Integrating Privacy and Trust in Voting Advice Applications

Aigul Kaskina and Andreas Meier
University of Fribourg
Boulevard de Pérolles 90
Fribourg, Switzerland
Email: {aigul.kaskina,andreas.meier}@unifr.ch

***Abstract*—Due to the privacy risks that citizens are exposed to while using online platforms, this research focuses on privacy and trust issues in the field of e-Democracy, particularly in *voting advice applications (VAAs)*. After a literature review, a *VAA profile privacy framework* will be introduced. Within this framework each citizen will be able to manage her/his political profile's privacy settings according to her/his personal preferences regarding information disclosure. By conducting an experiment based on real data collected from an online survey, the data sensitivity and visibility inherent to the VAA will be identified. Additionally, the privacy preferences of citizens have been clustered and classified according to their degree of openness. Moreover, as the core of the VAA, a recommender engine will be proposed to embed a trust network and privacy preferences in the recommendation process. This will preserve the VAA from unreliable users, as well as take into account citizens wishes related to personal privacy within the platform. Furthermore, conclusions and outlook for the future work will be discussed.**

I. Introduction

In the field of e-Democracy, voting advice applications (VAAs) have become increasingly popular in recent years and have been predominantly used in European countries [1]. VAAs are used during an election period and the main idea is to provide voters with recommendations of political parties/candidates that share their political attitudes. VAAs is a recommender-system oriented platform that calculates the distance between feature vectors of voters and parties/candidates that are based on the answers to policy issues statements [2]. Then, the closest parties/candidates are provided as a list of recommendations. Unlike commercialised recommender systems that are heavily rely on contextual data and additional information to improve recommendations, VAA recommendations are still limited to voters' answers to the policy issue statements. Current VAA research underestimates the aspect of using social information, which results in a low usage of the application after the election period is finished [3]. In this case, web platforms such as *social voting advice applications* (SVAAs) [4] will become more significant, especially when these tools will exploit advantages of Web 2.0 data. Embedding social data into the design of VAAs appears to improve the recommendation process. This will facilitate the citizen's decision making process and lead to the enhancement of citizen participation, which is of great importance for the e-Society. However, there are inherent drawbacks in enriching the data for recommendations. Being more sensible and visible in relation to citizen data presents a higher risk of privacy violation [5]. The higher the risk to the citizen's privacy the lower the citizen's trust in the application; this might hinder the adoption of the VAAs [6]. As a result, an extension of VAAs to SVAAs brings along increased privacy and trust issues.

The goal of this research is to consider privacy and trust issues while enriching the recommendation process in the design of SVAAs. It is also intended to improve the Swiss *smartvote* project [7], which is a VAA that is used for the local, cantonal, and national elections in Switzerland. The objectivity of this work is to develop a system prototype that satisfies requirements as follows: *(R1)* The system should include e-Discussion and e-Posting sections where citizens can exchange opinions, ideas and discussions about political issues. *(R2)* The system should provide citizens with a privacy management tool that allows to set up privacy settings for their profile. *(R3)* The system should integrate a trust network among users of the platform and use the trustworthiness of citizens in the recommendation process. *(R4)* The systems should integrate users' privacy preferences in the recommendation process. *(R5)* The system should provide the user with possibilities to personalise his/her recommendation output.

As far as system requirements are concerned the following research questions are posed: *(Q1)* How can a profile privacy framework be designed for SVAAs? *(Q2)* How can trust-aware recommendation techniques be embedded in the design of SVAAs? *(Q3)* How can privacy settings be used in the design of SVAAs? *(Q4)* What are the advantages and disadvantages of using the trust and privacy preferences in the recommendation process? *(Q5)* How should an evaluation framework be designed in order to test the prototype proposed? Research questions Q1, Q2 and Q3 have been covered in this paper.

The rest of the paper is organised as follows: Section 2 is a review of existing literature, focused on VAAs, and includes a discussion of existing privacy frameworks proposed within social networking sites. Section 3 presents a profile privacy framework designed specifically for the VAA platform. Then, Section 4 provides a first evaluation of the framework proposed and describes the data collection conducted for the experiment together with results of the data analysis. Section 5 explains the recommender architecture for the VAA, which includes the trust network and privacy preferences to be included in

the recommendation process. Finally, concluding remarks and outlooks are presented in Section 6.

