Journal of Applied Sciences

ISSN 1812-5654

Journal of Applied Sciences 14 (22): 2953-2966, 2014
ISSN 1812-5654 / DOI: 10.3923/jas.2014.2953.2966

Defeasible Logic-Based Strategies to Regulate Facebook

Mahdi Rohaninezhad, Shereena Mohd Arif and Shahrul Azman Mohd Noah
Knowledge Technology Research Group, Centre for Artificial Intelligence and Technology,
43600, UKM Bangi, Selangor, Malaysia

Abstract: Current social network sites like Facebook have not sufficiently addressed how to help users manage and create friend lists and satisfy privacy concerns and newsfeed content management. We conducted qualitatively designed study to investigate how we might enhance Facebook decision-making via a rule-based system able to deal with vast numbers of conflicting, exceptional and competing situations. These circumstances stem from the nature of the site which operates on the borders of private and social life, online and offline sphere. We introduced a defeasible logic framework to do reasoning and make decisions under those circumstances contributes to other approaches such as data-mining techniques, learning systems, neighborhood graphs and smartphone technologies. Our study revealed that this logic formalism can fill the gap between user and Facebook preferences in online-offline and private-public social life.

Key words: Defeasible logic, semantic web, social networks, facebook

INTRODUCTION

Social Network Sites (SNSs) are becoming an undeniable part of maintaining, extending or strengthening relationships, interests and activities (Ellison, 2007) in different spheres of social lives. Facebook is the most popular SNS with more than one billion users (Facebook, 2013b). Facebook was founded by Mark Zuckerberg in early 2004 only for Harvard University students (Facebook, 2013a) but now is the most trafficked site on the Web (Alexa, 2013) with more than 660 million active users (Facebook, 2013b).

Previous study on Facebook elaborated that the privacy threat and the segmentation between private and social (or professional) lives are users' main concerns (Debatin *et al*., 2009; Ellison *et al*., 2011a; Stutzman *et al*., 2012; Vitak *et al*., 2012; Peluchette *et al*., 2013). Some researchers revealed that the privacy concerns regarding Facebook mainly stem from the non-segmented structure of friend lists and the nature of privacy settings in the site (Lipford *et al*., 2008, 2010; Farnham and Churchill, 2011). Neighborhood graph and data mining techniques for friend classification and detecting a user's community (Fortunato, 2010) are the most successful approaches in this area (Fang and LeFevre, 2010; Cheek and Shehab, 2012; Mazzia *et al*., 2012; Min *et al*., 2013).

However, simulating real-life facets of Facebook may cause vast numbers of conflicting, exceptional or competing situations in this heterogeneous site. Because users have different (and sometimes contradictory) faceted identities (Farnham and Churchill, 2011; Peluchette *et al*., 2013) in their offline social lives with specific approaches to each facet. Furthermore, Facebook with assisting smartphone technologies is bridging and operating on the boundaries of the private-social and online-offline spheres (Min *et al*., 2013). These circumstances necessitate a mature reasoning system that perceives users' priorities and preferences to make decisions with contradictory evidences and exceptional situations.

The goal of this study is to introduce a non-monotonic rule-based approach for advanced Facebook use by smartphone technology and friend classifier. Defeasible logic (Nute, 2001) is a non-monotonic reasoning formalism (Antonelli, 2010) with low computational complexity (Maher, 2001). It can draw coherent and consistent conclusions under contradictory, exceptional or competing situations (Maher, 2002). This study's rule-based system plays the role of conflict and exception resolution to make decisions based on user preferences, site regulations and classified, mined data.

We first examine extensive research done by socialists to elaborate on Facebook's benefits and shortcomings accompanied with users' behavior strategies. In the latter part, we discuss technical investigations intended to address those problems and gain the benefits.

According to Lampe *et al*. (2006), Facebook users mostly employ the site to maintain their offline connections rather than extend their friendships. That is, Facebook is a social network for knowing more about

Corresponding Author: Mahdi Rohaninezhad, Knowledge Technology Research Group, Centre for Artificial Intelligence and Technology, 43600, UKM Bangi, Selangor, Malaysia

offline friends, rather than initiating relationships at which user's profile information acts as a signal to find friends (Lampe *et al*., 2007). However, Ellison *et al*. (2007) in an extensive study revealed the benefits of Facebook in bridging online and offline social life. They elaborated that Facebook plays a positive role not only for maintaining bridge social capital but also for initiating it via converting inactive latent ties into activated weak ties which is media's implication (Haythornthwaite, 2005). Moreover, Facebook contributes to bonding social capital by maintaining pre-existing close and actual relations. Nevertheless, the benefits of Facebook are intertwined with the user's connection strategies (Ellison *et al*., 2011b). Initiating, maintaining and information seeking are three connection strategies and effects of each strategy on user's social capital investigated in the study. They showed that the information-seeking strategy contributes to an organic correlation between online and offline social life while the two other connection strategies do not significantly contribute to social capital. It is worth noting that the initiating strategy is uncommon to Facebook users and the maintaining strategy (users' inclination to keep in touch only with actual friends) is not expected to be influenced by SNSs. The maintaining strategy leads to keeping connections with actual friends who are not necessarily close or intimate but mostly are people with whom we have strong offline relationships. Amongst these friends, only a small proportion are interacted with (Marlow, 2009) and appear in the newsfeed (Bucher, 2012). Moreover, Facebook newsfeed optimization (NFO) in the "Top news" mode which almost 95% of users employ, causes the threat of invisibility (Bucher, 2012) and unimportant stories appearing in the newsfeed (Paek *et al*., 2010). The threat of invisibility is the possibility of constantly being disappeared in the newsfeed. In other words, for appearing in the newsfeed, users need to behave according to NFO algorithm at which visibility is a reward of interaction.

However, privacy concerns are the major handicap to reaping Facebook's benefits (Debatin *et al*., 2009). Debatin *et al*. (2009) revealed that Facebook users are threatened by information disclosure not only because of the site's semi-private environment but also because of profile data mining and data matching by third-party developers seeking financial gain (Privacy International, 2007). Although, the site's ability to limit profile access to "friends only" provides a rudimentary and minimum level of privacy control, third-party developers can access this information via apps in a larger scale. Recent study demonstrated the crucial role of this concern in a user's willingness to disclose information in Facebook (Stutzman *et al*., 2012). More focused and detailed study (Vitak and Ellison, 2012) upheld that the privacy concern is the main barrier for gaining Facebook's benefits by users with both information-seeking (bridge social capital) and maintaining (bonding social capital) strategies.

Users' approaches to addressing this concern varies. According to Ellison's study, Facebook users utilize three kinds of strategies to control their audience, namely, friending behavior, privacy setting and self-disclosure approaches (Ellison *et al*., 2011a). However, the nature of the site makes it difficult to speculate who can see shared posts in newsfeeds (because of the newsfeed optimization algorithm and privacy setting interface) and to whom the posts will be sent. Further study focused on privacy concerns and the boundaries between work and private life (Vitak *et al*., 2012), lightening three forms of Facebook content collapse, restricting friendships to only a few trusted coworkers, creating multiple Facebook accounts or self-monitoring content sharing. Another study upheld users' inclination to segment between private and professional life (Peluchette *et al*., 2013) and showed the majority of Facebook users decline a manager's friend request or add him or her to a restricted friend list.

