Trust evaluation of websites: a comprehensive study

Article *in* International Journal of Advanced Intelligence Paradigms · January 2019

DOI: 10.1504/IJAIP.2019.10021413

2 authors:

Himani Bansal
Jaypee Institute of Information Technology
14 PUBLICATIONS **70** CITATIONS
SEE PROFILE

Shruti Kohli
8 PUBLICATIONS **14** CITATIONS
SEE PROFILE

Trust evaluation of websites: a comprehensive study

Himani Bansal*

Jaypee Institute of Information Technology,
Noida, Uttar Pradesh 201309, India
Email: singal.himani@gmail.com
*Corresponding author

Shruti Kohli

DWP Digital,
London, UK
Email: kohli.shruti@gmail.com

Abstract: People rely heavily on internet to fulfil even the minuscule of their need. According to a survey, 41% of time spent on web is for finding some information from search engines or reading some information. This is majorly due to easily accessible, cost effective and perceived high value information. But, this perceived high value information can prove fatal, if consumed without any authoritarian checks; especially if related to issues like health. Some template is necessitated to measure trustworthiness of such information. This paper explores a novel approach to quantify trust in such information-led websites. Analytical data is collected for various informational websites using *similarweb.com* and trust is modelled for these websites using human behaviour as an aggregate. Analytical data is believed to capture actual behaviour of each and every visitor visiting the website for information; thus making the study reliable and dependable. Results have been compared with some other acceptable studies and have found to be encouraging.

Keywords: content trust; health information; medical trust; online interaction; user satisfaction; web trust.

Reference to this paper should be made as follows: Bansal, H. and Kohli, S. (2019) 'Trust evaluation of websites: a comprehensive study', *Int. J. Advanced Intelligence Paradigms*, Vol. 13, Nos. 1/2, pp.101–112.

Biographical notes: Himani Bansal is ardently captivated by the world of big data, cloud computing and web analytics. She has more than two years of corporate experience, thus having hands on experience of live projects. Due to zealous inclination towards academics, she then moved to pursue her doctorate from BIT, Mesra, India. She has many national and international publications in the area of cloud computing and web analytics. She has been a remote centre coordinator for various workshops conducted by IIT Bombay and has qualified UGC NET. Her academics have been augmented by her research findings in various conferences, including IEEE, ACM and International Workshop of Machine Learning and Text Analytics held in South Asian University, New Delhi and in esteemed journals from Bentham Science and Elsevier.

Shruti Kohli interest area includes information retrieval, operational research, data mining and web analytics. She is totally fascinated by the variety of user behaviour patterns over net and has keen interest in web analytics and Big Data. She has sound publications in national and international journals. She also worked as web consultant and has supported industrial web analytic projects. Recently, she has been selected as a volunteer expert by Digital Analytics Association (DAA) for digital analytics competency development project (validation phase). She is an active member of IEEE, ACM, IAENG, DAA, INFORMS and is currently guiding PhD scholars.

1 Introduction

One of the major components of human interaction is trust. There are many definitions of trust in the literature. It is defined as "firm belief in the reliability, truth or ability of someone or something" or as an "acceptance of the truth of a statement without evidence or investigation" and "the state of being responsible for someone and something" (Oxford Dictionaries, 2015). One of the other definitions is that trust is a measure of confidence that an entity will behave in expected manner, despite the lack of ability to monitor or control the environment in which it operates (Singh and Bawa, 2007). Psychological definition of trust says that the trust is psychological state of the individual where he risks being vulnerable to the trustee based on the positive expectations of the trustee's intentions or behaviour (Rousseau et al., 1998). In sociology, trust is defined as a 'bet' about the future contingent actions of the trustee (Demouchel, 2005). Finally, there is trust categorised in computer science or computer applications in two ways:

1 trust with the user: it is a prejudiced analysis of one's behaviour and giving some future predictions about him/her by another (Mui, 2003)

2 trust with the system: it is the anticipation or the probability about the system or the device about its stanch behaviour to abide by the purpose for which it is proposed.

