Towards an Argumentation System for Assisting Users with Privacy Management in Online Social Networks

Ramon Ruiz-Dolz[0000-0002-3059-8520], Stella Heras[0000-0001-6212-9377], Jose Alemany, and Ana Garcia-Fornes[0000-0003-4482-8793]

Departament de Sistemes Informàtics y Computació
Universitat Politècnica de València
Camino de Vera s/n. 46022 Valencia (Spain)
{raruidol, sheras, jalemany1, agarcia}@dsic.upv.es

Abstract. In this paper, we present an argumentation system for supporting users of online social networks on their decision making. The purpose of the argumentation system is to give a reasoned recommendation to a specific user on whether he/she should or should not perform an action in the social network (e.g. post a comment, share a photo) taking into account his/her privacy preferences. We both define the argumentation framework and the architecture of the argumentation system. Finally, we illustrate the system with a practical example in a pedagogic social network.

Keywords: Argumentation · Persuasion · Social Networks · Privacy · Security

1 Introduction

One of the most concerning dangers of the last years is the unconscious sharing of sensitive information in online social networks (OSN). The main purpose of this work is to define the basis of an argumentation system that detects when sensitive data is being published, and persuades users to modify the content of the publication. Two main types of privacy threats can happen in an OSN. An indirect threat may occur when a user makes a publication involving other users in the post. It is possible that this publication violates the privacy policy of any of its members. On the other hand, a direct threat happens when the author of the publication violates its own privacy preferences. Even though this may seem incoherent, it is a usual threat in OSNs, since users commonly interact disregarding what they share or with who they share sensitive information. Our argumentation system can deal with both types of threat, and can help to minimise the number of undesired publications of sensitive data.

This paper is structured as follows, in section 2 we briefly survey related work; in section 3 we define our argumentation system; in section 4, we propose an example of use of the system; finally, in section 5 we summarise the conclusions and our future lines of work.

2 Related work

Arguing is the natural way for humans to explain themselves to resolve disputes and reach agreements. Thus, computational argumentation is a powerful tool that allows intelligent systems that interact with humans to generate arguments to explain their behaviour and hence, persuade their users to accept it (e.g. decisions, recommendations). In the specific domain of OSN, computational argumentation can help to structure user opinions and enhance dialogues [9], to model the dialogue between users that share their recommendations in the network [10] or to prevent users from unconsciously compromise their privacy or that of others [18].

By being able to generate persuasive arguments and engage with the user in a persuasion dialogue, the OSN can warn users of the implications and consequences of their actions. Therefore, we can find in the literature recent research that follows this trend and applies computational argumentation techniques in the context of preserving the users' privacy in this type of networks. For instance, in [11] authors propose an assumption-based argumentation model that allows agents representing users in a social network to argue and decide whether a content should be shared or not. To generate arguments, agents make use of semantic rules that represent their users' privacy constraints. In this work, authors assume that an agent is aware of the semantic rules of its user. However, our system is able to automatically generate arguments by using the users' information gathered from the social network.

A similar work [7] applied the theory of argumentation schemes to negotiate with users the setting of a privacy preference, thus managing multiparty privacy conflicts based on logical arguments. Users employ arguments to convince the other parties that their demands are reasonable and should be taken into account. However, this work is centred on presenting the theoretical model, but it does not specify how arguments are actually generated and evaluated. In a subsequent work [6], authors proposed a novel model for representing and reasoning about multiparty privacy conflicts by using contextual factors, user preferences, and user arguments. Here, argumentation is conceived as in internal process by which agents can resolve privacy disputes once this problem occurs, but not as a persuasion tool that the system may use to interact with the user to help him/her to make good decisions and avoid privacy conflicts.

3 Argumentation system

In this section, we define our argumentation system as an educational tool to preserve the privacy of the users of an OSN. To this end, we assume that the system operates in a OSN that includes the common features of this type of networks (e.g. user information and preferences, friends, groups, privacy configuration) and that allows users to perform common social actions (e.g. posting a comment, sharing a photo) [16].

3.1 Framework formalisation

Our Argumentation Framework is based on Quantitative Bipolar Argumentation Frameworks [2].

