"I Like" - Analysing Interactions within Social Networks to Assert the Trustworthiness of Users, Sources and Content

Owen Sacco and John G. Breslin
DERI, National University of Ireland, Galway
owen.sacco@deri.org and john.breslin@nuigalway.ie

***Abstract*—Online Social Network platforms provide users to create sensitive personal information such as user profiles that can be shared with other users within their social graph. Whilst these sites provide users with generic privacy settings to control who can be granted access, these platforms assume that all users in a social graph share the same level of trust. Moreover, these platforms also assume that what is shared within the Social Network can be trusted. Therefore, Social Networks do not take into consideration the notion of trust whilst users share or consume information. In this work, we conduct a user study to analyse the trends of interactions amongst users. We also analyse in detail the user's perception of trust whilst interacting within Social Networks. The results from this user study will help us understand how trust values can be asserted for users, sources and content by using information from within Social Networks.**

***Keywords*-Trust, Privacy, Social Web, Web of Data.**

I. Introduction

Social Networks have become one of the most used Web applications in our daily lives [4]. It enables users to be connected with one another that form a social graph and keep up to date with what their connected peers are up to. Through sharing of content, users discover news items or major events more rapidly in Social Networks than from the news sites themselves. Moreover, these platforms provide users to share personal information in the form of user profiles which they want others to know about. However, users become reluctant to share sensitive information as this might be misused by untrusted peers. Doubts also arise in the accuracy of the information shared by others.

Therefore, trust is a major concern in Social Networks since it is important in both directions: in one way it is important for users accessing content shared by others since users try to judge whether the information is factual or not. In the other direction, users want to know whether third party users can be trusted to access personal information such that they will not misuse the information.

A. Limitations of Current Social Networks

Social Networks provide privacy settings whereby users can set who can access specific parts of their profile information by selecting specific users or by selecting particular user groups. Although users can manually specify access settings for each particular person, this is time consuming and a laborious task for users to perform. Additionally, in some scenarios users will not know *a priori* who is going to access which information especially in public Social Networks where content can be accessed by anyone even by persons not in the user's social graph. Therefore, Social Networks assume that all connected users share the same amount of trust. These online Social Networks require ways how trust mechanisms are incorporated and enforced when users access personal information or content shared by others.

Content shared within these online platforms can contain any kind of information that might be factual or not. This information can be created by users within the Social Network or shared from external sources. Unfortunately, current online Social Networks do not provide any additional information that can help users decide which information to accept. It depends on the user's intuition whether to accept this information or not. Social Networks must provide additional information that would help users make decisions about which content to trust or not.

B. Factors Impacting Trust Judgements

Trust judgements depend on various social factors such as past experiences with other users, psychological factors based on past events and so forth [5]. It is difficult to implement an algorithm to compute trust judgements based on all of these social factors since Social Networks do not contain all the necessary information. Therefore, an analysis is required to understand what information can be extracted from Social Networks that can be used to compute trust.

Most current work on trust depend on the user assigning a trust value for another person [7] but most Social Networks do not provide this feature. Additionally, most users in Social Networks are connected to a large number of users and it is a tedious task for the user to assign a trust value for each connected peer. Moreover, trust changes over time and therefore this value has to be continuously updated to reflect the correct trust value.

Although one trusts a user, the user can be trusted for content on a particular topic and not on another which will not be reflected in the single trust value assigned to

This work is funded by the Science Foundation Ireland under grant number SFI/08/CE/I1380 (Líon 2) and by an IRCSET scholarship co-funded by Cisco systems.

978-0-7695-5137-1/13 $26.00 © 2013 IEEE
DOI 10.1109/SocialCom.2013.78

Table I
AGE OF PARTICIPANTS

Age Category	Participants
18 - 20	3%
21 - 29	45%
30 - 39	32%
40 - 49	13%
50 - 59	6%
60+	1%

this particular user. Furthermore, users not only carry out trust judgements about other users, but also perform trust judgements about content which is shared over these Social platforms. The relationship between the user sharing the content and the content itself might not exist and therefore, trust judgements for content has to be computed independently from the trust values asserted to users.

C. Summary of Results

This research paper presents in detail the results and analysis of a user survey which we have conducted to analyse how trust can be inferred from user interactions within Social Networks. We focus on the main user interactions provided by most Social Networks; which are the following: (1) sharing of content from external sources; (2) re-sharing or retweeting content; (3) "like" or "+1" or "favourite" of content; (4) comments or replies; and (5) tags or mentions within the Social Network. From this research, we can conclude that trust can be asserted for (1) the person sharing the content; (2) the person requesting the content; (3) the content; and (4) the source that created the content. The results from the user study also provide the usage trends of several user interactions within Social Networks.