1.1 Facets and types of trust

Trust includes three dimensions: trust originator, trust purpose and trust target (Mu and Yuan, 2010). "Trust is related to trust purpose. For example, an employee is trusted to deal with financial affairs below a certain amount by a company, but is possibly not trusted to be a spokesman" (Mu and Yuan, 2010). If X has trust on Y, there is a trust relationship between X and Y. In literature, trust is generally defined as direct, indirect and recommender trust (Mu and Yuan, 2010; Ou et al., 2009), where direct trust is when X has trust on Y for a certain purpose. When X has trust on Y which in turn provides trust on Z for a certain purpose, then Y is known as recommender and there is a recommender trust from X to Y and an indirect trust from X to Z.

Nepal et al. (2011) asserted that there are two main types of user trust in computer science: direct trust and recommendation trust, also referred to as peer-to-peer trust. Direct trust is measured on the basis of unswerving experience of the member, while recommendation trust is measured using the propagative properties of trust (Nepal et al., 2011).

1.2 Aspects of trust

Trust has many different aspects. When we talk about trust aspects, we consider a perspective from which we look at trust. This perspective often gives different semantics to the trust (Sherchan et al., 2013).

1 Calculative trust – It is calculated on the basis of member to capitalise on his stakes in the interaction (Tyler and Degoey, 1996). This aspect of trust can mainly be found in economics where the trust is described as a chance of gain to the chance of loss in ratio with the total probable loss to the total probable gain.

2 Relational trust – This aspect of trust is a result of recurring communications amid the member and trustee. In computer science, this is known as direct trust: "trust based on direct interactions between two parties" (Rousseau et al., 1998).

3 Emotional trust – It is defined as the refuge or console in relying on somebody (Kuan and Bock, 2005). In psychology, it is the result of undeviating interpersonal relationships between member and a trustee.

4 Institutional trust – It is defined as an outcome of an "institution providing environment that encourages cooperation between members and penalizes misbehaviours. Such supports can exist at organizational level and societal level as legal systems that protect individual rights and property" (Lewis and Weigert, 1985).

5 Dispositional trust – "Dispositional aspect of trust recognizes that, over the course of their lives, people develop generalized expectations about the trustworthiness of other people" (Rotter, 1967).

1.3 Properties of trust

Trust can have different properties. It can vary with time or be subjective. Properties of the trust have great influence in determining what kind of trust is being researched and modelled. Most important trust properties are (Sherchan et al., 2013):

1 Context specific – Trust can be context specific. If person X trusts person Y as his health advisor, he will not trust him as his accountant to keep records of his accounts. This implies that person X is trustworthy towards person Y in the context of seeking any advice regarding his/her health, but not in the context of sharing his account details.

2 Dynamic – "Trust can increase or decrease with time and new experiences, interactions or observations" (Staab et al., 2005). New interactions or observations are essential in comparison to previous ones, since they tend to get extraneous with time.

3 Propagative – This is a very important property of trust and it is explored in many works. It can be described with an example that if a person A trusts person B and person B trusts person C, then A, who does not know C, can derive some amount of trust on C based on how much she trusts B and how much B trusts C. Because trust is usually propagative, its information can be passed from one member to another in social network, creating trust chains. It is similar as the 'word of mouth' propagation of information for humans (Abdul-Rahman and Hailes, 2000).

4 Aggregative – While propagation of trust along social chain says that a person can form some trust on another person that is indirectly associated with it, it does not say how to behave when we have several chains of trust recommending different amount of trusts towards trustee. This information, from multiple chains, has to be composed to form final amount of trust (Golbeck, 2005).

5 Subjective – In general, trust can be subjective. If person A gives its opinion about someone, then trust computed from that opinion is subjective. "The subjective nature of trust leads to personalization of trust computation, where preferences of the member have a direct impact on the computed trust review" (Singal and Kohli, 2015a).