Definition 1 (Argumentation Framework for Online Social Networks). *We define an argumentation framework for online social networks as a tuple* $AFOSN = <A, R, P, \tau_p>$ *where:* A *is a set of* n *arguments* $[\alpha_0, \ldots, \alpha_n]$*;* R *is the attack relation on* A *such as* $A \times A \rightarrow R$*;* P *is the list of* e *profiles involved in an argumentation process* $[p_0, \ldots, p_e]$*; and* τ_p *is a function* $A \times P \rightarrow [0, \ldots, 1]$ *that determines the score of an argument* α *for a given profile* p*.*

In our framework, each individual argument $\alpha = (\beta, T, D)$ is defined by three parameters. β is the *claim* or bias of the argument. It is represented as a binary variable that determines whether an argument acts in favour or against performing an action in the social network. T is the label of the argument, which represents the four different types of arguments that can be generated by our argumentation system: Privacy, Trust, Risk and Content arguments. Finally, D is the *support* of the argument. This parameter consists of a value derived from all the information gathered from the social network in order to infer the *claim* of a determined type of argument, and hence depends on the type of argument.

Each relationship $r = (\alpha_i, \alpha_j)$ represents an attack from α_i towards α_j. As proposed in [12] and [13], a *rebuttal* attack occurs when an argument invalidates other argument's *claim* (e.g. α_1 = (-1, T_1, D_1) *rebuts* α_2 = (+1, T_2, D_2) and vice versa). On the other hand, an *undercut* attack is carried out when an argument's *claim* invalidates other argument's *support.* The internal argumentation process performed by our system to generate the *acceptable* arguments for a particular conflict in the OSN only allows *rebuttal* attacks. In the human interactive argumentation process carried out by our dialogue module both types of attacks will be considered.

Regarding the user profile, we define $p = (\nu,\rho,M)$ as the combination of the preference values ν, the personality ρ and a list of miscellaneous information M.

The preference values ν is a vector containing the preferences that each user has towards a concrete value that the arguments of our system may promote [3]. We propose the following preferences based on [15] to be considered in our system: *Privacy/Popularity*, *Closeness/Openness*, *Flexibility/Intransigence* and *Content Sensitivity.* The first three bipolar preferences $P/\overline{P}$, are defined as a value v in the [0,1] range, being v the value assigned to P and (1 - v) to $\overline{P}$. Therefore, a user profile with *Privacy/Popularity* = 0.2 would have a 0.2 preference for Privacy and (1 - 0.2) preference for Popularity. The *Content Sensitivity* preference is defined as a value v in the range [0, 1] being 1 the maximum concern about the content sensitivity and 0 if the user does not really care about this preference. This value is calculated as the average of the 6 different types of content considered in this work.

The personality of a user profile ρ is a 5 dimension vector that models the personality of a specific user based on the five parameters proposed in [14]. The personality dimensions taken into account are the *Openness*, *Conscientiousness*, *Extraversion*, *Agreeableness* and *Neuroticism*. Here we assume that this information is available since users of the network have undertaken a personality test or else, that these dimensions can be automatically determined by the activities of the user in the social network [8].

The last part of the user definition (M) is a set of general information extracted from a specific user profile such as the age, location, likes, etc.

Finally, we define the scoring function τ_p as the function that takes an argument and a profile as input and determines the value of the argument in the context of a specific user profile. In order to obtain this score, function τ_p is defined as,

$$\tau_p(\alpha, p) = \alpha_\beta \cdot \alpha_D \cdot p_\nu \tag{1}$$

Thus, the score of an argument for a specific user profile is basically the product of the *support* value of the argument, the preference value that promotes the argument and the bias of that argument.

Definition 2 (Defeat). *An argument $\alpha_i \in A$ defeats another argument $\alpha_j \in A$ in a context determined by a user profile p iff $(\alpha_i, \alpha_j) \in R \wedge |\tau_p(\alpha_i, p)| > |\tau_p(\alpha_j, p)|$.*

Then, we can define $defeat_p(\alpha_i, \alpha_j)$ if there exists an attack relationship between both arguments and the score of the argument α_i is higher than the score of the argument α_j. It means that the argument α_i is promoting a value that is preferred by the user that receives the argument.