The remainder of this paper is organised as follows: Section II provides the results from the user survey. Section III provides some insights based on the user study of how trust can be asserted from user interactions and from the information in Social Networks. Section IV provides some related work and section V concludes the paper.

II. USER STUDY

The user survey was an online survey and 178 participated in this study. The link to the online survey was shared in various Social Networks and whoever came across the link participated voluntarily.

The survey first asked for the participant's age, gender and occupation. The age of the participants is illustrated in table I and we observe that 77% of the participants are over 20 and under 40. Moreover, 65% of the participants were male and 35% were female. The occupations of the participants is illustrated in table II and some participants selected more than one occupation.

Table II
OCCUPATIONS OF PARTICIPANTS

Occupation Categories	Participants
Computer and Mathematics	59%
Education, Training & Library	26%
Business & Financial	13%
Management	8%
Architecture and Engineering	6%
Arts, Design, Entertainment, Sports & Media	5%
Life, Physical & Social Science	3%
Office & Administrative Support	2%
Healthcare Support	1%
Community & Social Service	1%
Sales	1%
Unemployed	1%

Table III
PARTICIPANT'S SOCIAL NETWORK ACCOUNTS

Social Networks	Participants
Facebook	88%
Google+	69%
Twitter	82%
LinkedIn	85%
None of the Above	1%

We based our survey on the most common used Social Networks that provide all the user interaction types mentioned in section I. These Social Networks are: Facebook, Google+, Twitter and LinkedIn. We then asked the users in which of these Social Networks they own an account. Table III shows the number of participants that have an account in these Social Networks.

We divided our survey in two parts: (1) Usage patterns and (2) User's trust perception in Social Networks.

The Usage patterns section analyses how often the users use each social user interaction and in which Social Network they use such user interactions. The participants had to choose one of the following options for each question and for each social network:

- No Account - represents that the participant does not have an account;
- Never - represents that the participant never uses this social user interaction;
- Occasionally - represents that the participant uses the social user interaction on a ***weekly*** basis; and
- Frequently - represents that the participant uses the social user interaction on a ***daily*** basis.

The User's trust perception in Social Networks section analyses what users trust when they use these social user interactions. We first asked the participant what trust means to him/her since the notion of trust can mean differently for each participant. The participant had to select one or more of the following options for this question:

1) When you share information with a person, that person will act according to your expectations.
2) When another person is sharing content with you, that person is reliable.

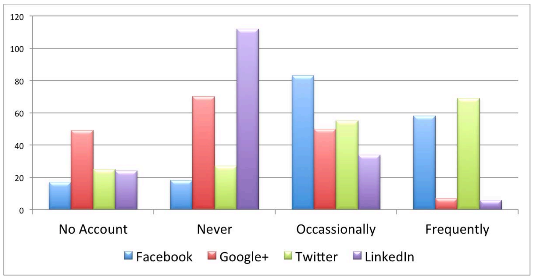

Figure 1. Participants frequency for sharing external content into each Social Network

3) The content being shared is true and of good value.
4) The source who created the content is reliable.

Subsequently, we then asked the participants what they trust when they use the social interactions in order to analyse the correlation between the social user interactions and what they trust. The participants had to select (one or more) from: (1) the person (with whom the user is interacting with), (2) the content and/or (3) the source.

The results for both sections are explained in detail in the following subsections.

A. Usage Patterns

The Usage patterns analyses the participants usage frequency of: (1) the share button from external Web sites; (2) the re-share or retweet button; (3) the like or +1 or favourite button; (4) the comment or reply button; and (5) the tag or mention features.

1) Sharing of content from external sources: Figure 1 illustrates the participants frequency for sharing external content into each Social Network. The results show that participants prefer to share content from external sources into Twitter and Facebook since 39% of the participants *frequently* share within Twitter and 33% within Facebook. 31% of the participants *occasionally* share external content into Twitter and 47% into Facebook. LinkedIn is the least used for sharing external content since 64% *never* share external content into LinkedIn. Google+ is also not popular for sharing since 40% *never* share content within Google+.