6 Asymmetric – Trust is characteristically asymmetric. "One member may trust another more than s/he is trusted back. Asymmetry occurs because of differences in people perceptions, opinions and beliefs" (Singal and Kohli, 2015a).

7 Self-reinforcing – Trust is also usually self-reinforcing. "Members usually act positively with other members whom they trust. Also, if the trust is really low between members it is highly unlikely that they will interact with each other, leading to even less trust on each other" (Yu and Singh, 2002).

8 Event sensitive – Trust usually takes an extended and elongated approach with lots of time to erect, but a lone high-impact occurrence may devastate it entirely (Nepal et al., 2010). That means that trust has event sensitive nature.

1.4 Trust representation

When we talk about trust representation, we think about different approaches in grading members trust towards another member. These approaches can be divided into two main categories: probabilistic and gradual. Probabilistic approaches deal with a single trust value in black and white fashion and compute probability that the trustee can be trusted (Rici et al., 2011). On the other hand, gradual approaches estimate trust values to some extent, as opposed to being either right or wrong. In gradual approaches trust values are not interpreted as probabilities, but rather values where higher value corresponds to a higher trust in an agent. Differences in trust representation have higher effect in computation of trust by peer-to-peer algorithms where even the whole algorithms depend on trust representation.

1.5 Information sources

There are three main sources of trust information in social networks (Sherchan et al., 2013):

1 Attitudes – Attitudes represent "an individual's degree of like or dislike for something" (Golbeck, 2005). They are constructive or destructive views about some entity. Attitudes are derived from user's interactions.

2 Experiences – Experiences describe perception of the member in their interactions with each other. Experiences are often used as an information source in peer-to-peer networks while computing trust between nodes in the network. These experiences are usually peers ratings of quality of interactions with other peers.

3 Behaviours – Behaviours are identified by patterns of interactions and its main information source is interaction. It can depend on type of interaction, frequency of interaction, or change of interaction. All these behaviours can be used to determine and compute trust between members in network.

1.6 Trust evaluation models

There are different ways of computing trust among members of a network in existing work. They can be categorised in three groups: network-based trust models, interaction-based trust models and hybrid trust models.

1 Network structure trust models – In this trust evaluation model, a trust network is formed for every member. With this model, members are represented as nodes in the graph, and trusts among members are represented as directed edges. A variety of algorithms are then applied to establish trust among any two nodes in the network. These algorithms use propagative nature of trust. One example of network-based trust model is tidal trust where trust is derived between two people in social network who are not directly connected.

2 Interaction-based trust models – Some models solely utilise the intra-network interactions to model and compute social trust. In these models, we can distinguish two types of trust: popularity trust and engagement trust. "Popularity trust refers to the acceptance and approval of a member in the community, representing the trustworthiness of the member from the perspective of other members in the community. Engagement trust refers to the involvement of the member in the community, representing the trust the member has towards the community. Combination of popularity trust and engagement trust forms the basis for determining the social trust in the community" (Nepal et al., 2010).

3 Hybrid trust models – These models encourages graph structures as well as intra-network interactions to measure social trust within a social network so that advantages of previous trust models can be exploited to the fullest.

2 Background of our work

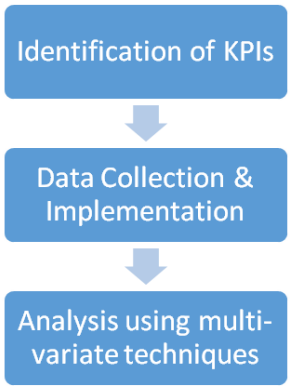
Whenever a query is fired on search engines in form of a search string, a list of uniform resource locators (URLs) appear according to the search engine optimisation applied by website owners, page rank, popularity index, page age etc. User or requestor of the information then applies self-decision based on experience, knowledge and perceptions to which information should be used as there is no other measure to check the trustworthiness of the information. Here, trust plays a major role play. This self-decision applied by the user can be exploited to standardise a mechanism which can help in quantifying trust. But, the major issue lies in capturing this human behaviour into quantifiable units. Here, web analytical tools play a major role. Analytical tools collect superfluous amount of data from websites using page tagging, web beacons, and/or log files. In current scenario of analytics revolution, the collected data is considered to be as precise as possible. Authors have tried to exploit this precise analytical data to quantify

trust value possessed or inherited by websites in the best possible manner using scientific research methodology.