Definition 3 (Acceptability). *An argument $\alpha_i \in A$ is acceptable in a context determined by a user profile p iff $\forall\ \alpha_j \in A \wedge defeat_p(\alpha_j, \alpha_i) \rightarrow \exists \alpha_k \in A \wedge defeat_p(\alpha_k, \alpha_j)$.*

In other words, an argument is acceptable if there are no other undefeated arguments attacking it.

3.2 System architecture

An argumentative process is defined by the achievement of four main tasks: identification, analysis, evaluation and invention [17]. Our system, graphically depicted in Figure 1 consists of four different modules designed to perform all these essential tasks.

Feature extraction module. This module is in charge of obtaining all the relevant information for our framework directly from the OSN. The information obtained by this module will be used to model user profiles and to get the parameters that will define an argument in our system.

The main purpose of modelling user profiles is to be able to learn which arguments are more persuasive to what type of user. Since one of our goals is to maximise the persuasion of our system, by defining a set of user profiles it is

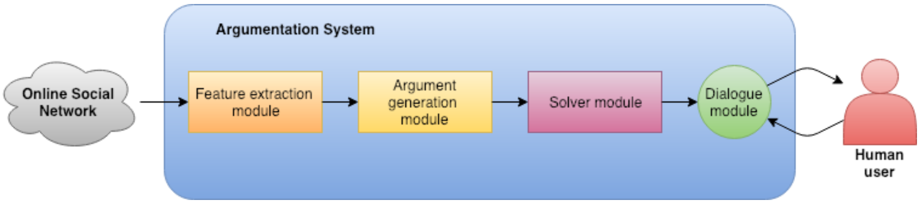

Fig. 1. Architecture of the argumentation system.

possible to do a generalisation of that problem depending on the user's activity in the social network. The information extracted to define the profiles of users is obtained basically from three sources: the privacy configuration, the personality analysis and the miscellaneous information.

From the **privacy configuration** of each user is possible to define a privacy value that characterises him/her. Usually, a social network user defines some privacy parameters when registering. Those parameters are the profile visibility (e.g. public, friends, private) and the default target of his/her publications (e.g. public, friends, group, private). With the use of the OSN this information can be updated in order to accurately model the privacy preferences of the users.

For the **personality analysis**, as pointed out before, the users' personality can be obtained either with a survey or by analysing users activity and interactions, considering the big five model [14].

Finally, when creating a profile in a social network some personal information is added by the user (e.g. the age, the location, the likes). All this data can also be extracted to generate the user profiles for our system. Concretely, the **miscellaneous information** can be useful to determine the differences between two different user profiles.

Apart from the users profile information, the feature extraction module also obtains the parameters required to generate arguments in our system. Those parameters are mainly divided into three types: the trust, the Privacy Risk Score and the content features.

Trust is commonly understood as a way to measure the strength of a tie in a social network. In order to formally define the trust metric we can assume a directed graph $G_t = (N, E)$ that represents the topology of the OSN. Let $N = \{i \in \{1, \ldots, |N|\}\}$ be the set of nodes where i represents a user, and $E = \{(i, j) \in N \times N\ \}$ be the set of edges representing an existing relationship from i towards j. Therefore, the trust value $t_{i,j}$ indicates the strength of the tie that links user i with user j. It is important to emphasise that, since one of the main properties of trust is bidirectionality, the value of $t_{i,j}$ may differ from $t_{j,i}$.

Another important parameter that the system extracts from the network usage is the **Privacy Risk Score** (PRS). Proposed in [1], PRS is an alternative way to measure the reachability of a specific user in the social network. Therefore, the PRS provides information of the risk of sharing a determined information to non-desired users.