2) Re-sharing and retweeting content: Figure 2 illustrates the participants frequency for re-sharing or retweeting content within each Social Network. The results show that participants prefer to re-share or retweet from within Twitter since 38% of the participants *frequently* retweet within Twitter. Although only 16% *frequently* re-share in Facebook, 56% do re-share *occasionally* whilst in Twitter 34% *occasionally* retweet. LinkedIn is the least popular Social Network for re-sharing since 70% *never* re-share. Google+ is the second least preferred Social Network since 46% *never* re-share.

3) "Like", "+1" and "Favourite" button: We focused on analysing two usage patterns for the "Like", "+1" and "Favourite" button. The first is to analyse how often participants use these features and the second is for what or for whom do they use these features.

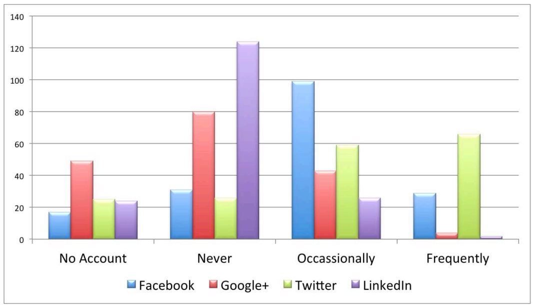

Figure 2. Participants frequency for re-sharing or retweeting content within each Social Network

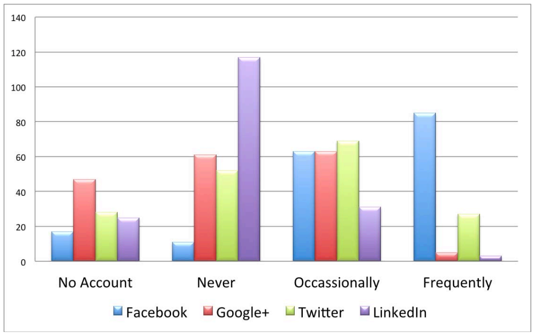

Figure 3. Participants frequency for using the like, +1 and favourite button within each Social Network

Figure 3 shows the participants frequency for using the "Like", +1 or "Favourite" button within each Social Network. The results show that the "Like" button in Facebook is the most *frequently* used since 48% of the participants use that functionality whereas only 13% *frequently* use the "Favourite" button in Twitter. However, 39% *occasionally* use the "Favourite" button in Twitter whereas 36% *occasionally* use the "Like" button in Facebook and the "+1" in Google+. LinkedIn is the least preferred Social Network for using the "Like" button since 66% never use this functionality.

Figure 4 shows what the participants use the "Like", "+1" and "Favourite" buttons for within each Social Network. In Facebook, comments, status updates, photos and external content are the most "liked". In the other Social Networks, the results show a similar trend whereby participants "Like", "+1" or "Favourite" more status updates, comments, external content and photos. Once again, LinkedIn is the least preferred Social platform for using the "Like" button.

4) Comments and replies: Figure 5 shows the participants frequency for comments and replies within each Social Network. The results show that commenting in Facebook and replying in Twitter are the most *frequently* used since

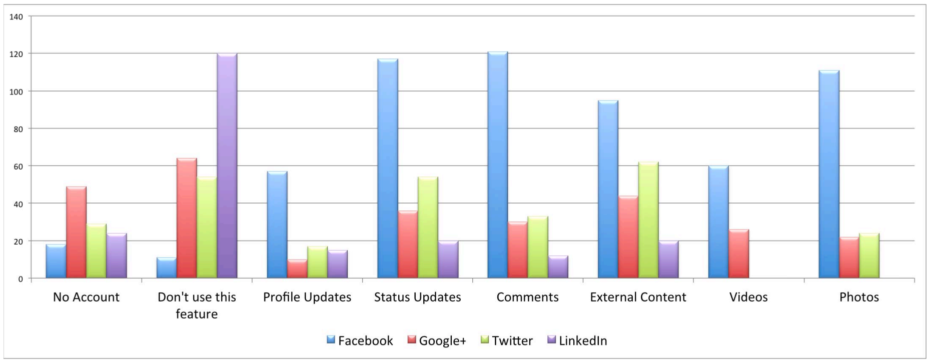

Figure 4. What participants click the like, +1 and favourite button for

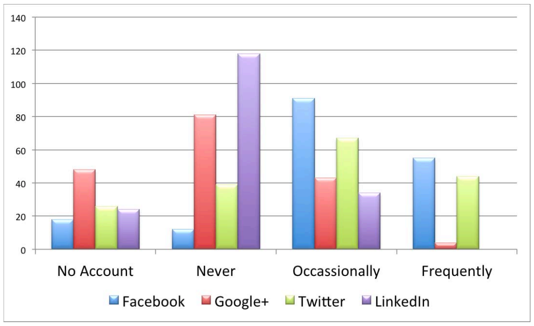

Figure 5. Participants frequency for commenting or replying within each Social Network