Lipford *et al*. (2008) did one of the first technical studies to address the ambiguous state of the site to speculate "who can see what." They proposed a prototype "audience view interface," now deployed by Facebook1, where Facebook users can see their profiles in the eyes of their audience rather than deal with complicated privacy setting options, the effects of which are unclear and not well understood by users. In their suggested scheme, users could grant or deny access to profile information to each friend and see the consequences. Mazzia *et al*. (2012) critiqued the Lipford approach, for which users can only visualize and modify the privacy of predefined friend lists while they proposed a method that detects a user's friend circles (communities) based on the neighborhood graph (Fortunato, 2010) and classification techniques.

Using a different perspective, Fang and LeFevre (2010) addressed the issue throughout a learning paradigm called certainty sampling, based on a question-answering technique about unlabeled friends to recognize users' privacy preferences. Their methodology was based on recognizing and learning a user's privacy preferences for each community obtained from the user's neighborhood graph to extract classification features. They visualized and represented the outcome through a decision tree that demonstrates the permission of friend lists. Their findings also uphold previous social study that users conceive their privacy policy within circles of communities (life facets). Cheek and Shehab (2012) in a similar study, introduced a semi-automated approach called same-as policy management. In this policy managing technique, users should list their friends throughout a listing assistant prototype at which friends are already classified via CNM (Clauset Newman Moore clustering algorithm) and users could set the lists' privacy policy. In the final step, users were allowed to except some list members to access specific information which was nominated as a policy exception in the system.

Other study, in this regard, emphasized a user's faceted identity that leads to variant strategies to maintain social boundaries within social technologies (Farnham and Churchill, 2011). Convergent study (Ozenc and Farnham, 2011) offered a model for online social technologies to maintain the social boundaries inspired from the natural model of the social organism of a user's life. Family, work and socializing are perceived as the three main facets of everyone's life. They visualized friend group segmentations of users based on the time, location, groups, number of people and similarity. They suggested focused sharing vs. a tough privacy policy. Smartphone technology plays a central role in filling the gap between offline and online social life and helps determine a user's mode (user's current facet). Min *et al*. (2013) continued the idea of smartphone technology for classifying facets of social life. They obtained 90.5% accuracy of classification by using call and text message logs based on Android smartphone technology synchronized with Facebook profiles. Another study done by the Google+team (Kairam *et al*., 2012) suggested a focused sharing rather than an all-or-nothing sharing strategy. They investigated users' motives to share information and indicators for selecting audiences that emphasize the need for organizing friend lists based on life facets and tie strength.

Generally, addressing privacy concerns on a large scale is intertwined with providing a scheme for simulating users' faceted offline social lives into online social networks. Most of the solutions revolve around segmentation and classification of friend lists so audience selectors and privacy controllers can be visualized, modified and assigned on that basis.

THEORETICAL FOUNDATION

Basics of defeasible logic: Defeasible logic (Nute, 2001) intuition is to be able to draw plausible conclusion from partial or even conflicting information. It conveys five types of knowledge; facts, strict rules, defeasible rules, defeater rules and superiority relation among rules. Essentially, defeaters prevent some conclusions from being drawn while superiority relations provide information about the relative strength of rules. A set of rules (i.e., the knowledge base) consisting of these items is called defeasible theory. For instance, the following knowledge base is a defeasible theory:

R1: $Bat(X) \rightarrow mammal(X)$	Strict rule
R2: $Mammal(X) \Rightarrow \neg fly(X)$	Defeasible rule
R3: $Bat(X) \Rightarrow fly(X)$	Defeasible rule
R4: $Bird(X) \Rightarrow fly(X)$	Defeasible rule
R5: $HeavyBird(X) \rightarrow \neg fly(X)$	Defeater rule
R6: $Bat(X)$	Fact
R3: >R2	Superiority relation

At which "r1" implies bats definitely are mammal. Mammals typically do not fly (r2) and birds typically fly (r4). This theory by means of superiority relation (r3>r2) tell us despite bats are mammal; they normally can fly (r3). And defeater rule implies that although birds can fly, heavy birds might not fly (r5).

There are two types of conclusions in Defeasible Logic (DL), namely strict and defeasible conclusions (Antoniou *et al*., 2001). Strict conclusions are those for which their antecedents are provable through strict rules and given facts, whereas for defeasible conclusions, both strict and defeasible rules are taken into account in proof theory algorithms. In addition, defeasible conclusion algorithms should consider the superiority between defeasible rules, attacks from contradictory rules and defeaters.

It is worth to note that the sentences that contain terms like "typically", "normally" and other similar modifiers convey defeasible rules and the sentences containing "maybe", "might" and other probabilistic auxiliary verbs represent defeater rules.

Defeasible logic proof theory: According to Antoniou *et al*. (2001), the conclusion of D is a tagged literal, unlike monotonic reasoning that has two types of provability ($+\Delta q$, $-\Delta q$), can have one of the following four forms:

- $+\Delta q$ which is intended to mean that q is definitely provable in D
- $-\Delta q$ which is intended to mean that we have proved that q is not definitely provable in D
- $+\partial q$ which is intended to mean that q is defeasibly provable in D
- $-\partial q$ which is intended to mean that we have proved that q is not defeasibly provable in D

That means, to prove $+\Delta q$ or $-\Delta q$ only facts and strict rules will be considered as classical sense. While for proving $+\partial q$ or $-\partial q$, we use all DL epistemic knowledge features and also might need to consider possible attacks in reasoning chain that supports ¬q.

Semantic inheritance network: A semantic inheritance network (Horty *et al*., 1990) is a direct graph used to represent defeasible inference and ambiguous states. The initial node of the network refers to a particular individual and all non-initial nodes represent kinds, categories or properties. This graph supports a bottom-up reasoning technique and there is an analogy between path and arguments in the network.

Ambiguous states are an issue in DL proof theory that are rooted in its skeptical nature of reasoning. It appears when an individual stands in a contradictory situation with the same superiority level. There are two different approaches for dealing with ambiguity; ambiguity blocking and propagating. A semantic inheritance network is compliant with defeasible logic, as information of a specific kind can override information of a more general kind. It is an instance of defeasible logic inference with respect to superiority relation (Billington *et al*., 1990). The upper nodes refer to more general concepts and lower nodes contain more specific information that refers to higher priority rules in conflicting or ambiguous situations.

We used this knowledge representation technique to better understand a skeptical situation and more importantly demonstrate superiority relation between states. Based on this notion, suggested semantic inheritance network for Facebook mechanism conveys superior states and also visualize ambiguous states that are there to be resolved.

METHODOLOGY

The methodology of this study is based on a defeasible interpretation of Facebook NFO algorithm and neighborhood graph for content managing and community detecting with a focus on contradictory, exceptional and competing states. We address a defeasible interpretation of current Facebook mechanisms and use the SPINdle defeasible logic reasoner to make decision. As in previous study (Fang and LeFevre, 2010; Fortunato, 2010; Mazzia *et al*., 2012), we use neighborhood graph approach as a community detector but with a defeasible interpretation of community members and boundaries.

We use the SPINdle 2.2.1 defeasible logic reasoner to draw conclusions and proof our scenario outcomes. SPINdle is a data-driven defeasible reasoner compliant with semantic web technologies (Lam and Governatori, 2009). For deploying scenarios in this study, we enhanced the reasoner in language to be prolog-like and support D-RuleML version 1.0 (Bassiliades *et al*., 2013). We also enhanced the reasoning routine to support competing rules. It is worth pointing out that, in the new prolog-based syntax of SPINdle notation, the symbols to represent strict, defeasible, defeater rules and negations are ":-," ":=," ":~," and "¬", respectively. In addition, like a prolog logic programming language, we follow the reduction tradition of rules representation for which a rule's head comes at the left and the body comes after implication notations at the right-hand side. For example, the defeasible theory of is as follows in our prolog-like language:

R1: mammal(?x) :- bat(?x)
R2: ¬fly(?x) := mammal(?x)
R3: fly(?x) := bat(?x)
R4: fly(?x) := bird(?x)
R5: ¬fly(?x) :~ heavyBird(?x)
R6: bat(?x)
R3>R2

In each part of following section, we simulate and elaborate controversial situations via appropriate scenarios that are converted into defeasible theories by human assistance. The results of the reasoner for the simulated situation will be discussed and analyzed in each scenario.