The third parameter used in our model to build arguments is the result of analysing the own content of the publication. The **content features** can come from two main sources: the text from the publications, and the images uploaded. We have defined the following classes of sensitive information considering the ones proposed in [4]:

- **Location**: information that reveals the location of any user involved in the interaction.
- **Medical**: information that reveals the medical condition of any user involved in the interaction.
- **Drug**: information that reveals the use of any kind of drugs.
- **Personal**: information that reveals any kind of personal information. From the sexual orientation or the job, to more identifiable information as the credit card number, the address or the birth date of any user involved in the interaction.
- **Family/Association**: information that reveals the user's family members or their associations.
- **Political**: information that reveals political orientation or any kind of ideological content.

The feature extraction module must determine whether a publication contains any sensitive information or not, and classify its content in any of those classes.

Argument generation module. The argument generation module processes all the information gathered by the feature extraction module in order to create abstract arguments following the guidelines of the argumentation framework. This module generates four different types of arguments based on the type of information extracted from the OSN:

- **Privacy Arguments**. This class of arguments emphasise on privacy vulnerabilities. The argumentation system is able to create privacy arguments with the data obtained from the user profile modelling. The argument is generated by computing the distance between the privacy configuration of the user and the privacy configuration of the publication. If the distance does not surpass a predefined threshold, the argument will have a positive bias. On the other hand, if it surpasses the threshold the bias of the argument will be negative. Let us assume for example, a user profile with a very restrictive privacy configuration. If that user tries to make a publication containing personal information and sharing it with all the network, the argumentation system will create a set of arguments regarding the privacy incoherence between the user profile and the action being done. Therefore, the main feature to generate privacy arguments is the privacy configuration vector of each user.
- **Trust Arguments**. Since the purpose of an OSN is to interact with other users, it is a very common situation when a user involves other users with its

actions. An effective way to handle those privacy conflicts is to generate trust arguments. An argument of trust contains all the information extracted from the social network relative to the strength of the ties between users. These arguments are generated from the trust computed with the information from the feature extraction module. Concretely, if trust from users involved in the publication towards the user making the publication is not enough (i.e. does not surpass an established threshold), an argument of trust against performing the action will be generated.

- **Risk Arguments**. When making a publication, it is impossible for the author to estimate how many users will be able to reach the information being published. Risk arguments are generated in order to warn the user about the risk of the publication being read by any undesired user of the network. The main feature used to generate arguments of this type is the PRS, since the own metric is a risk indicator. Having a high risk value will make the system generate an argument of risk against making the publication.
- **Content Arguments**. Content arguments are generated from the data obtained by the content features analyser. Therefore, there can be as many content arguments as classes of content defined before. In addition, depending on the user personality and privacy configuration some types of content arguments may be more or less persuasive. Let us suppose that there is a user that usually shares political information on his/her posts. To warn that user of the risks of sharing political information may have no sense. But, we will now assume that he/she makes a post containing some sensitive medical information. In this case the system will detect the risk and start an argumentation process in order to warn the user of the risk of making the medical information public.

The output of this module is an argumentation graph $G_a = (A, R)$ where arguments are the set of nodes $A = \{\ \alpha \in \{1, \ldots, |A|\}\}$ where each α is an argument, and edges are the relationships $R = \{(i, j) \in A \times A\}$, where argument i attacks argument j. Therefore, once the set of arguments is generated, the module also creates the relationships between arguments.

In our argumentation framework, a relationship between arguments is defined by the attack relation. To determine if there exist an attack relationship between two different arguments, the parameter *bias* is used. An argument positively biased and an argument negatively biased are both attacking each other by definition.

Solver module. The solver module of our argumentation system performs the task of evaluating the argumentation graph. To solve our argumentation graph, the function τ_p is applied to the set of arguments generated and the profiles involved in the argumentation process. Finally, all the scores are added and the system checks whether the result score is positive or negative to decide the set of *acceptable* arguments. If the result is positive, there are no reasons to persuade the user on modifying his/her action. On the other hand, if the result is negative, the system keeps all the negative biased arguments and sorts them by their score in order to try to persuade the user to modify his/her action.

Dialogue module. The purpose of this module is to handle the communication between the argumentation system and the human user. This module receives the set of A *acceptable* arguments and an argumentation strategy π_a. We define an argumentation strategy as the policy (order to present the arguments) that an argumentation agent adopts when facing an *opponent* (either human or agent). The dialogue module uses each argument $\alpha_n \in A$ following the strategy π_a in order to persuade the user to modify his/her action. The definition of concrete argumentation strategies remains future work.