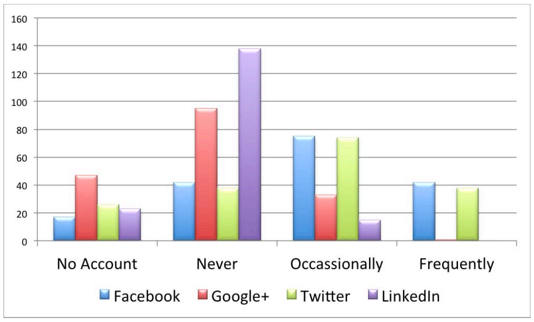

Figure 6. Participants frequency for tagging or mentioning other users within each Social Network

31% *frequently* comment in Facebook and 25% reply in Twitter. Moreover, 52% *occasionally* comment in Facebook and 38% reply in Twitter. Once again, LinkedIn is the least preferred Social Network for commenting since 67% participants *never* comment in LinkedIn. Moreover, in Google+ 46% *never* comment.

5) Tags and mentions: Figure 6 shows the participants frequency for tags and mentions within each Social Network. The results show that tagging and mentioning other users is the least of the user interaction types used. Only 24% *frequently* tag in Facebook; 21% *frequently* mention other users in Twitter and in Google+ only 1% *frequently* tag. Moreover, 42% *occasionally* tag users in Facebook, 42% *occasionally* mention users in Twitter and 19% *occasionally* tag users in Google+. Again, LinkedIn is the least preferred Social Network for tagging since 78% of the participants never tag. In twitter, 21% *never* mention users; in Facebook 24% *never* tag users; and in Google+ 54% *never* tag.

B. User's Trust Perception in Social Networks

The second part of the user survey analyses the participants perception of trust by first understanding what trust means for the participant. This is important in order to know *for what* and *for whom* we should be asserting trust. The study then examines the participants perception of trust judgements whilst using the social user interaction types within Facebook, Google+, Twitter and LinkedIn.

1) User's meaning of trust: Figure 7 shows the participants perception of trust. From the results it can be noted that 65% of the participants are more concerned with trusting the source. 57% of the participants perceive trust as trust in the content and trust in the belief that a person will act according to the user's expectations. Surprisingly, only 45% of the participants have selected that trust means a person is reliable if s/he shares content with the participant.

2) User's perception of trust whilst sharing external content: Table IV depicts the results of the participants perception of trust whilst sharing external content within each Social Network. The results show that participants trust the content most when they use the share button.

3) User's perception of trust whilst re-sharing or retweeting: Table IV shows that the participants also perceive trusting the content more whilst re-sharing or retweeting what other users have already shared.

4) User's perception of trust whilst using the "Like", "+1" or "Favorite" buttons: Table IV illustrates the results of the participants trust perception whilst using the "Like", "+1" and "Favourite" button within each Social Network. The results show that by using these features, participants trust the content and the person who is sharing the content.

Table IV
WHAT USERS TRUST WHILST INTERACTING WITHIN FACEBOOK, GOOGLE+, TWITTER AND LINKEDIN

Social User Interaction Types	The Other Person	The Content	The Source
Sharing external content	-	70%	55%
Re-sharing or Retweeting content	43%	70%	47%
Like, +1 or “Favourite” content	48%	58%	35%
Comment or Reply	56%	37%	24%
Tag or Mention other users	61%	44%	32%
Tagged or Mentioned by other users	55%	33%	27%