3 Methodology

As depicted in Figure 1, a three-step methodology was followed to carry out our objective of efficiently categorising websites according to the trust quotient they possess. Initially, a survey was carried out among internet users to call in most appropriate key performance indicators (KPIs) from analytical data which can be used as precursors of trust in informational websites (Kohli and Singal, 2015). These precursors were also tested for complimentary relation with distrust possessed by these websites through the survey (Singal and Kohli, 2015a, 2015b). The precursors leading to KPIs were: average daily visits, bounce rate, pages per visit and average time on website.

Figure 1 Research methodology (see online version for colours)



The data was collected for identified KPIs from Similarweb Ltd. (Similarweb, 2014) which uses latest big data technologies to collect analytical data at the global level.

4 Implementation

Multiple discriminant analysis (MDA) technique was used to analyse the data, as it is best suitable technique for the data gathered, since all the web metrics gathered are metric whereas trust is non-metric in nature. In MDA, a variate is formed so as to create scores for each observation that maximally differentiates between groups of observations. On the basis of nature of variate, MDA can further be of two types:

a linear discriminant analysis (LDA)

b quadratic discriminant analysis (QDA).

Both LDA and QDA were applied on data to corroborate the results to maximum accuracy. The results obtained are discussed in next session.

5 Results

To strengthen the acceptability of the methodology, top health related search queries were used to compare the results. The shortlisted queries were the most searched health queries on WebMD and Medscapes (Ashley, 2015) and Google Search Engine (Mulpeter, 2015) in year 2015.

Data was collected from Similarweb for complete one year, i.e. from January, 2015 to December, 2015. Data was then cleaned; normalised and analysed using MDA techniques using open-source statistical software R. Table 1 enlists the classification matrix and misclassification error of each case. Three classes of trust were used: 1 (most trustworthy), 2 (somewhat trustworthy) and 3 (least trustworthy).

Table 1 Results for top health search queries of year 2015

S. no.	*Search query*	*Classification matrix obtained as result of LDA*				*Classification matrix obtained as result of QDA*			
1	Is bronchitis contagious?		1	2	3		1	2	3
		1	13	0	2	1	18	0	0
		2	0	2	1	2	0	4	1
		3	8	4	21	3	3	2	23
		Misclassification error: 29.41%				Misclassification error: 11.76%			
2	Physician burnout		1	2	3		1	2	3
		1	9	1	1	1	15	0	2
		2	0	1	1	2	1	2	0
		3	9	6	25	3	2	6	25
		Misclassification error: 33.96%				Misclassification error: 20.75%			
3	How many calories should I eat?		1	2	3		1	2	3
		1	20	6	10	1	12	0	0
		2	0	0	0	2	6	8	3
		3	6	4	10	3	8	2	17
		Misclassification error: 46.42%				Misclassification error: 33.92%			
4	Lewy body dementia		1	2	3		1	2	3
		1	28	5	16	1	24	0	0
		2	1	2	0	2	2	4	2
		3	0	0	2	3	3	3	16
		Misclassification error: 40.74%				Misclassification error: 18.51%			
5	How far along am I?		1	2	3		1	2	3
		1	5	0	1	1	6	0	2
		2	1	7	3	2	3	8	5
		3	5	1	26	3	2	0	23
		Misclassification error: 22.44%				Misclassification error: 24.48%			

Table 1 Results for top health search queries of year 2015 (continued)