4 System Operation

In this section, we provide an example on how our argumentation system can be implemented in a specific OSN to serve as an educational tool to help the users of the network to preserve their privacy.

4.1 Pesedia: raising awareness of privacy risks in OSNs

Pesedia is an OSN for educational and research purposes that includes: (i) the design and development of new metrics to analyze and quantify privacy risks [1]; (ii) the application of methods to change users' behaviour regarding their privacy concerns; (iii) the implementation of new features to improve the management of users' content; (iv) and the evaluation and testing of new proposals with real users.

The underlying implementation of Pesedia uses Elgg [5], which is an open source engine that is used to build social environments. The environment provided by this engine is similar to other social networks (e.g. Facebook). The Pesedia architecture has two main components: the *Platform Layer* and the *User Layer*. The *Platform Layer* is the core of the architecture. This layer contains the *Social Network Services*, which provide the main functionality of the social network, and the *Storage System*, which provides persistent storage of all of the information generated in the social network. Among other modules, the Social Network Services include the module which deploy the argumentation system proposed in this work. The *User Layer* is in charge of managing information associated to each user. This information is divided into three categories: contacts (grouped or non-grouped); information (e.g., profile items, publications); and settings, which are mainly focused on privacy settings, such as privacy policies and privacy thresholds.

4.2 Usage example

As mentioned before, a multiparty privacy conflict (MPPC) may happen when multiple users are tagged in the same post or photo. The most common reason for this type of conflicts are the differences between privacy policies of the users that appear in the publication. We will now assume that a MPPC occurs in Pesedia in order to give an example of how our argumentation system would behave.

Thus, let us assume that user *Alice* wants to upload a photo to Pesedia where also appears user *Bob*. Based on the features obtained by the feature extraction module, the system will determine the profile information of both users as can be seen in Table 1. In this example, user Alice main preferences regarding contents are: Location(0.3), Medical(1.0), Drugs(0.8), Personal(0.5), Family/Asociation(0.6) and Political(0.9). Meaning that when higher the value, user Alice does less publications with that content. Values vector indicates that Alice gives the values: privacy(0.3), popularity(1-0.3), closeness(0.5), openness(1-0.5), flexibility(0.5), intransigence(1-0.5) and the content of the publications(0.68). These values allow us to order the priorities of the users so that we can determine the scores of the arguments for a given user. In this case, the values of popularity, closeness and the content sensitivity are the preferred values for Alice, so arguments regarding these issues will be more *effective* than others. Finally the personality vector makes possible to model the user. In this example, Openness(0.2), Conscientiousness(0.6), Extraversion(0.1), Agreableness(0.7), Neuroticism(0.5); Alice can be seen as an introverted user (0.1 in extraversion) among other parameters. This same analysis can be made equivalently with user Bob in this example.

	Alice	**Bob**
Content preferences	[0.3,1.0,0.8,0.5,0.6,0.9]	[0.1,0.7,0.9,0.4,0.6,0.3]
Values	[0.3,0.5,0.5,0.68]	[0.9,0.7,0.7,0.56]
Personality	[0.2,0.6,0.1,0.7,0.5]	[0.7,0.8,0.6,0.5,0.3]
Information	[21,"Aachen"]	[23, "Brussels"]

Table 1. User profile features

The module will also obtain the most important features of the content of the post. Alice shares a photo where location and personal information is revealed, and selects her friends as the audience to share the photo. As two users appear in the post, the system also computes the trust between them in both directions. In this example, the following trust values are considered: $t_{Alice \to Bob} = 0.6$ and $t_{Bob \to Alice} = 0.3$; meaning that Alice tie strength towards Bob is considerably higher than the inverse tie. Taking into account both profiles and publication features, the argument generation module generates the following set of arguments:

A = \{α_1(-1, $Trust$, LO(0.3)), α_2(+1, $Privacy_A$, OK(0), α_3(-1, $Privacy_B$, ER(0.4)), α_4(+1, $Risk_A$, LO(0.23)), α_5(-1, $Risk_B$, HI(0.78)), α_6(-1, $Content_A$, Location(0.4)),α_7(+1, $Content_A$, Medical(0)), α_8(+1, $Content_A$, Drug(0)), α_9(-1, $Content_A$, Personal(0.6)), α_{10}(+1, $Content_A$, Family(0)), α_{11}(+1, $Content_A$, Political(0)), α_{12}(-1, $Content_B$, Location(0.4)), α_{13}(+1, $Content_B$, Medical(0)), α_{14}(+1, $Content_B$, Drug(0)), α_{15}(-1, $Content_B$, Personal(0.6)), α_{16}(+1, $Content_B$, Family(0)), α_{17}(+1, $Content_B$, Political(0))\}

The set of arguments generated contain arguments from all the four types existing in our system. It is also possible to observe how, when more than a user is involved in an argumentation process, some arguments are duplicated taking into account all the different user profile features. Once all the arguments are generated, the argument generation module also creates the argumentation graph depicted in Figure 2. The graph generated is a bipartite graph on which two different sets can be seen. A set with the arguments against making the publication (top) and a set supporting the action of making the publication (down).

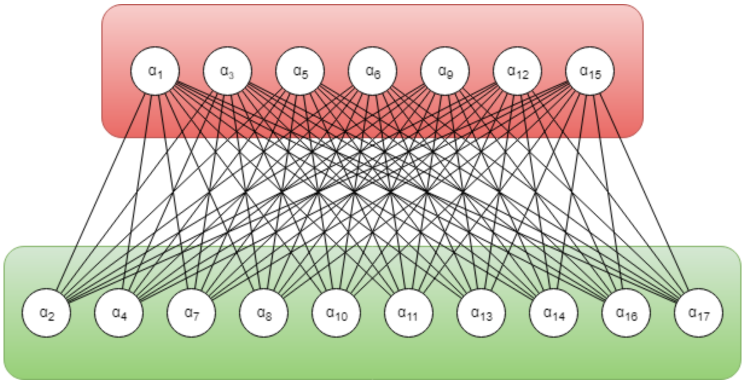

Fig. 2. Argumentation graph built from the set of arguments generated.

The solver module receives the graph generated by the argument generation module and proceeds with the argument evaluation by applying the score function to each argument and profile involved in the process. The results of the evaluation can be observed in Table 2.

The result of aggregating all those values is -1.6 meaning that the module will infer that the action entails some risks for both users involved in the publication. Therefore, the dialogue module will receive the set of negative biased arguments. They will be used following a persuasion policy π_{Alice} in order to maximise the persuasion for that concrete user. Even though the design of the dialogue module is still future work, we would like to illustrate how arguments will be seen by human users in order to clearly distinguish between the shape of arguments in the internal computation and the dialogue phase. It is important

Argument	**Value**	**Argument**	**Value**	**Argument**	**Value**	**Argument**	**Value**
α_1	-0.21	α_6	-0.12	α_{11}	0	α_{16}	0
α_2	0.3	α_7	0	α_{12}	-0.04	α_{17}	0
α_3	-0.36	α_8	0	α_{13}	0		
α_4	0.07	α_9	-0.3	α_{14}	0		
α_5	-0.7	α_{10}	0	α_{15}	-0.24		

Table 2. Score obtained by each argument.

to remark that, although the system has information regarding both users Alice and Bob, the dialogue phase will only be performed with the author of the publication, Alice in this case. Therefore, sensitive data regarding other users in the publication will never be revealed. Let's take into account the argument α_{15}, an argument against making the publication, based on Bob's personal content sensitivity. The dialogue module will translate the argument from its computational shape (-1, $Content_B$, Personal(0.6)) to a human readable text like ”*It is highly recommended not to make this publication since it may infringe Bob's content privacy preferences, please consider to modify the content of the publication or to get Bob's approval before making the publication.*" where no specific sensitive details of privacy preferences of other users are revealed.