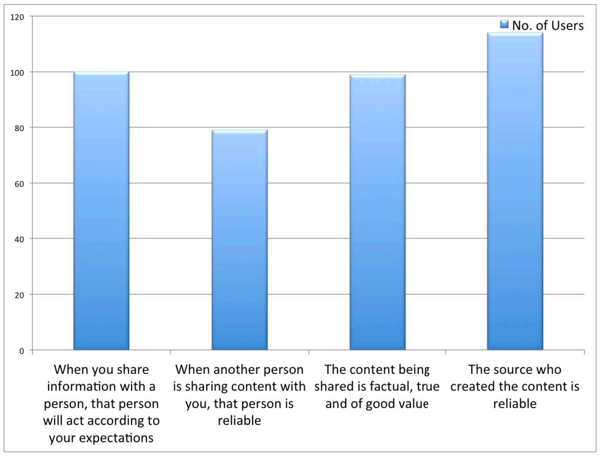

Figure 7. User’s Perception of their Meaning of Trust

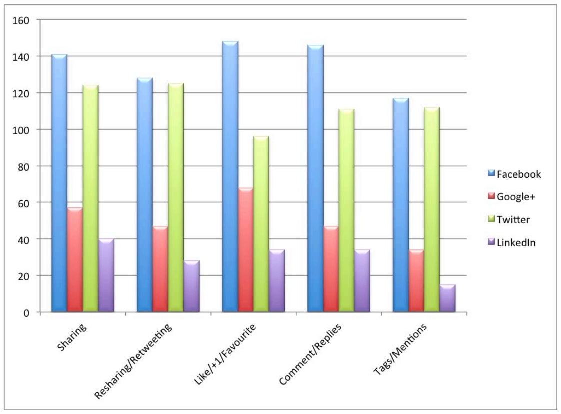

Figure 8. Overall Participant’s Activity of Social User Interactions

5) User’s perception of trust whilst commenting or replying: Table IV shows the results of the participants trust perception whilst commenting or replying within each Social Network. With this user interaction type, participants trust more the person who created the post. This is because comments or replies might also contain content that might reflect distrust in the content or source. However, it would be interesting as future work to analyse how to capture trust or distrust from the semantics of the comments or replies.

6) User’s perception of trust whilst tagging or mentioning other users: Table IV illustrates the results of the participants trust perception whilst tagging or mentioning other users within each Social Network. The results show that the participants trust more the person who they are tagging.

7) User’s perception of trust whilst tagged or mentioned by other users: Table IV shows the results of the participants trust perception when s/he is tagged or mentioned by other users within each Social Network. These results illustrate that the perception of trust in the other person tagging or mention the user is lower than the perception of trust in the other person being tagged or mentioned by the user.

III. ASSERTING TRUST

The user study reveals important insights to the several trends in Facebook, Google+, Twitter and LinkedIn. Figure 8 summarises the overall activity of participants interactions within these Social Networks. These results show that all the user interaction types are mostly used in Facebook and Twitter. Hence, these Social Networks are the optimal for capturing trust for these social user interaction types.

Table V illustrates the average and standard deviation of the participants activity using the outlined social user interactions within these Social Networks. As can be noted, sharing of external content into the Social Networks is the most common user interaction activity amongst the participants. This is followed by liking, +1 or favouring content; comments or replies; and re-sharing or retweeting. Surprisingly, tags or mentions is the least user interaction type used.

The survey also provides useful results about the participants perception of trust. Figure 9 summarises the overall participants perception of trust when using these social user interactions. This illustrates that we can therefore correlate trust and the user interactions as follows:

- The trust for the source who created the content can be captured using (1) the sharing and (2) the re-sharing or retweeting user interactions;
- The trust for the content can be captured using (1) the sharing, (2) the re-sharing or retweeting; and (3) the “like” or “+1” or “favourite” user interactions; and
- The trust for the user requesting personal information can be captured using (1) the “like” or “+1” or favourite; (2) the comments or replies; (3) tags or

Table V
AVERAGE AND STANDARD DEVIATION OF THE PARTICIPANTS ACTIVITY OF THE SOCIAL USER INTERACTIONS

Social User Interaction	Average Activity	Standard Deviation
Sharing	62.76%	31.28%
Resharing / Retweeting	56.78%	33.57%
Like / +1 / Favourite	60.29%	30.33%
Comment / Replies	58.27%	33.40%
Tags / Mentions	47.91%	34.25%

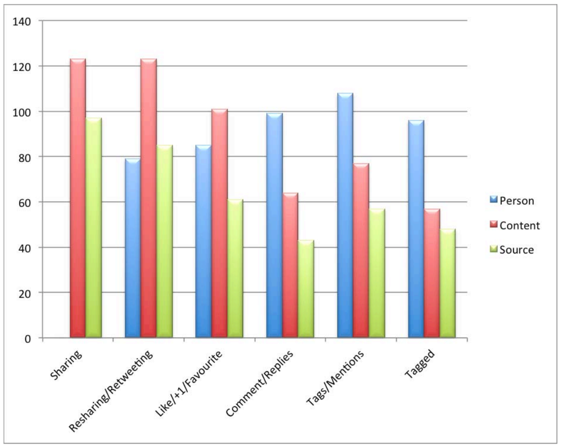

Figure 9. Overall Participant's Perception of Trust

mentions and (4) tagged or mentioned user interactions.

