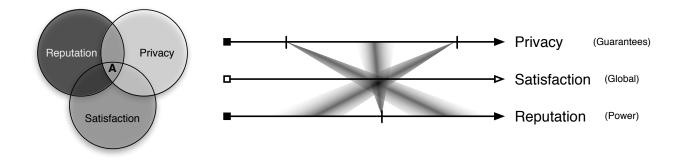
Interactions among these three concepts can be complementary or antagonistic, for instance:

- the more a user trusts towards the system, the more she is satisfied, and the more she is satisfied, the more she trusts towards the system.

- In the same way, the more the reputation mechanism is efficient, the more users trust towards the system, and the more a user trusts towards the system, the more she contributes honestly to the reputation mechanism.

- Similarly, the more the reputation mechanism is efficient, the more users are satisfied, and the more a user is satisfied, the more the reputation mechanism will be efficient.

- It is possible that the reputation mechanism be efficient and concludes that the majority of users are untrustworthy. In this case, users will not trust the system even if they continue to contribute to the reputation mechanism.

- Concerning privacy, the more information is gathered, the more the reputation mechanism is efficient. And the less a user trusts towards the system, the less she discloses information. Finally, the more a user's privacy is respected, the more this user is satisfied and inversely.

4. OBJECTIVES

The first issue we are working on is identifying the common, but also the incompatible, properties of the three considered dimensions (*cf.* left side of Figure 2). Clearly, privacy and reputation are closely related by the quantity/type of shared information. Concerning satisfaction and privacy, one link is the privacy respect which depends on, for instance, the respect of user's PPs. The relationship between reputation and satisfaction can be for instance the efficiency of reputation mechanism. Thus, different levels of privacy and reputation guarantees may lead to different levels of satisfaction. Therefore, reaching a point located in the intersection area of all these dimensions (*i.e.*, Area A in the figure) represents a good tradeoff to attend a high level of trust towards the system.

---

[2]Privacy breaks can be due to specific malicious users or to the system itself. They should not be treated in the same manner and should not imply the same consequences.

Figure 2: Spatial representation of our 3-facet characterization and mutual impact of the two main settable aspects on global satisfaction.

In addition, our main objective is to define a generic metric that takes into account all these dimensions and helps the designer to maximize the users' trust towards the system while respecting the system/application constrains.

The right side of Figure 2 illustrates the mutual impact of privacy, reputation and satisfaction in the following terms.

- **Privacy.** It represents the satisfaction in terms of privacy guarantees which can be the amount of information that it is *not* necessary to share within the system or the respect of PPs.

- **Reputation.** It represents the satisfaction of the reputation mechanism in terms of power as reliability, efficiency and most of all, consistency with the reality.

- **Satisfaction.** In this context, it represents the global users' satisfaction according to the first two axes.

The figure shows that the less the amount of shared information is, the most the privacy satisfaction is. However, that implies a low reputation satisfaction range. Obviously, both dimensions have an antinomic impact. Nevertheless, we can infer that the same global satisfaction can be reached by using different settings, which depend on the applicative context requirements.

Finally, the main aim of our study is to find a method to obtain the right settings in order to maximize the user' trust towards the system. The latter could be reach by finding the best tradeoff between all the proposed dimensions that leads to the point located as far as possible on the right of the satisfaction axis.

5. CONCLUSION AND OPEN ISSUES

Social networks actually take an important place in our everyday life. However, most of social systems do not take into account user's trust as an aim. In our works, we propose to increase the users' trust towards the system by designing some methods to raise the aforementioned aim in terms of reputation, privacy and satisfaction. In our opinion, these three dimensions are hardly linked and have to be studied in a correlated way.

Nevertheless, it is obvious that user's trust is not only linked to reputation, satisfaction and privacy, but our work consists in a first step and we have make the choice to start with this focus. Moreover, each of these dimensions has to be handled more generally than the preliminary examples presented in this position paper (quantity of shared information, efficiency of reputation system, and so forth).

There is numerous open questions, for example, to identify the common and the incompatible properties of the three dimensions, but also, to define generic metrics that takes into account these dimensions and helps the designer to maximize the users' trust towards the system while respecting the system and/or application constrains.

6. REFERENCES

[1] Esma Aimeur, Sebastien Gambs, and Ai Ho. Towards a Privacy-Enhanced Social Networking Site. *Conference on Availability, Reliability and Security*, 0:172–179, 2010.

[2] Elli Androulaki, Seung Geol Choi, Steven M. Bellovin, and Tal Malkin. Reputation systems for anonymous networks. In *the 8th international symposium on Privacy Enhancing Technologies (PETS '08)*, pages 202–218, Berlin, Heidelberg, 2008. Springer-Verlag.