II. Literature Review

A. Voting Advice Applications

VAAs are the web-based online tools that provide voting recommendations by positioning on a visual landscape candidates/parties together with voters, indicating which candidate/party is the closest to a particular voter based on the answers to policy issues statements. In addressing VAAs issues much attention has been given to their impact on political behaviour [1], as well as to estimating the effects of the VAAs on voter turnout [8], [9]. There are several studies, in which technical aspects of VAAs have been explored. In his work, Mendez [10] described a methodological aspects of VAA design such as the matching of voters' policy preferences with candidates/parties to provide recommendations. He compared predictive performance of high-dimensional mapping and low-dimensional mapping using different proximity metrics. In his earlier work [2], Mendez presented an empirical test of four different algorithms matching voters and candidates/parties.

A different technique using a collaborative filtering approach in which like-minded voters are clustered based on their profiles has been proposed in the work of Katakis et al. [11]. This approach outperformed traditional citizen-candidate similarity metrics and comparatively produced better recommendation results. In his work, Teran [3] evaluated a number of VAAs and found that they didn't generally use technologies such as Web 2.0, Web 3.0, audio, video, interactive video, and synchronous communications channels from which VAAs could take a significant advantage. To deal with this problem the SmartParticipation platform was presented by Teran [3]. The platform allows citizens to create virtual communities based on their profiles, such as new political parties, thematic groups, and civic networks, and participate in national issues and debates through the use of ICTs and Web 2.0. Advanced functionalities inherent to social networking applications have also been applied in the work of Katakis et al. [4] where the VAA was supplemented with a social voting advice module. Specifically, researchers implemented social features such as community-based voting recommendations, a "friend" function for comparing political views, interaction between users, and a blog feature for comments.

In fact, incorporating social information into a VAA design brings up a spectrum of opportunities to improve its recommendations. Moreover, socialised VAAs can attract citizens' interest in the platform and enhance their participation in the building political community processes.

B. Privacy Frameworks

Privacy and trust are reasonable issues to be raised in exploring ways to improve VAAs design and its adoption. Embedding social data into the design of a VAA has considerable potential to improve its services and enhance citizens' participation. Therefore it is important to consider the citizen's personal desire regarding privacy disclosure and the trust estimation within the platform. In his work, Westin [12] has defined an individual's privacy right as follows: *"each individual is continually engaged in the personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others according to the surrounded conditions and social norms"*. Indeed, it is important to consider a privacy-minded design for VAAs where the citizen is given a right to decide what data s/he wants to disclose about herself/himself.

The development of privacy frameworks is a main concern of social networking sites. In order to enable users to communicate their privacy preferences before allowing access to their data, Aimeur et al. [13] presented a privacy framework where privacy concerns like security, reputation and credibility, and profiling were addressed. They derived users' privacy levels and tracking levels by categorising the user data, the user privacy concerns, and profile viewers. However, both privacy levels and tracking levels were limited to a static configuration that cannot fully characterise each user's personal "taste" of privacy settings. To this end, another study proposed a privacy wizard [14]. By collecting users' privacy specifications and extracting features from user's neighbourhood (list of friends), the wizard inferred a privacy-preference model describing the user's personal privacy preferences. Afterwards the model was used to automatically configure user privacy settings, thus reducing the user effort. Certainly, it is important to consider user's effort in configuring personalised privacy settings, but in this case it was not proven that the relation to a user's list of friends provides adequate information to build such a model. An alternative framework that takes into account the privacy settings of users with respect to their profile items as well as their positions in the social network has been described by Liu et al. [5]. The framework computes privacy scores of users in an online social network, and estimates their potential privacy risks. Additionally, the framework includes a privacy setting recommendation for the target user by comparing her/his privacy score with the privacy score of the user's social graph.

The common feature inherent in the aforementioned privacy frameworks and other studies [15], [16], [5], [13], [14] is that the user's profile is represented as a central data source in order to elicit user privacy preferences. Privacy preferences are mainly defined by the user's *profile items (the data)*, her/his *social network*, and her/his *engagement within the system*. The two dimensions, the user's data and social network are used to determine her/his disclosure behaviour and to maintain the preferred degree of privacy.

People choose to explicitly disclose or share information about themselves, their opinions, and their activities as means of declaring their loyalties or differentiating themselves from others [17]. Indeed, disclosure behaviour differs from person to person, and can vary depending on the personal motives. Either the person is willing to be publicly open or s/he prefers to keep her/his profile as private as possible. At this point, it is vital for political platforms like VAAs to be concerned about a citizen's desire to position herself/himself within the platform by expressing her/his privacy preferences. Moreover,

the trust among citizens should be also considered, thus the system will be able to prevent the appearance of unreliable and untrustworthy users.