Table VI illustrates the average and standard deviation of the participants trust perception of the outlined social user interactions within these Social Networks. It can be noted that re-sharing or retweeting is considered as the most user interaction type that captures trust. This is followed by liking, +1 or favouring content; tags or mentions and sharing. Comments or replies are the user interaction types that users perceive as the least activity to capture trust.

Therefore, based on these results we now examine how trust can be asserted.

A. Trusting The Source

The results reveal that the trust for the source can be asserted using the (1) sharing and (2) re-sharing or retweeting of content. Computing trust based on this metric, the algorithm will take into consideration the number of times the content related to the source was shared and re-shared. However, since trust is very personal and subjective, taking all the number of shares and re-shares for any content related to the source would not result in a personal subjective trust value since there might be users who shared and re-shared the content that the user might not trust.

Table VI
AVERAGE AND STANDARD DEVIATION OF THE PARTICIPANTS TRUST PERCEPTION

Social User Interaction	Average Trust Perception	Standard Deviation
Sharing	41.67%	10.61%
Re-sharing / Retweeting	53.33%	14.57%
Like / +1 / Favourite	47%	11.53%
Comment / Replies	39%	16.09%
Tags / Mentions	45.67%	14.57%

Therefore, when assessing the trust judgement for the source, the social graph must also be taken into consideration. However, those who are not direct connections, their trust can be inferred through the notion of transitivity – a person in the social graph can recommend the trustworthiness of another person not directly connected to the user. Transitvity can be asserted using algorithms such as in [6].

The user's subjective trust value for the source can therefore be calculated as the weighted average of all the shares and re-shares of content related to the source weighted by the trust of users. This is represented as follows:

$$\bar{\tau} = \frac{\sum_{i=1}^{n} w_i s_i}{\sum_{i=1}^{n} w_i} \tag{1}$$

where $\bar{\tau}$ denotes the user's subjective trust value of a particular source, w denotes the trust value a third party user has in the user's social graph and s denotes the number of shares and re-shares related to the source the third party user has fulfilled.

Definition 1: Trusting the source. Let ST be the subjective trust value for the source SO, U a user identified by a URI, P a directly or indirectly connected peer identified by a URI and SH a shared content or a re-shared content or a retweet. Let $Trusts(P, U)$ mean that P is trusted by U, $SharedBy(SH, P)$ or $SharedBy(SH, U)$ mean that SH is shared by P or SH is shared by U, $Related(SH, SO)$ mean that SH is related to SO, $AssertedBy(SO, U)$ mean that SO is asserted by U and $AssignTrust(ST, SO)$ mean that SO is assigned ST, where $ST \in [-1, 1]$. Thus, trusting the source is defined:

$$\begin{aligned} &\forall \mathit{SH}(\mathit{Trusts}(P,U) \wedge (\mathit{SharedBy}(SH,P) \\ &\vee \mathit{SharedBy}(SH,U)) \wedge \mathit{Related}(SH,SO) \\ &\wedge \mathit{AssertedBy}(SO,U)) \Rightarrow \mathit{AssignTrust}(ST,SO) \end{aligned} \tag{2}$$

B. Trusting The Content

The user study results show that trust for content can be asserted from: (1) the share button; (2) the re-share or retweet button; and (3) the "Like", "+1" and "Favourite" buttons. The "like", "+1" and "favourite" buttons capture trust for the content types as illustrated in figure 4. Similar to computing user's subjective trust for the source, the user's social graph must be taken into consideration in order to compute an accurate and personalised trust value. Therefore, only the weights from the directly connected trusted users or from the indirectly connected trusted users the algorithm should take into consideration.

The user's subjective trust value for the content can therefore be calculated as follows:

$$\bar{\tau} = \frac{\sum_{i=1}^{n} w_i c_i}{\sum_{i=1}^{n} w_i} \tag{3}$$

where $\bar{\tau}$ denotes the user's subjective trust value of a particular content, w denotes the trust value a third party user has in the user's social graph and c denotes the number of shares, re-shares, likes, +1s and favourites related to the same content the third party user has fulfilled.