S. no.	*Search query*	*Classification matrix obtained as result of LDA*				*Classification matrix obtained as result of QDA*			
6	Flu and flu vaccine		1	2	3		1	2	3
		1	31	6	11	1	30	0	0
		2	2	2	0	2	3	7	0
		3	0	0	7	3	0	1	8
		Misclassification error: 32.20%				Misclassification error: 6.77%			
7	How long does the flu last?		1	2	3		1	2	3
		1	13	0	2	1	18	0	0
		2	0	2	1	2	0	4	1
		3	8	4	21	3	3	2	23
		Misclassification error: 29.41%				Misclassification error: 11.76%			
8	What is gluten?		1	2	3		1	2	3
		1	13	0	2	1	18	0	0
		2	0	2	1	2	0	4	1
		3	8	4	21	3	3	2	23
		Misclassification error: 29.41%				Misclassification error: 11.76%			
9	HIV		1	2	3		1	2	3
		1	25	10	12	1	16	0	0
		2	0	0	0	2	8	7	1
		3	1	1	6	3	2	4	17
		Misclassification error: 43.63%				Misclassification error: 27.27%			
10	What is lupus?		1	2	3	Grouping too small for analysis			
		1	26	4	9				
		2	0	0	0				
		3	0	0	10				
		Misclassification error: 26.53%							
11	Mammograms		1	2	3		1	2	3
		1	35	8	9	1	14	0	0
		2	0	0	0	2	11	5	2
		3	2	0	3	3	12	3	10
		Misclassification error: 33.33%				Misclassification error: 49.12%			
12	Measles		1	2	3		1	2	3
		1	30	2	6	1	28	0	0
		2	0	0	0	2	0	5	1
		3	3	3	9	3	5	0	14
		Misclassification error: 26.41%				Misclassification error: 11.32%			

Table 1 Results for top health search queries of year 2015 (continued)

S. no.	*Search query*	*Classification matrix obtained as result of LDA*				*Classification matrix obtained as result of QDA*			
13	When do you ovulate?		1	2	3		1	2	3
		1	32	5	11	1	18	0	1
		2	0	0	0	2	2	5	1
		3	0	2	7	3	12	2	16
		Misclassification error: 31.57%				Misclassification error: 31.57%			
14	Is pneumonia contagious?		1	2	3		1	2	3
		1	30	2	6	1	28	0	0
		2	0	0	0	2	0	5	1
		3	3	3	9	3	5	0	14
		Misclassification error: 26.41%				Misclassification error: 11.32%			
15	Transgender and gender identity		1	2	3		1	2	3
		1	30	2	6	1	28	0	0
		2	0	0	0	2	0	5	1
		3	3	3	9	3	5	0	14
		Misclassification error: 26.41%				Misclassification error: 11.32%			
16	How much water should I drink?		1	2	3		1	2	3
		1	30	2	6	1	28	0	0
		2	0	0	0	2	0	5	1
		3	3	3	9	3	5	0	14
		Misclassification error: 26.41%				Misclassification error: 11.32%			

The results confirm the fulfilment of aim of finding a classification criteria which helps in annotating the websites according to their levels of trust. Though QDA yields more appropriate results, LDA can be preferred for lower complexity and comparable accuracy for most trustworthy websites (marked with 1).

6 Existing work and comparison

This same experiment was run using two existing tools:

1 web of trust (WOT)

2 WebCast

6.1 Web of trust

WOT is an outstanding website reputation rating tool that helps in making informed decisions about whether to trust a website or not when we are searching, shopping or browsing online. WOT extension shows website reputations as traffic lights next to search results when we use Google, Yahoo! Bing or any other search engine: green for good, red for bad, and yellow as a warning to be cautious. By clicking the traffic light

icon you can find out more about a website's reputation, safety information and users' opinions. A green traffic light means users have rated the site as trusted and reliable, red warns about potential online threats and yellow indicates that you need to be cautious when using a site (Web of Trust, 2015).