[3] Mohamed Bakhouya and Jaafar Gaber. A Query Routing Approach Based on Users' Satisfaction for Resource Discovery in Service-Oriented Networks. *Conference on World Wide Web (WWW)*, 13(1-2):61–73, 2010.

[4] John Bethencourt, Elaine Shi, and Dawn Song. Signatures of Reputation: Towards Trust Without Identity. In *14th International Conference on Financial Cryptography and Data Security (FC '10)*, Tenerife, Canary Islands, Spain, January 2010.

[5] Dania Bilal. Children's use of the yahooligans! web search engine: Ii. cognitive and physical behaviors on research tasks. *JASIST*, 52(2):118–136, 2001.

[6] Sonja Buchegger, Doris Schiöberg, Le Hung Vu, and Anwitaman Datta. PeerSoN: P2P Social Networking - Early Experiences and Insights. In *ACM Workshop on Social Network Systems Social Network Systems, co-located with Eurosys*, Nürnberg, Germany, March 2009.

[7] Xiaowei Chen, Kaiyong Zhao, and Xiaowen Chu. Seprep: A novel reputation evaluation model in peer-to-peer networks. In *ATC '08: Proceedings of the 5th international conference on Autonomic and Trusted Computing*, pages 86–99, Berlin, Heidelberg, 2008. Springer-Verlag.

[8] Cyril W. Cleverdon. The significance of the cranfield tests on index languages. In Abraham Bookstein, Yves Chiaramella, Gerard Salton, and Vijay V. Raghavan, editors, *SIGIR*, pages 3–12. ACM, 1991.

[9] Lorrie Cranor, Marc Langheinrich, Massimo Marchiori, Martin Presler-Marshall, and Joseph Reagle. The Platform for Privacy Preferences 1.0. (P3P 1.0) Specification. W3C Recommendation, April 2002.

[10] Leudo Antonio Cutillo, Refik Molva, and Thorsten Strufe. Privacy Preserving Social Networking Through Decentralization. In *Conference on Wireless On-Demand Network Systems and Services (WONS)*, pages 133–140, Piscataway, NJ, USA, 2009. IEEE Press.

[11] Bernard J. Jansen and Udo W. Pooch. A review of web searching studies and a framework for future research. *JASIST*, 52(3):235–246, 2001.

[12] Mohamed Jawad, Patricia Serrano-Alvarado, Patrick Valduriez, and Stéphane Drapeau. A Data Privacy Service for Structured P2P Systems. In *Mexican International Conference on Computer Science (ENC09)*, Mexico, D.F. Mexico, 09 2009.

[13] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. The Eigentrust algorithm for reputation management in P2P networks. In *Conference on World Wide Web (WWW)*, pages 640–651, New York, NY, USA, 2003. ACM.

[14] Benjamin Ludwig Markus Ackermann, Krister Hymon and Kai Wilhelm. HelloWorld: An Open Source, Distributed and Secure Social Network. In *W3C Workshop on the Future of Social Networking, Position Papers*, Barcelona, January 2009.

[15] Sergio Marti and Hector Garcia-Molina. Taxonomy of Trust: Categorizing P2P Reputation Systems. *Computer Networks*, 50(4):472–484, 2006.

[16] OECD. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data: `http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00%.html`, 1980.

[17] Jorge-Arnulfo Quiané-Ruiz, Philippe Lamarre, and Patrick Valduriez. A Self-Adaptable Query Allocation Framework for Distributed Information Systems. *The VLDB Journal*, 18(3):649–674, 2009.

[18] Marco Remondino and Guido Boella. How users' participation affects reputation management systems: The case of p2p networks. *Simulation Modelling Practice and Theory*, In Press, Corrected Proof, 2010.

[19] Mark Sanderson and Justin Zobel. Information retrieval system evaluation: effort, sensitivity, and reliability. In Ricardo A. Baeza-Yates, Nivio Ziviani, Gary Marchionini, Alistair Moffat, and John Tait, editors, *SIGIR*, pages 162–169. ACM, 2005.

[20] Aameek Singh and Ling Liu. TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems. In *Conference on Peer-to-Peer Computing (P2P)*, page 142, Washington, DC, USA, 2003. IEEE Computer Society.

[21] Tribler. Tribler: A Fully Distributed File-Sharing System. `http://www.tribler.org/`.

[22] Ellen M. Voorhees. Evaluation by highly relevant documents. In W. Bruce Croft, David J. Harper, Donald H. Kraft, and Justin Zobel, editors, *SIGIR*, pages 74–82. ACM, 2001.

[23] Alan F. Westin. *Privacy and Freedom*. Atheneum, New York, 1967.

[24] Runfang Zhou and Kai Hwang. PowerTrust: A Robust and Scalable Reputation System for Trusted Peer-to-Peer Computing. *IEEE Transactions on Parallel and Distributed Systems*, 18(4):460–473, 2007.