Definition 2: Trusting the content. Let CT be the subjective trust value for the content CO, U a user identified by a URI, P a directly or indirectly connected peer identified by a URI, SH a shared content or a re-shared content or a retweet and LI a "Like", "+1" or "Favourite". Let $Trusts(P, U)$ mean that P is trusted by U, $SharedBy(SH, P)$ or $SharedBy(SH, U)$ mean that SH is shared by P or SH is shared by U, $ClickedBy(LI, P)$ or $ClickedBy(LI, U)$ mean that LI is clicked by P or LI is clicked by U, $Related(SH, CO)$ or $Related(LI, CO)$ mean that SH is related to CO or LI is related to CO, $AssertedBy(CO, U)$ mean that CO is asserted by U and $AssignTrust(CT, CO)$ mean that CO is assigned CT, where $CT \in [-1, 1]$. Thus, trusting the content is defined:

$$\begin{aligned} &\forall SH \forall LI(Trusts(P,U) \wedge (SharedBy(SH,P) \\ &\vee SharedBy(SH,U)) \wedge (ClickedBy(LI,P) \\ &\vee ClickedBy(LI,U)) \wedge Related(SH,CO) \\ &\wedge Related(LI,CO) \wedge AssertedBy(CO,U)) \\ &\Rightarrow AssignTrust(CT,CO) \end{aligned} \tag{4}$$

C. Trusting The User

The trust value assigned to the user requesting information, known as the requester, the user study results show that it can be asserted from: (1) the "Like", "+1" and "Favourite" buttons; (2) the comments or replies to posts between the user and the requester; (3) the tags of the requester tagged by the user; and (4) the tags of the user tagged by the requester. The "likes", "+1s" and "favourites" capture trust for the content types as illustrated in figure 4. Moreover, the content within the comments or replies are not taken into consideration since as mentioned earlier, this might reflect in distrust. However, in this work, we only focus on the act of the interaction. Therefore, capturing trust through comments or replies means the act that a requester interacted with the user through commenting or replying to posts.

Asserting the user's subjective trust value for the requester will therefore take into consideration the number of times these user interactions were used. The computation will take the sum of these weights and compare them to the total amount of the user's interactions with all users.

The user's subjective trust value for the requester can therefore be calculated as follows:

$$\tau = \frac{\sum_{i=1}^{n} r_i}{\sum_{i=1}^{n} u_i} \tag{5}$$

where τ denotes the user's subjective trust value of a requester; r denotes the number of "likes", "+1s" and "favourites" of the content related to the user and the requester, comments between the user and the requester, and tags of or tagged by the requester; and u denotes the number of all the user's interactions in the Social Web platform.

Definition 3: Trusting the user (i.e. requester). Let UT be the subjective trust value for the requester RE, U a user identified by a URI, LI a "Like", "+1" or "Favourite", CM a comment or reply and TA a tag or mention. Let $ClickedBy(LI, U)$ or $ClickedBy(LI, RE)$ mean that LI is clicked by U or LI is clicked by RE, $CommentedBy(CM, U)$ or $CommentedBy(CM, RE)$ mean that CM is commented by U or CM is commented by RE, $TaggedBy(TA, U)$ or $TaggedBy(TA, RE)$ mean that TA is tagged by U or TA is tagged by RE, $Related(LI, U)$ or $Related(LI, RE)$ mean that LI is related to U or LI is related to RE, $Related(CM, U)$ or $Related(CM, RE)$ mean that CM is related to U or CM is related to RE, $Related(TA, U)$ or $Related(TA, RE)$ mean that TA is related to U or TA is related to RE, $AssertedBy(RE, U)$ mean that RE is asserted by U and $AssignTrust(UT, RE)$ mean that RE is assigned UT, where $UT \in [-1, 1]$. Thus, trusting the requester is defined:

$$\begin{aligned} &\forall LI \forall CM \forall TA(((ClickedBy(LI,U) \wedge Related(LI,RE)) \\ &\vee (ClickedBy(LI,RE) \wedge Related(LI,U))) \\ &\wedge ((CommentedBy(CM,U) \wedge Related(CM,RE)) \\ &\vee (CommentedBy(CM,RE) \wedge Related(CM,U))) \\ &\wedge ((TaggedBy(TA,U) \wedge Related(TA,RE)) \\ &\vee (TaggedBy(TA,RE) \wedge Related(TA,U))) \\ &\wedge AssertedBy(RE,U)) \Rightarrow AssignTrust(UT,RE) \end{aligned} \tag{6}$$

Asserting trust for requesters with no previous interactions with the user will result in zero trust. In this case, the requester's trust can be asserted using our previous work [13]. In this work, we had presented a trust model to assert trust for requesters from information in the Social Web.

IV. Related Work

There are various research that study user patterns in Social Networks. The authors in [2] conduct a survey about the use of Facebook. Although they show interesting trends, they do not analyse the user interaction types which we have analysed in our survey and focus more on the privacy aspects rather than on trust.