DEFEASIBLE ENHANCEMENT OF FACEBOOK

First-Order Logic (FOL) is not enough to regulate and make decisions for such a heterogeneous SNS. Specifically, with the existence of friend lists in both life facets and tie strengthening dimensions and also bridged online and offline social life, it has to deal with a huge number of exceptional, contradictory and competing situations that is far beyond the capability of FOL. For example, FOL cannot draw conclusion in a case that user makes his boss an exception amongst study list to be confined to see only public posts. More generally, FOL will be stuck in ambiguous state and cannot make decision for friend lists with different access levels that has intersection (common members). We can extend this example for all cases that user preferences are not compatible with Facebook preferences to approach to the friend lists.

Figure 1 demonstrates the total view of the Facebook interaction model with standard friend lists and NFO. It shows two types of friend lists accommodate life facets and tie strength. Close, restricted and acquaintance friend

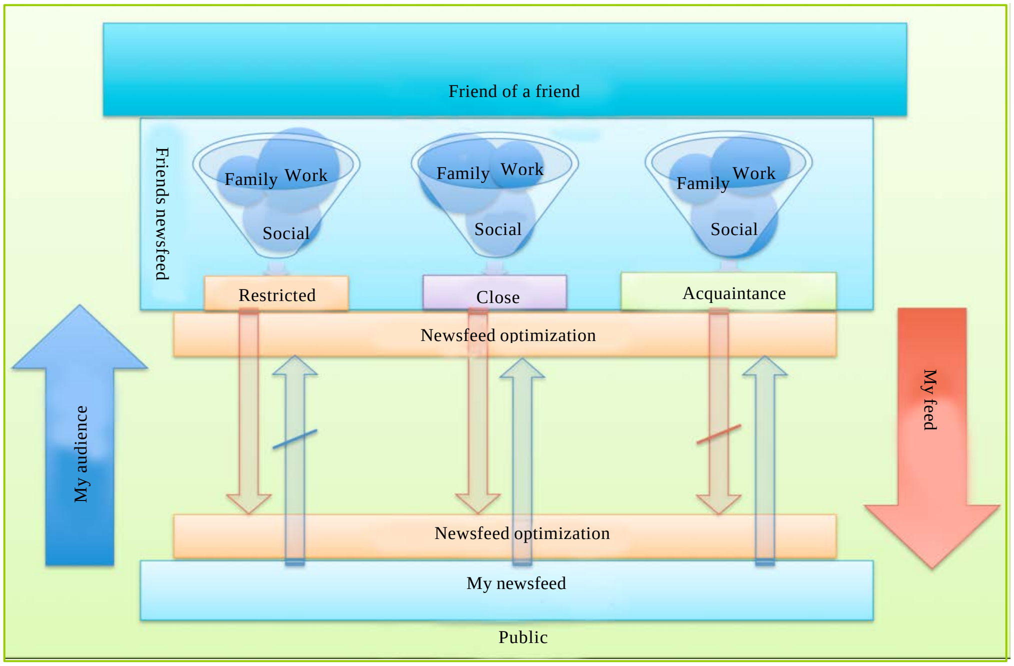

Fig. 1: Facebook content manager

lists categorize tie strength and play an important role for selecting audiences and adjusting the newsfeed. Using a different perspective, family, work and social friend lists categorize facets of users' identities (Ozenc and Farnham, 2011; Min *et al*., 2013) for which each friend list, in turn, can be segmented into tie strengthening lists. NFO acts as a ranking system to provide a user's top news stories. This conceptual framework is accessible with current Facebook architecture and tools if users define friend lists appropriately.

Newsfeed has two different modes, called "Top news" and "Most recent". Based on the Facebook help center, "Top news" are the most favorable stories for users calculated by the Facebook EdgeRank algorithm (Fig. 2). The EdgeRank algorithm calculates "top news" based on an object's affinity, weight and time decay, for which an object is any story appearing in the newsfeed such as status, photos, etc. Affinity (u_e) represents the relation strength between user and each connection such as friends, pages and so on, that leverages hearing from friends which user has liked or commented on the stories. Weight (w_e) is the value of each story based on the likes or comments it receives. The time decay score (d_e) implies how long has passed since the story was created, considering old stories lose priority and the newsfeed will remain fresh with new stories.

$$\sum_{\text{edges } e} u_e \quad W_e \quad d_e$$

u_e: affinity score between facebook user and edge creator

W_e: edge weighting

d_e: time decay factor based on recency of edge creation

Fig. 2: Facebook newsfeed optimization

Nevertheless, a user's actual favorable newsfeed is subjective and might vary from one to another, rather than be an objective routine to be determined by EdgeRank algorithm. EdgeRank algorithm speculates favorite stories based on creators, not content which causes unimportant stories to appear in the newsfeed (Paek *et al*., 2010). Facebook, however, has provided some tools and mechanisms for users to adjust their newsfeed such as adding friends or pages into the interest lists or hiding them from the newsfeed. In a privative perspective, users can determine whom they do not want to hear from (via the acquaintance list) or friends whom they do not want to disclose to (via restricted list). Moreover, NFO algorithm outcomes and friends privacy setting are two

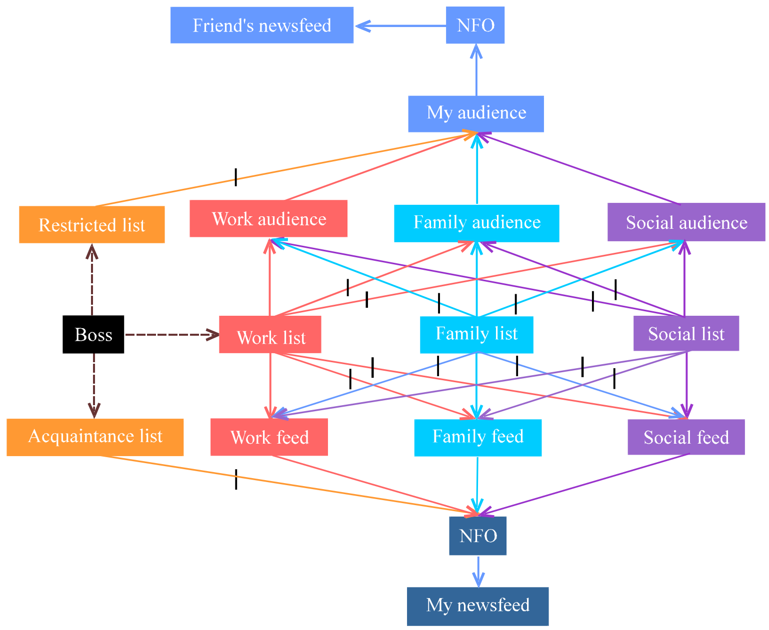

Fig. 3: Model via Semantic inheritance network

major inaccessible indicators that prevent speculation about who will actually see our stories at the end of the day. That is, the presumed audiences are all friends, except for restricted ones but the actual audience remains concealed to users.