III. Profile Privacy Framework for VAAs

This section presents a profile privacy framework that reflects an environment where the main actor is a citizen who is able to set up her/his profile privacy settings within a VAA. The components of the framework are designed according to the needs of the VAA and are based on the concepts of MyPolitics and OurPolitics introduced by Ladner and Meier [18]. MyPolitics is the citizen's personal political diary, where citizens may store their political preferences, VAA evaluations, and individual opinions about elections, as well as their electronic votes. According to the citizen's desire for disclosure, s/he might partly open this political diary to individuals, family members, friends, or various communities. On the other hand, there is the OurPolitics option; a citizen can choose to become a member of the non-profit platform of OurPolitics. In OurPolitics, users can meet other citizens or politicians with similar preferences and exchange ideas and information. The design of the framework was also influenced by related work in social networking sites described in Section II-B.

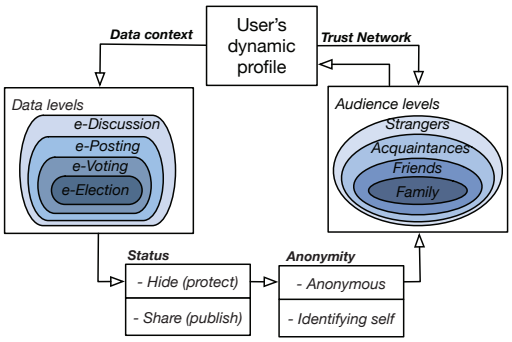

Fig. 1. User profile privacy framework

The resulting privacy framework in which citizens are allowed to define privacy settings for their political profiles is presented in Fig. 1. The framework consists of four main components: *Data levels, Audience levels, Status, and Anonymity*

- *Data levels*. Citizens privacy settings reflect their decisions on information disclosure. Recent research has found that user information disclosure is highly dependent on the information context [19]. Indeed, the development of social VAAs is intended to involve diversified types of political data that contain a rich context. Therefore, four data levels are proposed as follows*: e-Election, e-Voting, e-Posting, and e-Discussion*. These data levels have been inferred from the process steps of e-Voting and e-Election described by Meier [20]. Each data level contains different types of data as displayed in Table I. The framework allows users to express their own perceptions about data levels in terms of their degree of importance. A specific colour corresponds to the degree of importance the citizen allots to the data. The most important and valuable data is stored in the core of the component, whereas the less valuable information is set on the outer layers.

TABLE I
Data levels and data types

Data level	*Data type*
e-Election	Votes for candidates, parties
e-Voting	Votes for political issues
e-Posting	Blogs participation, wall posts
e-Discussion	Discussion topics, questions, answers

- *Audience Levels*. The citizen sets her/his information disclosure to a particular group of people depending upon her/his perceptions on each data levels. Therefore the second component of the framework belongs to *the audience levels* that will be derived from *the trust network* between citizens. The audience levels are based on social relationships and behavioural mechanisms used to regulate the desired levels of privacy, as presented by Altman [21]. As a result, audience levels have been classified as peripheral relationship bonds represented by strangers and acquaintances, more extensive relationship bonds such as in-laws and friends, and close relationship bond such as family members. Similar to the data levels, each person could perceive people differently in terms of relationship bonds. The extent of the relationship bonds are also indicated by color and layer. The family members are in the core of the component as the closest bonds of the citizen, and strangers and acquaintances are in the outer layers, as the peripheral bonds of the citizen.
- *Status*. The citizen by her/his personal wish can assign a particular status: *share* or *hide*. Assigning a *share* status on a particular data level to a particular audience means that this data level is opened to people for opinion exchange, feedback, discussion, or interaction. By default, the *hide* status means that the citizen wishes to keep her/his data private and unpublished.
- *Anonymity*. The citizen determines whether s/he is sharing the data anonymously or identifying herself/himself.

Within this framework citizens are allowed to define the level of importance of the political data by identifying the audience levels with which they would like to share a given. As an example of the privacy settings configuration, assume that a citizen considers it important to share e-Voting data with her/his family. Nonetheless s/he would like to share e-Posting information only with acquaintances and strangers, anonymously, keeping the rest of the data private. The formal notation of the privacy settings definitions based on the framework is described below in detail, and Table II displays the aforementioned example of privacy settings configuration.