Most work on trust focus on assigning trust values manually. In [6] the authors focus on inferring trust and reputation in Social Networks. The trust ratings are assumed to be manually inserted by users. The authors in [7] also focus on inferring trust in Social Networks from relationships, however they also assume that the user manually provides a rating to other users they are connected to.

The authors in [10] propose a method to propagate trust in Social Networks but they also assume that the trust value is provided. Similarly, the authors in [8] propose algorithms to propagate trust and distrust, however they also assume that the trust value amongst nodes is provided.

The authors in [5] propose a method for recommending trust amongst users based on how similar they are to each other according to their tastes for films and their film ratings. The ratings however are inserted manually by the user. The authors [14] also propose a profile similarity approach whereby they also try to assess similarity based on the trust decisions rather than on the actual profile attributes.

The authors in [9] present a framework to derive a degree of trust for users from their ratings and expertise. However, the framework is not suitable for capturing and deriving trust degrees from social user interactions in Social Networks. The authors in [11] also propose a model for predicting trust values. However, their work also focus on using user's ratings.

The authors in [3] outline several factors that effect trust decisions on content however they assume that users are trusted and also users insert manually trust ratings to the content.

The authors in [1] provide a comprehensive survey about trust that covers policy-based trust, reputation-based trust, general models of trust and trust in information resources. However, most of the work relies on users entering manually trust values or the trust value is provided.

V. Conclusion and Future Work

In this work we focused on analysing the user's perception of trust and how trust can be inferred from Social Networks. We carried out a user survey that analysed on one hand the trends and usage patterns in Facebook, Google+, Twitter and LinkedIn of (1) the "share" button from external Web sites, (2) the "re-share" or "retweet" button, (3) the "like" or "+1" or "favourite" button, (4) the "comment" or "reply" button; and (5) the "tag" or "mention" features. On the other hand, the survey analysed the user's perception of his/her meaning of trust and the perception of trust in these interactions. The results have shown that users are concerned in asserting trust for: (1) the source that created the content, (2) the content itself, and (3) the users requesting personal information. From the survey results, we explained which of the above user interactions are useful to assert trust values for these three entities.

As future work, we will be implementing these trust assertions within our Privacy Preference Framework [12] in order to enforce privacy preferences based on these trust assertions.

References

[1] D. Artz and Y. Gil. A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, June 2007.

[2] D. Boyd and E. Hargittai. Facebook privacy settings. Who cares? *First Monday*, 15(8), August 2010.

[3] Y. Gil and D. Artz. Towards content trust of web resources. *Web Semantics: Science, Services and Agents on the World Wide Web*, Dec. 2007.

[4] S. Goel, J. M. Hofman, and M. I. Sirer. Who does what on the web: A large-scale study of browsing behavior. In *AAAI Conference on Weblogs and Social Media, ICWSM'12.*, 2012.

[5] J. Golbeck. Trust and nuanced profile similarity in online social networks. *ACM Transactions on the Web*, Sept. 2009.

[6] J. Golbeck and J. Hendler. Accuracy of metrics for inferring trust and reputation in semantic web-based social networks. In *EKAW'04*, 2004.

[7] J. Golbeck and J. Hendler. Inferring binary trust relationships in web-based social networks. *ACM Transactions on Internet Technology*, Nov. 2006.

[8] R. Guha, R. Kumar, P. Raghavan, and A. Tomkins. Propagation of trust and distrust. In *WWW'04*, 2004.

[9] Y. A. Kim, M.-T. Le, H. Lauw, E.-P. Lim, H. Liu, and J. Srivastava. Building a web of trust without explicit trust ratings. In *ICDEW'08*, 2008.

[10] Y. A. Kim and H. S. Song. Strategies for predicting local trust based on trust propagation in social networks. *Knowledge-Based Systems*, 2011.

[11] H. Liu, E.-P. Lim, H. W. Lauw, M.-T. Le, A. Sun, J. Srivastava, and Y. A. Kim. Predicting trusts among users of online communities: an epinions case study. In *EC'08*, 2008.

[12] O. Sacco, A. Passant, and S. Decker. An Access Control Framework for the Web of Data. In *IEEE TrustCom-11*, 2011.

[13] O. Sacco, A. Passant, and S. Decker. Fine-Grained Trust Assertions for Privacy Management in the Social Semantic Web. In *IEEE TrustCom-13*, 2013.

[14] C.-N. Ziegler and J. Golbeck. Investigating interactions of trust and interest similarity. *Decision Support Systems*, Mar. 2007.