In Fig. 3, we introduce a defeasible interpretation of current Facebook interactions that contribute to more flexible and robust online communication. The figure represents the analogous inheritance network of the defeasible interpretation model. In the current site, if a user places a friend on the restricted list, he or she will not receive any story of the user created for friends, except public stories. While in the following design, restricted people belonging to one or several facets of the user's social life are allowed to hear stories shared related to the facet via focused sharing. For instance, in Facebook, if a user puts his or her boss on the restricted list and work list, the boss will not receive any story, even work stories. While, by doing this, the boss can receive work stories (via focused sharing) but not stories shared for friends or friends of friends. However, if a user's boss only belongs to the restricted friend list, then he or she will not receive the user's stories, even those shared for study list. As another example, if a user puts his or her boss on the acquaintance list, in the current Facebook mechanism, the boss's stories will not appear in the newsfeed but in the proposed model, those stories shared with co-workers can appear in the feed with the high priority. These examples are only two of the vast number of exceptional situations in a social life. Every friend may belong to more than one friend list and a user's approach to each list might vary. In our model, both users' audiences and newsfeeds are segmented based on the life facets and tie strengthens lists that play the role of defeasible audience selector and newsfeed adjustor. The outcome of NFO provides classified data for the defeasible reasoner in our scheme and the reasoner decides actual feed amongst mined feeds at the end of the day.

We simulated our approach to Facebook via universal defeasible regulations and various conceivable scenarios. Regulations are defeatable in the light of further detailed information about users obtained from Facebook's data mining engines or users' mode (time and location) signalling via smartphones. All scenarios' consequences were proved via modified SPINdle reasoner 2.2.1 for this purpose and will be discussed here.

The following regulations imply that a user's audience typically belongs to the work, family, or social facet of his or her life. For instance, R1 demonstrates that if a friend "?f" is from the work audience of the user "?u," then she or he is typically among the user's audience or if the friend "?f" is restricted, she or he normally will not be considered an audience of the user "?u" (R5). The terms "normally" or "typically" imply it is possible to be on the work list but not be the actual audience of the work stories because of placement on the restricted list. Also, being on the study list does not necessarily imply receiving the study stories because of the NFO mechanism. Friends who are not classified in the life facet friend list only receive stories shared amongst all friend lists (not focused sharing):

R1: myAudience(?f,?u) := workAudience(?f,?u)
R2: myAudience(?f,?u) := familyAudience(?f,?u)
R3: myAudience(?f,?u) := socialAudience(?f,?u)
R4: myAudience(?f,?u) := acquaintanceList(?f,?u)
R5: ¬myAudience(?f,?u) := restrictedList(?f,?u)

However, R6 is a strict rule because it is impossible to be placed on the study list but not be amongst the study audience while normally, colleagues are not family or a social audience (R7 and R8). This implies that there are exceptional situations that defeat these rules, like belonging to both work and social lists (R9-R14 has the same interpretation). All life facets friend lists belong to a bigger set called the friend list, so that in non-focused sharing, all facet life lists are amongst audiences R15-R17:

R6: workAudience(?f,?u) :- workList(?f,?u)
R7: ¬familyAudience(?f,?u) := workList(?f,?u)
R8: ¬socialAudience(?f,?u) := workList(?f,?u)
R9: familyAudience(?f,?u) :- familyList(?f,?u)
R10: ¬workAudience(?f,?u) := familyList(?f,?u)
R11: ¬socialAudience(?f,?u) := familyList(?f,?u)
R12: socialAudience(?f,?u) :- socialList(?f,?u)
R13: ¬familyAudience(?f,?u) := socialList(?f,?u)
R14: ¬workAudience(?f,?u) := socialList(?f,?u)
R15: workAudience(?f,?u) := friendList(?f,?u)
R16: familyAudience(?f,?u) := friendList(?f,?u)
R17: socialAudience(?f,?u) := friendList(?f,?u)

The following nine rules clarify the relationship between friend lists and the newsfeed. For instance, R18 implies that if the friend "?f" is in the work list of the user "?u," then he or she typically appears in the work newsfeed of the user. However, study list members are not typically considered the family or social newsfeed (R19 and R20). The rules R21-R26 interpret the same way:

R18: workFeed(?f,?u) := workList(?f,?u)
R19: ¬familyFeed(?f,?u) := workList(?f,?u)
R20: ¬socialFeed(?f,?u) := workList(?f,?u)
R21: familyFeed(?f,?u) := familyList(?f,?u)
R22: ¬workFeed(?f,?u) := familyList(?f,?u)
R23: ¬socialFeed(?f,?u) := familyList(?f,?u)
R24: socialFeed(?f,?u) := socialList(?f,?u)
R25: ¬workFeed(?f,?u) := socialList(?f,?u)
R26: ¬familyFeed(?f,?u) := socialList(?f,?u)

The following rules (R27-R30) show that, if life facet friend lists share a story, it will be sent to NFO to calculate EdgeRank:

R27: NFO(?f,?u,?s) :- workFeed(?f,?u), shareStory(?f,?s)
R28: NFO(?f,?u,?s) :-familyFeed(?f,?u), shareStory(?f,?s)
R29: NFO(?f,?u,?s) :-socialFeed(?f,?u), shareStory(?f,?s)
R30: NFO(?f,?u,?s) :-acquaintanceList(?f,?u), shareStory (?f,?s)

After calculating EdgeRank, high-ranked stories appear in the user's newsfeed. However, acquaintances have a low affinity score (R32), so that their shared stories typically receive a low rank (R33):

R31: edgeRank (?f,?u,?s):- NFO(?f,?u,?s)
R32: affinity(?f,?u,low) :- AcquaintanceList(?f,?u)
R33: rankIs(?s,low) := Affinity(?f,?u,low), shareStory (?f,?s)

Now, we regulate the correlation between newsfeed and audience. If a friend's story appears in the user's newsfeed, then the user has definitely been an audience. That is, the user is an actual audience of the friend:

R34: audience(?u,?f) :- newsFeed(?f,?u)

However, if a friend is amongst the user's audience, he or she defeasibly receives the story in his or her newsfeed because of Facebook NFO and the friend's privacy settings:

R35: newsFeed(?u,?f) := audience(?f,?u)

Throughout the following scenarios, we discuss the consequences and abilities of the proposed rule-based system to address Facebook's shortcomings based on our literature review.

Work and private life: Imagine the user's boss places her in the restricted friend list. The user shares two stories, one within the colleague circle (focused sharing) and another one within all friends (non-focused sharing). With the current Facebook approach, the boss receives nothing even if the shared story is about and for the workplace. The defeasible audience selector provides a flexible scheme that facilitates the proper action in both cases. If a user "?u" shares a story "?s" for the friend list, then all friend members "?f" are audiences of the story except for the restricted person:

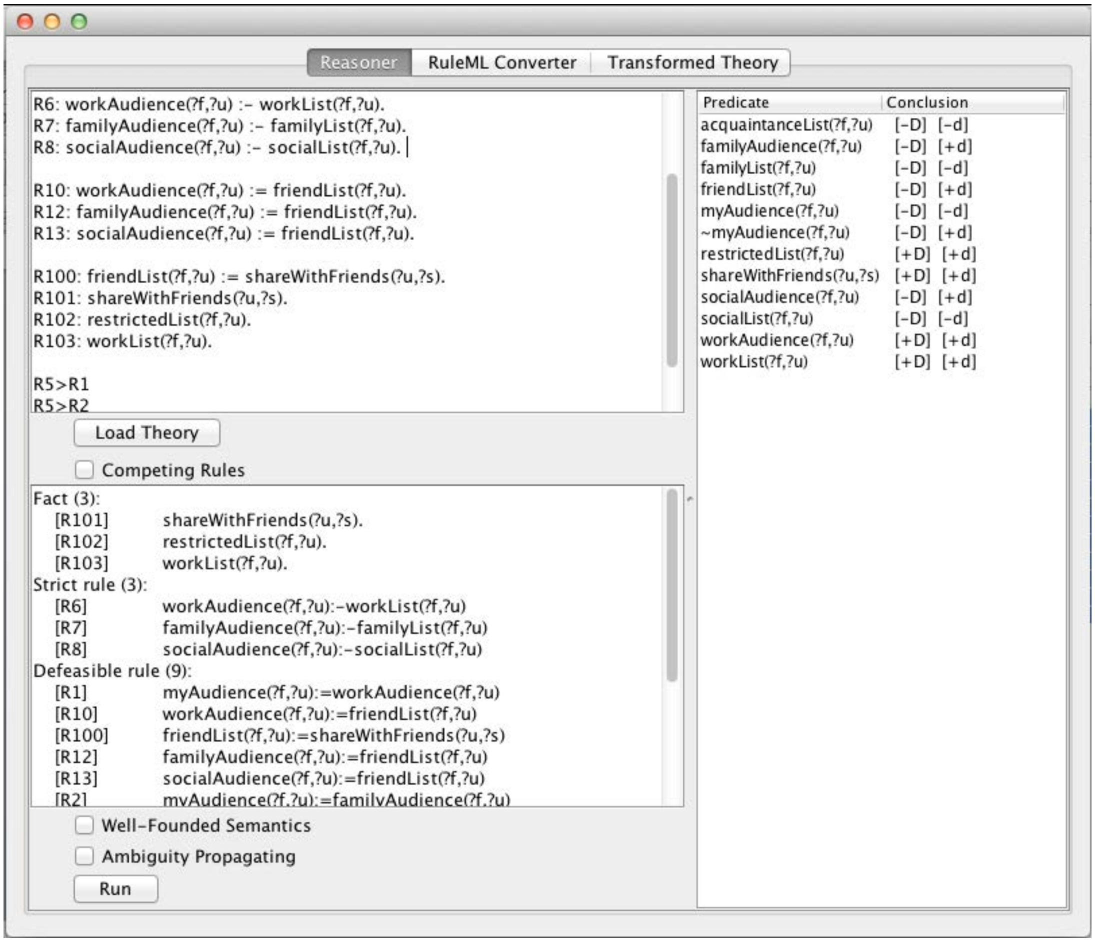

Fig. 4: SPINdle result for the first input defeasible theory

R100: friendList(?f,?u) := shareWithFriends(?u,?s)
R101: shareWithFriends(?u,?s)
R102: restrictedList(?f,?u)
R103: workList(?f,?u)
R5>R1, R5>R2, R5>R3, R5>R4

The following result shows that the user's boss is not amongst the story's audience (¬myAudience(?f,?u) [+d]). Figure 4 is a screen shot of the reasoner result and Fig. 5 represents the D-RuleML format of the input defeasible theory:

- myAudience(?f,?u) [-D] [-d]
- ¬myAudience(?f,?u) [-D] [+d]

However, if the user shares the story only with the work list, then the audience is all colleagues, including the restricted person, the boss:

R100: workList(?f,?u) := shareWithWorkmate(?u,?s)
R101: shareWithWorkmate(?u,?s)
R102: restrictedList(?f,?u)
R103: workList(?f,?u)
R1>R5, R2>R5, R3>R5, R4>R5

The results of the above scenarios are as follows. They imply that the user's boss also is amongst the user audience for this story (myAudience(?f,?u) [+d]):

- myAudience(?f,?u) [-D] [+d]
- ¬myAudience(?f,?u) [-D] [-d]

Superiority relations provide a flexible ground to deal with the restricted list so that focused sharing leads to sharing stories with restricted friends while non-focused sharing causes non-disclosure with the restricted one. This reveals how defeasible logic simply makes a flexible

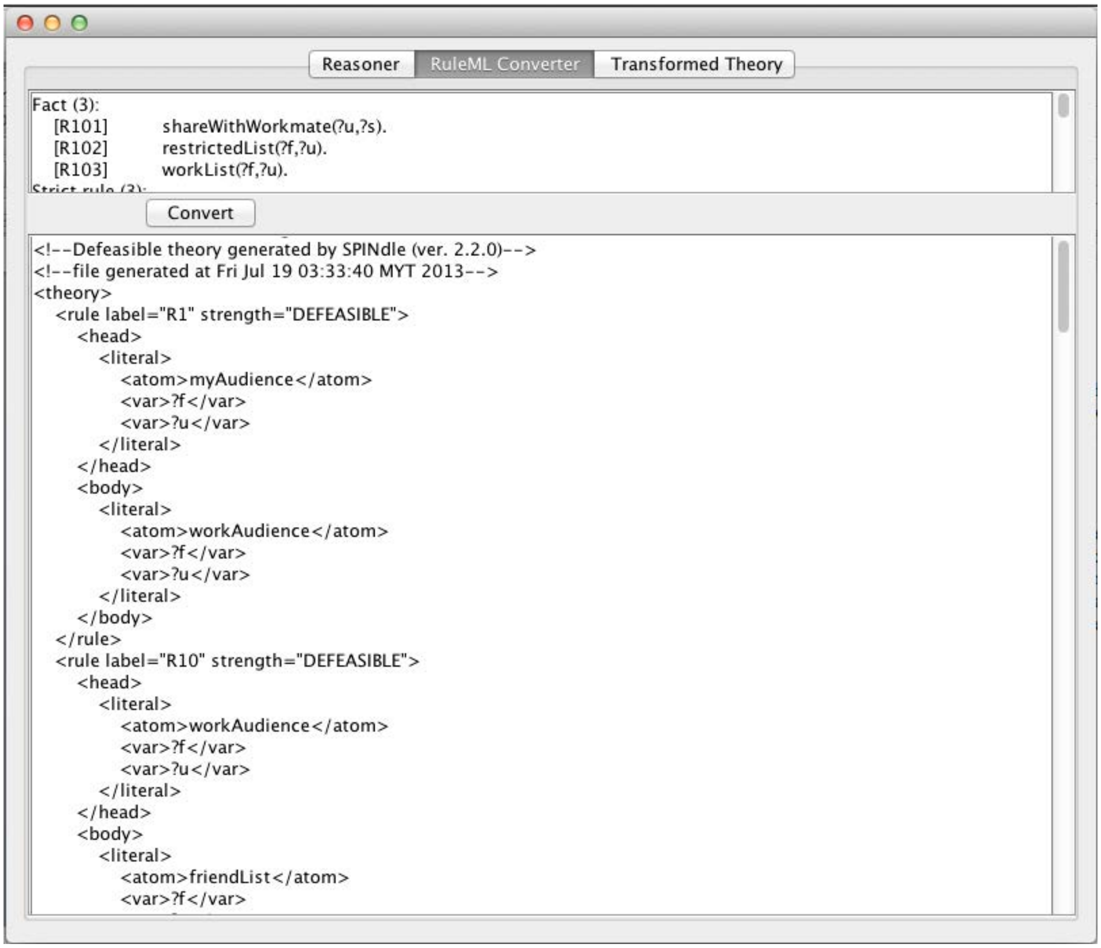

Fig. 5: RuleML format of the input query

audience selector and facilitates a kind of communication that would be very complex without this kind of decision-making. It is worth pointing out that, in both mentioned scenarios, decisions made by the reasoner are defeatable and can be defeated with further information about the user's preferences.