> "WOT stands for the personal online security and web safety. Web of Trust is based on the crowd sourcing approach. Millions of users rate websites throughout the Internet and share their personal experience. This helps in avoiding online threats that only real life experience can detect, such as scams, untrustworthy links, and rogue web stores." (Web of Trust, 2015)

> "Web of Trust (WOT) has been featured in the New York Times, CNET, PC World, Kim Komando show, Tech Republic, PC Welt and many other popular media. WOT ratings and reviews are powered by a global community of millions of users who rate websites based on their personal experiences. In addition, trusted third-party sources are used to warn the users about malicious software and other online threats that they might encounter." (Web of Trust, 2015)

6.2 WebCAST

> "Web Credibility Assessment Support Tool (WebCAST) considers multiple factors (type of website, popularity, sentiment, date of last update, reputation and review based on users' ratings reflecting personal experience) for assessing the credibility of information and returns a summary indication of the credibility of a website. It uses Potentially All Pairwise RanKings of all possible Alternatives (PAPRIKA) method of Multi-Criteria Decision Analysis (MCDA) to give weights to the scale values on each factor, representing the relative importance of the attributes. An empirical evaluation of the tool was conducted by computing the correlation between the tool-generated credibility scores and that of human judges. The correlation was found to be 0.89, thus verifying the validity of the tool." (Aggarwal et al., 2014)

6.3 Comparison

Statistical analysis was performed to compute the correlation between the QDA generated rankings and those generated from WOT and WebCAST. We achieved a positive correlation with both the tools having values 0.87 and 0.71 respectively. The results are encouraging and illustrate this methodology of evaluating trust as acceptable.

7 Discussion and conclusions

Trust is an impending factor for relationships to thrive. Detailed literature analysis had revealed that different trust policies use different features for trust calculation, and since all websites are different, there is no common approach to calculate trust. The mechanism proposed can act as standard trust policy at least domain-wise, thus can be easily coupled with search engines. It is also simple and easy to implement by search engines as all the required data is readily available with them, thus having no limitations to be faced. In nutshell, it can act as a standard trusted platform model (TPM) which can be compliance at least with domain-specific content-driven websites.

The data used in this research work is primary in nature and has been outsourced from Similarweb Ltd (2014).

> "Similarweb is a global company that doesn't rely on any single channel for data collection. They work with a wide variety of sources to create the most accurate and reliable picture of the digital world. All of this data is fed into Similarweb's data processing servers where they turn billions of daily data points into insightful information. Data comes from 4 main sources: 1) A panel of monitored devices, currently the largest in the industry. 2) Local internet service providers (ISPs) located in many different countries. 3) Our web crawlers that scan every public website to create a highly accurate map of the digital world, and 4) Hundreds of thousands of direct measurement sources from websites and apps that are connected with us directly. This last source of data helps to constantly improve the learning set, fine tune the algorithms and reach accurate estimations about traffic stats for all websites. SimilarWeb spent several years building the data collection infrastructure and refining the data collection processes before launching. They are confident that they offer the most accurate and unbiased data covering the digital world." (Similarweb, 2014)

The required data is not available to such extent, for personal or commercial use with any other vendor. Sincere efforts have been made to extend the work as much as possible.

References

Abdul-Rahman, A. and Hailes, S. (2000) 'Supporting trust in virtual communities', *Proceedings of the 33rd Hawaii International Conference on System Sciences*, IEEE Computer Society, pp.1–9.

Aggarwal, S., Oostendorp, H.V., Reddy, Y.R.B. and Indurkhya, B. (2014) 'Providing web credibility assessment support', *European Conference on Cognitive Ergonomics ECCE'14*.

Ashley, W. (2015) *Top Health Searches of 2015* [online] http://www.cbsnews.com/media/top-health-news-searches-of-2015/ (accessed 8 July 2016).

Demouchel, P. (2005) 'Trust as an action', *European Journal of Sociology*, Vol. 46, No. 1, pp.417–428.

Golbeck, J.A. (2005) *Computing and Applying Trust in Web Based Social Networks*, PhD Thesis, University of Maryland at College Park, MD.