5 Discussion

In this paper we have proposed an argumentation system to handle privacy threats and assist users in online social networks. We have formally defined the argumentation framework and the architecture of our system. In order to demonstrate its operation, we have presented an usage example, where we illustrate how the arguments are generated and how our system solves the underlying argumentation graph.

As future work, we plan to completely integrate the proposed argumentation system in the Pesedia network, and therefore raise awareness of the privacy issues for the network users. We also plan to develop a chatbot to manage the dialogue module of our system. We will implement a model based on reinforcement learning able to learn argumentation strategies in order to improve the persuasive efficiency of the system.

6 Acknowledgements

This work is partially supported by the Spanish Government project TIN2017-89156-R, the Valencian Government project PROMETEO/2018/002, the FPI grant BES-2015-074498 and the grant program for the recruitment of doctors for the Spanish system of science and technology (PAID-10-14) of the Universitat Politècnica de València.

References

1. Alemany, J., del Val, E., Alberola, J., García-Fornes, A.: Estimation of privacy risk through centrality metrics. Future Generation Computer Systems **82**, 63–76 (2018)
2. Baroni, P., Rago, A., Toni, F.: How many properties do we need for gradual argumentation? AAAI (2018)
3. Bench-Capon, T.: Value based argumentation frameworks. arXiv preprint cs/0207059 (2002)
4. Caliskan Islam, A., Walsh, J., Greenstadt, R.: Privacy detective: Detecting private information and collective privacy behavior in a large social network. In: Proceedings of the 13th Workshop on Privacy in the Electronic Society. pp. 35–46. ACM (2014)
5. Costello, C.: Elgg 1.8 social networking. Packt Publishing Ltd (2012)
6. Fogues, R.L., Murukannaiah, P.K., Such, J.M., Singh, M.P.: Sharing policies in multiuser privacy scenarios: Incorporating context, preferences, and arguments in decision making. ACM Transactions on Computer-Human Interaction (TOCHI) **24**(1), 5 (2017)
7. Fogues, R.L., Murukanniah, P., Such, J.M., Espinosa, A., Garcia-Fornes, A., Singh, M.: Argumentation for multi-party privacy management (2015)
8. Golbeck, J., Robles, C., Turner, K.: Predicting personality with social media. In: CHI'11 extended abstracts on human factors in computing systems. pp. 253–262. ACM (2011)
9. Heras, S., Atkinson, K., Botti, V., Grasso, F., Julián, V., McBurney, P.: Research opportunities for argumentation in social networks. Artificial Intelligence Review **39**(1), 39–62 (2013)
10. Heras, S., Rebollo, M., Julián, V.: A dialogue game protocol for recommendation in social networks. In: International Workshop on Hybrid Artificial Intelligence Systems. pp. 515–522. Springer (2008)
11. Kökciyan, N., Yaglikci, N., Yolum, P.: An argumentation approach for resolving privacy disputes in online social networks. ACM Transactions on Internet Technology (TOIT) **17**(3), 27 (2017)
12. Nute, D.: Defeasible logic. In: International Conference on Applications of Prolog. pp. 151–169. Springer (2001)
13. Prakken, H., Sartor, G.: A dialectical model of assessing conflicting arguments in legal reasoning. In: Logical models of legal argumentation, pp. 175–211. Springer (1996)
14. Rothmann, S., Coetzer, E.P.: The big five personality dimensions and job performance. SA Journal of Industrial Psychology **29**(1), 68–74 (2003)
15. Schwartz, S.H.: An overview of the schwartz theory of basic values. Online readings in Psychology and Culture **2**(1), 11 (2012)
16. Subrahmanyam, K., Reich, S.M., Waechter, N., Espinoza, G.: Online and offline social networks: Use of social networking sites by emerging adults. Journal of applied developmental psychology **29**(6), 420–433 (2008)
17. Walton, D.: Argumentation theory: A very short introduction. In: Argumentation in artificial intelligence, pp. 1–22. Springer (2009)
18. Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P.G., Cranor, L.F.: I regretted the minute i pressed share: A qualitative study of regrets on facebook. In: Proceedings of the seventh symposium on usable privacy and security. p. 10. ACM (2011)