Subjective NFO and invisibility: The importance of shared stories not only depends on the affinity between story creator and user or the weight of the created story but also depends on the user's mode and the content of story itself (Paek *et al*., 2010; Pak and Paroubek, 2010). Users might be interested in seeing related stories with stories shared by their own or those who interacted with them, even if created by acquaintances. The following section addresses the problem of invisibility that contributes to more subjective decision-making in speculating stories favorable to the user.

To do this, we used a recent Facebook feature called Hashtag (#) to detect similar stories. This notion can be extended to a prototype to capture other user preferences. Users' preferences might be to see an advertisement, similar stories from acquaintances, items in interest lists and any other desired feed.

Acquaintance and interest lists demonstrate user preferences for their newsfeed. Stories shared by interest list members will definitely appear in the newsfeed (R200) while acquaintance stories, because of low affinity, automatically receive low edgeRank and typically do not appear in the newsfeed (R32, R33, R201). However, users might be interested to hear similar stories with those that receive high rank by NFO, even stories that are shared by acquaintances (R203). If a user interacts with those similar stories, then acquaintances' similar stories would be user favourable (R04) and defeat the NFO result (R204>R201). R205-R210 represents facts the system knows about a shared story and its creator, for which the story's creator belongs to both the work and acquaintance list (R205 and R206). The user has received and interacted with a similar story in his or her newsfeed previously (R207 to R210):

R200: newsFeed(?f,?u,?s):-interestList(?f,?u), share Story(?f,?s)
R201: ¬newsFeed(?f,?u,?s):= edgeRank(?f,?u,?s), rankIs (?s,low)
R202: newsFeed(?f,?u,?s):= edgeRank(?f,?u,?s), rankIs (?s,high)
R203: newsFeed(?f,?u,?s):~ acquaintanceList(?f,?u), shareStory(?f,?s), similarStory(?s,?s0), newsFeed (?f,?u,s0)
R204: newsFeed(?f,?u,?s) := acquaintanceList(?f,?u), shareStory(?f,?s), similarStory(?s,?s0), interact with Similar Story(?u,?s0)
R205: workList(?f,?u)
R206: acquaintanceList(?f,?u)
R207: similarStory(?s,?s0)
R208: shareStory(?f,?s)
R209: interactWithSimilarStory(?u,?s0)
R210: newsfeed(?f,?u,s0)
R204>R201

The result implies that the user definitely receives the story shared by a coworker (newsFeed(?f,?u,?s) [+D]) from the newsfeed acquaintance list if he has previously interacted with a similar story in his newsfeed:

- newsFeed(?f,?u,?s) [+D] [+d]
- ¬newsFeed(?f,?u,?s) [-D] [-d]
- rankIs(?s,high) [-D] [-d]
- rankIs(?s,low) [-D] [+d]

Online and offline bridge: A recent Google project about mobile social networking, called Latitude, brings the benefits of sharing a location with an Android smartphone contact list (Google, 2013). In addition, android smartphone technology provides the ease of synchronizing a contact list with a Facebook profile. Thus, smartphone technology will be able to act as a communication-based, ad-hoc networking device to process information and offer it to one's personal life. Defeasible reasoning can play an important role in bringing the benefits of non-monotonic reasoning in the context of an intelligent environment in which information is naturally imperfect (Lam *et al*., 2012; Bikakis and Antoniou, 2011; Fong *et al*., 2012).

In our scheme, time and location which help recognize a user's mode in the offline social sphere, are two important defeaters of the NFO algorithm. That is, low-ranked edge stories would be favorable to appear in the "Top news" based on the user's mode. This provides the possibility of sharing in different dimensions, namely, time and location. Imagine users able to share a story with friends who are located at a university now (a subset of a university friend list) or a subset of family members who are at a party by selecting location of the party. The stories can be shared publicly but amongst people who are located in a specific time and place. Users typically are not interested in hearing from acquaintances except for stories that are shared from a fascinating location or at an important time. This brings time and location dimensions to both the audience selector and newsfeed adjustor. For instance, a faculty member who is in the user's acquaintance list may announce a story amongst students who currently are in the faculty:

R300: newsFeed(?f,?u,?s) := Edge Rank(?f,?u,?s), acquaintanceList(?f,?u), share Story From (?f,?s,? location, ?time), user(?u,? location, ?time)
R301: edgeRank(?f,?u,?s)
R302: acquaintanceList(?f,?u)
R303: shareStoryFrom(?f,?s,?location,?time)
R304: user(?u,? location,?time)
R300>R201

We know following rules from the past:

R31: edgeRank(?f,?u,?s):- NFO(?f,?u,?s)
R32: affinity(?f,?u,low) :- acquaintanceList(?f,?u)
R33: rankIs(?s,low) := affinity (?f,?u, low), shareStory (?f,?s)
R201: ¬newsFeed(?f,?u,?s) := edgeRank(?f,?u,?s), rankIs (?s,low)

The following results show that the shared story appears in the user's newsfeed (newsFeed(?f,?u,?s) [+d]) although the person who shared it is amongst acquaintance friend list:

- newsFeed(?f,?u,?s) [-D] [+d]
- ¬newsFeed(?f,?u,?s) [-D] [-d]

Smart friend lists and privacy: Facebook provides smart friend lists such as acquaintances, close friends and restricted peoplethat should be managed and updated by users and assigned privacy policy manually. In the literature review, we discussed previous study for automating smart friend lists based on data mining and classification, a learning system, neighborhood graphs, mobile technology and visualization techniques (Fang and LeFevre, 2010; Fortunato, 2010l; Lipford *et al*., 2010; Stutzman and Kramer-Duffield 2010; Ozenc and Farnham, 2011; Cheek and Shehab, 2012; Mazzia *et al*., 2012; Min *et al*., 2013). In a different view with previous mentioned techniques and compliant with our study, Governatori and Iannella (2011) used defeasible and deontic logic to augment the policy language for social network. They enriched the policy language called Open Digital Right Language (ODRL) with non-monotonic reasoning to bear conflicting and exceptional cases for Facebook and Flicker.

One of the most successful approaches to detect and classify life facet communities was suggested by Fang and LeFevre (2010), Mazzia *et al*. (2012). They argued rule-based privacy models are not comprehensive enough for users. They proposed a visualizing tool, called PViz, based on a user's Facebook neighborhood graph to detect communities and specify their access level. Figure 6 represents the community model of an actual Facebook user obtained at this study. In this figure, G1, G2 and G3 represent a user's communities and G20, G21 and G22 are sub-communities of G2. Blue points illustrate friends who are granted access to specific profile information and grey points are friends who are denied. As it is clear from the shape, the user privacy policy approach throughout each community follows a group-based mental model. Their model was based on group and single tasks to assign privacy to communities and individuals, respectively.

However, there are two main conflicting and ambiguous states in the introduced scheme. The first is an ambiguous state to partition a social network into communities. Illustrated in Fig. 6, this implies whether G2 should be divided into smaller communities-G20, G21 and G22-or not. They suggested the edge-betweenness algorithm accompanied with maximizing modularity (Newman and Girvan, 2004; Noack, 2009) to resolve the ambiguous state. And the second popular conflicting state occurs when a friend belongs to several communities with contradictory privacy policies. The single task is to resolve these conflicting states by asking users about those specific friends. However, this approach is not effective enough for cases in which a community contains several subsets (like G2) with contradictory privacy items. Regarding the defeasible logic notion, any subset community rule can defeat superset policy regulation because subset communities convey more details about community members.