Kohli, S. and Singal, H. (2015) 'A methodological approach for quantizing trust from human behavior for content-driven websites', *International Journal of Sensors, Wireless communications and Control (IJSWCC)*, SI: Cyber Security, Privacy and Forensics for Complex Systems, Vol. 5, No. 1, pp.32–46, Bentham Science Publishers, ISSN: 2210-328.

Kuan, H. and Bock, G. (2005) 'The collective reality of trust: an investigation of social relations and networks on trust in multi-channel retailers', *Proceedings of the 13th European Conference on Information Systems*.

Lewis, J.D. and Weigert, A. (1985) 'Trust as a social reality', *Social Forces*, Vol. 63, No. 4, pp.967–985.

Mu, B. and Yuan, S. (2010) 'A method for evaluating initial trust value of direct trust and recommender trust', *IEEE International Conference on Computer Design and Applications*, pp.185–190.

Mui, L. (2003) *Computational Models of Trust and Reputation: Agents, Evolutionary Games, and Social Networks*, PhD Thesis.

Mulpeter, K. (2015) *9 Burning Health Questions People Asked Google This Year* [online] http://news.health.com/2015/12/04/top-health-searches-google-2015/ (accessed 9 July 2016).

Nepal, S., Sherchan, W. and Paris, C. (2011) 'STrust: a trust model for social networks', *Proceedings of the 10th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp.841–846.

Nepal, S., Zic, J., Lisu, D. and Jang, J. (2010) 'Trusted computing platform in your pocket', *Proceedings of the IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, IEEE Computer Society, Los Alamitos, pp.967–985.

Ou, W., Wang, X., Han, W. and Wang, Y. (2009) 'Research on trust evaluation model based on TPM', *IEEE International Conference on Frontier of Computer Science and Technology*.

Oxford Dictionaries (2015) Electronic References [online] http://oxforddictionaries.com/ (accessed 19 July 2016).

Rici, F., Rokach, L., Shapira, B. and Kantor, P.B. (2011) *Trust and Recommendations. Recommender Systems Handbook*, pp.645–675, Springer, London, ISBN 978-0-387-85820-3.

Rotter, J.B. (1967) 'A new scale for the measurement of interpersonal trust', *International Journal of Personality*, Vol. 35, No. 4, pp.651–665.

Rousseau, D.M., Sitkin, S.B., Burt, R.S. and Camerrer, C. (1998) 'Not so different after all: a cross-discipline view of trust', *Academy Management Review*, Vol. 23, No. 3, pp.393–404.

Sherchan, W., Nepal, S. and Paris, C. (2013) 'A survey of trust in social networks', *ACM Computing Survey*, Vol. 45, No. 4, Article 47.

Similarweb (2014) [online] http://www.similarweb.com/.

Singal, H. and Kohli, S. (2015a) 'Escalation of trust analysis in web', *12th ACM International Conference on Computing Frontiers*.

Singal, H. and Kohli, S. (2015b) 'Trust and distrust in websites: two sides of a same coin or poles apart?', *Proceedings of Springer CSI Digital Life*.

Singh, S. and Bawa, S. (2007) 'Privacy, trust and policy based authorization framework for services in distributed environments', *International Journal of Computer Science*, Vol. 2, No. 2, pp.85–92.

Staab, S., Hwang, K., Zhou, R. and Kwok, Y.K. (2005) 'Trusted p2p transactions with fuzzy reputation aggregation', *IEEE Internet Computing*, Vol. 4, No. 6, pp.24–34.

Tyler, T.R. and Degoey, P. (1996) 'Trust in organizational authorities: the influence of motive attributions on willingness to accept decisions', *Trust in Organizations: Frontiers of Theory and Research*, Sage Publications, Thousand Oaks.

Web of Trust (2015) [online] http://www.mywot.com (accessed 7 May 2016).

Yu, B. and Singh, M.P. (2002) 'An evidential model of distributed reputation management', *Proceedings of the 1st International Joint Conference on Autohomous Agents and Mulit-Agent Systems*, ACM Press, New York, pp.967–985.