We assume a set of N citizens $C = \{\overrightarrow{c_1}, \overrightarrow{c_2}, ..., \overrightarrow{c_N}\}$ that have to define a set of 16 privacy settings $S = \{s_1, s_2, ..., s_{16}\}$. Privacy settings are inferred from the privacy framework and represented as a tuple of $\{$*data level, audience level*$\}$. Each citizen $c_i \in C$ is a representation of a vector space

model $c_i = \{c_{(i,1)}, ..., c_{(i,k)}, ..., c_{(i,16)}\}$, where $c_{(i,k)} \in K$ is a set of the citizen's assigned statuses that correspond to *"Hide, ShareToStrangers, ShareToAcquaintances, ShareToFriends, ShareToFamily"* and equals, respectively, the values in the range of $K = \{0, 1, 2, 3, 4\}$. Thus a citizen's preferred privacy settings are defined as vector of 16 features. According to the framework the importance of the data and the group of people should be defined. This characterises two data privacy properties that appear as *data sensitivity* and *data visibility*.

TABLE II
PRIVACY SETTINGS

Data / Audience	e-Election	e-Voting	e-Posting	e-Discussion
Strangers	0	0	1	0
Acquaintances	0	0	2	0
Friends	0	0	0	0
Family	0	4	0	0

- *The sensitivity* of the data is defined by the citizen's decision to share a particular data level and represented as a tuple of $\{$*data level, status*$\}$. The sensitivity also expresses the extent to which the particular data level is valuable to the citizen.
- *The visibility* captures the audience level chosen for sharing or hiding a particular data level, and, identified as a tuple of $\{$*audience level, status*$\}$.

IV. Evaluation of the Framework

To the best of our knowledge, none of the past researches focused on developing the profile privacy framework specifically to the needs of social VAAs. Liu et al. [5] presented a similar privacy framework design in order to estimate a privacy score that measured the user's potential privacy risk according to his/her information disclosure behaviour. However, the central part of our framework is a citizen's profile provided with a privacy management tool in order to integrate the preserved privacy and trust into the VAA's recommendation process.

To test the framework and evaluate how people would feel about privacy issues while using social VAAs, an online survey was conducted. The survey consisted of four multiple-choice questions, with four possible answers. Respondents were explicitly asked to express preferences on the profile privacy settings as if they had been using the VAA platform. The questions in the survey were constructed according to the privacy framework components described in Section III. Respectively, each question was seeking to determine a person's willingness to share a particular data level. Each multiple-choice answer was a checkbox related to the group of people (audience level) with whom the respondent wished to share the data. If the person left an empty checkbox, it was considered that the data level was kept private (hidden). In total, 70 people were asked to express their privacy preferences; 57% were representatives of Central Asia, and 43% were representatives of European countries. The respondents' ages ranged from 22-35 years. In result, a dataset of a 70-by-16 matrix was collected. Each row of the matrix represents a person, and each column represents a person's assigned values to privacy settings. In order to measure the sensitivity and visibility of the data within the framework proposed, we calculated total number of *"share"* occurrences in each privacy settings attributes $\{$*data level, audience level*$\}$. The results are displayed in the Fig. 2 and Table III.

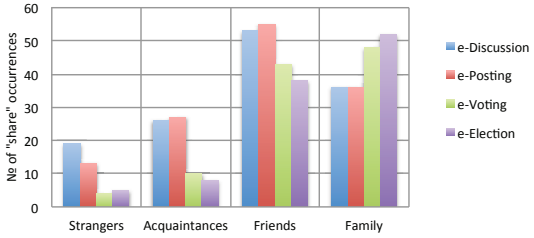

Fig. 2. Privacy settings distribution

TABLE III
DATA SENSITIVITY AND VISIBILITY

Sensitivity		**Visibility**	
Data Level	*% of "share"*	*Audience level*	*% of "share"*
e-Discussion	47.8 %	Friends	67.5 %
e-Posting	46.7 %	Family	61.4 %
e-Voting	37.5 %	Acquaintances	25.3 %
e-Election	36.7 %	Strangers	14.6 %

First, according to Table III, people clearly tend to consider e-Voting and e-Election as the most sensible data, whereas e-Posting and e-Discussion are perceived as the least sensible data within the VAA. Second, it can be concluded that people consider friends and family as the most reliable and trustworthy audience with whom they wish to share their political data, thus most of the data is visible to friends and family. However, from the privacy settings distribution a dependency can be noticed between users' perceptions of the data sensibility and visibility. For example, Figure 2 shows that for some people the sensitivity of the data increases from e-Discussion to e-Election when it is visible to strangers, acquaintances, and friends, while it decreases from e-Discussion to e-Election when it is visible to family. Moreover, the sensitivity of e-Election and e-Voting is the lowest when it is visible to family and friends, whereas the highest sensitivity is observed when it is visible to strangers and acquaintances. The extent of visibility (a chosen audience for sharing the data) directly depends on the data sensitivity. However, privacy preferences might vary considerably between different people; therefore, we have applied clustering techniques in order to group people based on their privacy preferences.