In the following scenario we use grounded variables because we are talking about communities of a specific user not a global regulation. According to R400 and R401, if a user assigns a label to a community, then the system

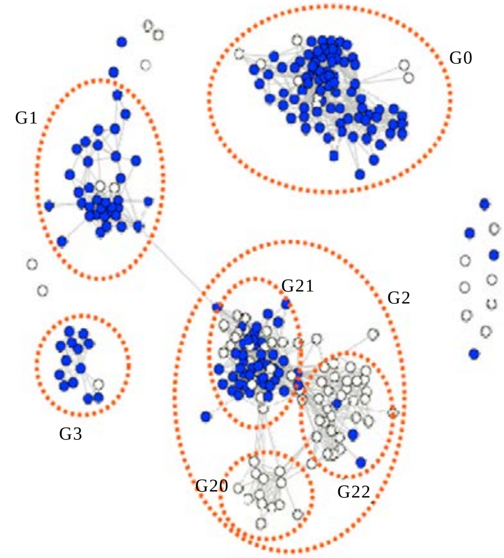

Fig. 6: Neighborhood graph of a user Facebook profile

tags community members accordingly. Imagine that G0, G1 and G2 are family, work and social communities, respectively. The social community, in turn, contains G20, G21 and G22 subsets that are a book club (e.g., Goodreads), classmates and tea party friend circles, respectively. In a group task, the user denies social community access to the wall posts shared by his or her friends (R409). However, he or she makes an exception for classmates (R410). R402 and R403 determine the relation between community and community member's access to the wall posts for social and classmate friend circles respectively, at which R403 is superior to R402. Based on defeasible logic intuition, we can always perceive that subset rules has higher priority than superset rules because contains more information about members.

R400: lable community(G2,L2) :- user lable community (G2,L2)
R401: tagMembers(m, L2) :- lable community(G2,L2), member(m,G2)
R402: ¬membersAccess(m,statusUpdates) := community access(G2,statusUpdates), member(m,G2)
R403: membersAccess(m,statusUpdates) := community access(G21,statusUpdates), member(m,G21)
R404: member(m,G2):- Subset(G21,G2), member(m,G21)
R407: subset(G21,G2)
R408: member(m,G21)
R409: ¬communityAccess(G2,statusUpdates)
R410: communityAccess(G21,statusUpdates)
R403>R402

The result implies that classmate community members grant access to a user's friend status updates while the social circle is denied.

- membersAccess(m,statusUpdates) [-D] [+d]
- ¬membersAccess(m,statusUpdates) [-D] [-d]

The discussed scenario was about two subset communities and does nothing for intersected communities as a whole. In this case, decision-making cannot be based simply on the presumed superiority of one community over another and must take other criteria into consideration. Simplicity is still an effective approach to resolving those privacy conflicts. However, the specific contribution of our approach is to resolve privacy conflicts at the community level and as a group task rather than as a single task and with individuals as friends. The strategy of maximum modularity resolves the ambiguous state of community division but leads to creating many specific, small-group communities, for which assigning all privacy options would be an arduous task. In our scheme, users could determine policy for a big superset community, then extract exceptional subset communities. Finally, we believe a defeasible rule-based system is one of the best compliant approaches to regulate and make decisions with a PViz comprehensive tool because some conflicts and exceptional cases are indispensable and the system should bear them, not wipe them out. Conflicting states of friends' access to profile information (like phone, email, political view, birthday, etc.) could be resolved by a single task while they are not removable in the case of shared posts such as status updates, videos and pictures. This type of conflict for friends belonging to more than one community stems from the dynamic characteristic of content sharing in Facebook and should be resolved based on user-focused sharing behavior.

CONCLUSION

In this study, we proposed a defeasible rule-based system to regulate Facebook routines. We showed how a defeasible agent is able to contribute to a newsfeed adjustor and audience selector in a focused sharing, dynamic, smart friend list and bridge online and offline social life with smartphone technology. In our scheme, the audience selector showed a flexible behavior based on a user's sharing approach to control the disclosure level between life facets communities. Defeasible regulation upon NFO addressed the invisibility threat and brought a user's mode into the feed decision-making process with assisting smartphone technology. Finally, we used the defeasible rule-based system to address contradictory states of the group-based privacy assignment. In summary, this study drew an outline for an agent-driven Facebook to make decisions based on classified data and user's preferences based on users' intuitive strategies for dealing with the site.

The limitation of the study was empirical studies about the contributions throughout prototyping and quantitative evaluation. However, the proposed framework aggregates the benefits of other evaluated approaches in an integrated, mature, rule-based system that sometimes may not happen in the absence of non-monotonic reasoning. Another shortcoming of the study was the SPINdle reasoner and its extension toward predicate logic, list processing and object orientation to recognize the RDF axiomatic in semantic technology. Although, the outputs were converted into the D-RuleML 1.0 format, input scenarios were prolog based and provided by human assistant.

In future study, we are planning to deploy a prototype of the proposed framework based on the neighborhood graph and inheritance network knowledge representation on an actual Facebook user's profile. This work was based on a data-driven defeasible reasoner that will be extended toward integrated defeasible reasoning to retrieve goal-driven information in a query-base defeasible reasoner like DR-DEVICE which brings a more advanced contribution regarding smartphone technology and social networking in an ambient intelligent environment. The SPINdle reasoner also should be extended toward supporting list processing for dealing with sets and set operations.

ACKNOWLEDGMENT

Special thanks goes to Professors Governatori and Boley for their precious advises and suggestions for enhancing SPINdle reasoner and extending it towards semantic web technology. This study is funded under grant LRGS/TD/2011/UITM/ICT/01/02 and FRGS/2/2013/ICT02/UKM/02/2 by National University of Malaysia.

REFERENCES

Alexa, 2013. Top sites 2013. http://www.alexa.com/topsites.

Antonelli, G.A., 2010. Non-monotonic logic. The Stanford Encyclopedia of Philosophy, April 14, 2010. http://plato.stanford.edu/entries/logic-nonmonotonic/.

Antoniou, G., D. Billington, G. Governatori and M.J. Maher, 2001. Representation results for defeasible logic. ACM Trans. Comput. Logic, 2: 255-287.

Bassiliades, N., G. Governatori, B. Grosof, G. Antoniou and A. Paschke *et al*., 2013. Schema specification of defeasible RuleML version 1.0. http://ruleml.org/1.0/defeasible/defeasible.html.

Bikakis, A. and G. Antoniou, 2011. Contextual defeasible logic and its application to ambient intelligence. IEEE Trans. Syst. Man Cybernetics A: Syst. Hum., 41: 705-716.

Billington, D., K. De Coster and D. Nute, 1990. A modular translation from defeasible nets to defeasible logics. J. Exp. Theor. Artif. Intell., 2: 151-177.

Bucher, T., 2012. Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. New Media Soc., 14: 1164-1180.

Cheek, G.P. and M. Shehab, 2012. Policy-by-example for online social netstudy. Proceedings of the 17th ACM symposium on Access Control Models and Technologies, June 20- 22, 2012, Newark, New Jersey, USA., pp: 23-32.

Debatin, B., J.P. Lovejoy, A.K Horn and B.N. Hughes, 2009. Facebook and online privacy: Attitudes, behaviors and unintended consequences. J. Comput. Mediated Commun., 15: 83-108.

Ellison, N.B., 2007. Social network sites: Definition, history and scholarship. J. Comput. Mediated Commun., 13: 210-230.

Ellison, N.B., C. Steinfield and C. Lampe, 2007. The benefits of Facebook friends: Social capital and college students use of online social network sites. J. Comput. Mediated Commun., 12: 1143-1168.

Ellison, N.B., C. Steinfield and C. Lampe, 2011a. Connection strategies: Social capital implications of Facebook-enabled communication practices. New Media Soc., 13: 873-892.

Ellison, N.B., J. Vitak, C. Steinfield, R. Gray and C. Lampe, 2011b. Negotiating Privacy Concerns and Social Capital Needs in a Social Media Environment. In: Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web, Trepte, S. and L. Reinecke (Eds.). Chapter 3, Springer, New York, USA., ISBN: 9783642215209, pp: 19-32.

Facebook, 2013a. Facebook news press. http://newsroom.fb.com/.

Facebook, 2013b. Facebook reports first quarter 2013 results. http://investor.fb.com/releasedetail.cfm?ReleaseID=761090.

Fang, F. and K. LeFevre, 2010. Privacy wizards for social networking sites. Proceedings of the 19th International Conference on World Wide Web, April 26-30, 2010, Raleigh, NC., USA., pp: 351-360.

Farnham, S.D. and E.F. Churchill, 2011. Faceted identity, faceted lives: Social and technical issues with being yourself online. Proceedings of the ACM 2011 Conference on Computer Supported Cooperative Work, March 19-23, 2011, Hangazu, China, pp:359-368.

Fong, J., H.P. Lam, R. Robinson and J. Indulska, 2012. Defeasible preferences for intelligible pervasive applications to enhance eldercare. Proceedings of the IEEE International Conference on Pervasive Computing and Communications Studyhops, March 19-23, 2012, Lugano, Switzerland, pp: 572-577.

Fortunato, S., 2010. Community detection in graphs. Phys. Rep., 486: 75-174.

Google, 2013. Latitude 2013. http://google.about.com/od/mapsanddirections/p/Latitude_WhatIs.htm.

Governatori, G. and R. Iannella, 2011. A modelling and reasoning framework for social netstudy policies. Enterprise Inform. Syst., 5: 145-167.

Haythornthwaite, C., 2005. Social netstudy and Internet connectivity effects. Inform. Commun. Soc., 8: 125-147.

Horty, J.F., R.H. Thomason and D.S. Touretzky, 1990. A skeptical theory of inheritance in nonmonotonic semantic netstudy. Artif. Intell., 42: 311-348.

Kairam, S., M. Brzozowski, D. Huffaker and E. Chi, 2012. Talking in circles: Selective sharing in google+. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 5-10, 2012, Austin, Texas, USA., pp: 1065-1074.

Lam, H.P. and G. Governatori, 2009. The making of SPINdle. Proceedings of the International Symposium on Rule Interchange and Applications, November 5-7, 2009, Las Vegas, NV., USA., pp: 315-322.

Lam, H.P., G. Governatori, K. Satoh and H. Hosobe, 2012. Distributed Defeasible Speculative Reasoning in Ambient Environment. In: Computational Logic in Multi-Agent Systems, Fisher, M., L. van der Torre, M. Dastani and G. Governatori (Eds.). Springer, Berlin, Heidelberg, pp: 43-60.

Lampe, C., N. Ellison and C. Steinfield, 2006. A face(book) in the crowd: Social searching vs. social browsing. Proceedings of the 20th Anniversary Conference on Computer Supported Cooperative Work, November 4-8, 2006, Banff, Alberta, Canada, pp: 167-170.

Lampe, C.A.C., N. Ellison and C. Steinfield, 2007. A familiar face(book): Profile elements as signals in an online social network. Proceedings of the SIGCHI Conference On Human Factors In Computing Systems, April 28-May 3, 2007, San Jose, CA., USA., pp: 435-444.

Lipford, H.R., A. Besmer and J. Watson, 2008. Understanding privacy settings in facebook with an audience view. Proceedings of the 1st Conference on Usability, Psychology and Security, April 14, 2008, San Francisco, CA., USA., pp: 1-8.

Lipford, H.R., J. Watson, M. Whitney, K. Froiland and R.W. Reeder, 2010. Visual vs. compact: A comparison of privacy policy interfaces. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 10-15, 2010, Atlanta, GA., USA., pp: 1111-1114.

Maher, M.J., 2001. Propositional defeasible logic has linear complexity. Theor. Pract. Logic Prog., 1: 691-711.

Maher, M.J., 2002. A model-theoretic semantics for defeasible logic. Proceedings of the Paraconsistent Computational Logic, July 27, 2002, Copenhagen, Denmark..

Marlow, C., 2009. Maintained relationships on facebook. March 9, 2009. http://www.facebook.com/note.php?vnote_id=55257228858&id=8394258414&ref=nf.

Mazzia, A., K. LeFevre and E. Adar, 2012. The PViz comprehension tool for social network privacy settings. Proceedings of the 8th Symposium on Usable Privacy and Security, July 11-13, 2012, Washington, DC., USA.

Min, J.K., J.Wiese, J.I. Hong and J. Zimmerman, 2013. Mining smartphone data to classify life-facets of social relationships. Proceedings of the Conference on Computer Supported Cooperative Work, February 23-27, 2013, San Antonio, Texas, USA., pp: 285-294.

Newman, M.E.J. and M. Girvan, 2004. Finding and evaluating community structure in netstudy. Phys. Rev. E, Vol. 69, 10.1103/PhysRevE.69.026113

Noack, A., 2009. Modularity clustering is force-directed layout.Phys.Rev.E,Vol.7910.1103/PhysRevE.79. 02 61 02

Nute, D., 2001. Defeasible Logic. In: Web Knowledge Management and Decision Support, Bartenstein, O., U. Geske, M. Hannebauer and O. Yoshie (Eds.). Springer, Berlin, Heidelberg, ISBN-13: 9783540006800, pp: 151-169.

Ozenc, F.K. and S.D. Farnham, 2011. Life modes in social media. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, May 7-12, 2011, Vancouver, BC., Canada, pp: 561-570.

Paek, T., M. Gamon, S. Counts, D.M. Chickering and A. Dhesi, 2010. Predicting the importance of newsfeed posts and social network friends. Proceedings of the 24th AAAI Conference on Artificial Intelligence, July 11-15, 2010, Atlanta, GA., USA., pp: 1419-1424.

Pak, A. and P. Paroubek, 2010. Twitter as a corpus for sentiment analysis and opinion mining. Proceedings of the 7th Conference on International Language Resources and Evaluation, May 17-23, 2010, Valletta, Malta, pp: 1320-1326.

Peluchette, J.V.E., K. Karl and J. Fertig, 2013. A Facebook 'friend' request from the boss: Too close for comfort? Bus. Horizons, 56: 291-300.

Privacy International, 2007. A race to the bottom: Privacy rankings of Internet service companies. Consultation Report, Privacy International, June 9, 2007.

Stutzman, F. and J. Kramer-Duffield, 2010. Friends only: Examining a privacy-enhancing behavior in facebook. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, April 10-15, 2010, Atlanta, GA., USA., pp: 1553-1562.

Stutzman, F., J. Vitak, N.B. Ellison, R. Gray and C. Lampe, 2012. Privacy in interaction: Exploring disclosure and social capital in facebook. Proceedings of the 6th International Conference on Weblogs and Social Media, June 4-7, 2012, Dublin, Ireland, pp: 330-337.

Vitak, J. and N.B. Ellison, 2012. There's a network out there you might as well tap: Exploring the benefits of and barriers to exchanging informational and support-based resources on Facebook. New Media Soc., 15: 243-259.

Vitak, J., C. Lampe, R. Gray and N.B. Ellison, 2012. Why won't you be my Facebook friend?: Strategies for managing context collapse in the workplace. Proceedings of the iConference, February 7-10, 2012, Toronto, Ontario, Canada., pp: 555-557.