A. Fuzzy C-Means Clustering

The goal of applying a clustering technique to the dataset was to classify groups of people based on their privacy preferences. Clustering is an unsupervised learning task, where

a clustering algorithm organises a given set of objects into similar groups (clusters). Objects belonging to the same cluster are as similar as possible to each other. Two types of clustering techniques are well known: sharp and fuzzy clustering. With sharp clustering each element is classified with only one cluster. In contrast, fuzzy clustering allows objects to be associated with many clusters according to their membership degree value, based on the fuzzy set theory introduced by Zadeh [22]. In this work, we exploit a fuzzy c-means clustering algorithm in order to organise citizens into clusters. Citizens will be similar with their feature vector expressing their privacy preferences. As a result, fuzzy clustering will produce groups of like-minded citizens. The main goal of the fuzzy c-means algorithm is to compute the similarity that an object shares with each cluster using a membership function. The membership function calculates the membership degree of each object in every cluster with values in the range of [0,1]. A high degree of similarity between the object and a cluster is assigned when a membership value is close to 1, whereas values close to 0 imply a low similarity between the object and that cluster [23]. Using the in-built function *fcm()* in Matlab environment, the fuzzy c-means algorithm was applied to our dataset. According to the number of audience levels, the initial number of clusters was set to four. The fuzzy c-means algorithm uses the Euclidean distance similarity measure in a vector space to execute the partitioning of objects into clusters. After 35 iterations a matrix of final cluster centers was generated. The final fuzzy partition matrix that contains each object with membership values for each cluster. The maximum value of the membership degree identifies the cluster to which the object belongs, and the first row of Table IV displays the distribution of objects into clusters. The percentage of openness within each cluster was calculated in terms of "share" status on each privacy setting attribute {*data level, audience level*}. This is shown in Table IV.

TABLE IV
CITIZENS DISTRIBUTION INTO CLUSTERS

Open to:	Cluster 1	Cluster 2	Cluster 3	Cluster 4
Strangers	10%	9.5%	4.3%	8.5%
Acquaintances	22.9 %	16.7%	4.3%	14.2%
Friends	62.9%	37.5%	21.4%	35.7%
Family	4.3%	36.3%	70%	35.7%

After an analysis of each cluster by maximum and minimum value of openness, the following four classifications of people in terms of VAA privacy settings were identified: *Cluster 1* - people are willing to share all data levels with friends, and hide it from family; *Cluster 2* - people are willing to share all data levels with family and friends, and hide it from strangers; *Cluster 3* - people are willing to share all data levels only with family, and hide it from acquaintances and strangers; *Cluster 4* - people are willing to share only e-Election/e-Voting with family, and to share only e-Posting/e-Discussion with friends. They are willing to hide the data from strangers.

Partitioning of people into clusters allowed us to distinguish patterns of profile openness. The advantage of fuzzy clustering is that it assigns each person to every cluster, thus avoiding discriminative clustering into groups. This could be beneficial for citizens while providing them with recommendations. The membership degree values of each citizen could further be used to improve the VAA recommendations.

V. RECOMMENDER ENGINE

In this section, the architecture of the VAA's recommender engine is proposed, as shown in Fig. 3.

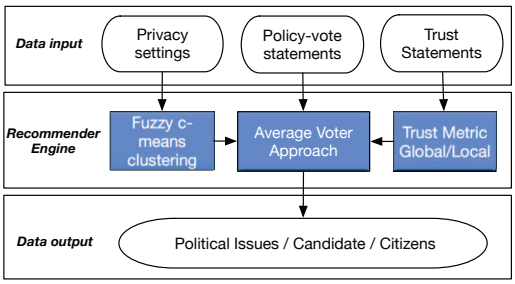

Fig. 3. Recommendation engine architecture.

The general idea is to extend traditional VAA functionality by exploiting a citizen's profile privacy settings and a trust network before a final recommendation is generated. Traditional VAAs provide recommendations by calculating the proximity between feature vectors of a citizen and parties/candidates. An alternative approach of community-based recommendations has been proposed by Katakis et al. [4]. The so-called *average voter* approach is adapted for the core part of the recommender engine. Usually the answers to policy statements from political parties are either coded by experts or given by representatives of political parties, who might intentionally design their profiles to be as close as possible to citizens' political preferences. For that reason, the advantage of the average voter approach is that it ignores the party/candidate profile and considers the similarity on political attitudes only between citizens or communities. The algorithm calculates the distance between a citizen and the average voter on each political issue. Then the distance is calculated based on the Euclidean similarity metric. Finally, the political issues of the k-nearest average voters are proposed as a list of recommendations.

Second, by including a forum section, which represents e-Discussions among citizens, the architecture proposes to use a trust-aware recommender technique to preserve the privacy of the system and to protect it from unreliable users. Current SVAAs have a "friend" functionality where citizens can compare political views with each other. It is assumed that by interacting with another citizen for comparing political views, a target citizen will be explicitly asked to rate to what extent s/he finds another citizen politically close and reliable, thus expressing her/his *trust statement*. For those citizens who have no social interactions, the trust metric exploits propagation to predict for each citizen how much s/he should trust every other citizen. The trust computation will be based on the global and local trust metrics that use two propagation methods:

propagation by average and propagation by multiplication [24]. With an inclusion of trust values the system provides two types of recommendations: citizens (communities), and community-based political issues.

Third, as the final step in the recommendation process, a privacy settings should be considered before the final recommendation is generated. The fuzzy c-means algorithms using Euclidean distance (Section IV-A) have been applied as a similarity metric of citizens' privacy preferences. At the current state of research, we propose calculating a privacy score for each citizen based on her/his privacy preferences that would feed the trust score, as well as excluding the data from the recommendation process that has been protected by the citizens. Finally, the prototype gives citizens an option to choose a type of recommendation output, either based solely on the average voter similarity metric, or trust-enhanced recommendations.

VI. Conclusions

Current trends in the development of VAAs demand both improvements in algorithmic approaches and extensions of functionalities. However, this can lead to privacy issues that are of high importance for VAAs. This paper proposed to extend functionalities of a Swiss VAA, smartvote.ch, towards a social voting advice application. For that reason, a profile privacy framework was designed according to the needs of VAAs. This framework provides a privacy management tool that enables citizens to set up their privacy settings. Using real-data collected from people who provided their privacy preferences as if they were using a VAA, the data sensibility and visibility within the framework were analysed. Due to the diversified disclosure behaviours of citizens, a fuzzy c-means clustering algorithm was applied in order to differentiate people based on their privacy settings and deduce the classification of groups of people according to extent of their profiles' openness. Finally, a recommender engine was proposed to use the citizens' trust network and privacy preferences in the recommendation process.

As future work, the evaluation of the VAA with trust techniques will be conducted to analyse how recommendations will improve in accuracy and effectiveness. The privacy settings will also be included in the recommendation process and evaluated. Additionally, the citizens' activity in the e-Discussion section will be considered for inclusion to enrich the calculation of political issue recommendations.

Acknowledgment

The authors would like to thank the members of the Information System Research Group at the University of Fribourg (http://diuf.unifr.ch/is) for contributing valuable thoughts and comments.

References

[1] D. Garzia and S. Marschall, "Voting advice applications under review: the state of research," *International Journal of Electronic Governance*, vol. 5, no. 3, pp. 203–222, 2012.

[2] F. Mendez, "Matching voters with political parties and candidates: An empirical test of four algorithms," *International Journal of Electronic Governance*, vol. 5, no. 3, pp. 264–278, 2012.

[3] L. F. T. Téran, *SmartParticipation: A Fuzzy-Based Recommender System for Political Community-Building*. Springer, 2014.

[4] I.Katakis, N. Tsapatsoulis, F. Mendez, V. Triga, and C.Djouvas, "Social voting advice applications—definitions, challenges, datasets and evaluation," *Cybernetics, IEEE Transactions*, vol. 44, no. 7, pp. 1039–1052, 2014.

[5] K. Liu and E. Terzi, "A framework for computing the privacy scores of users in online social networks," in *2009 Ninth IEEE International Conference on Data Mining*, 2009.

[6] F. Bélanger and L. Carter, "Trust and risk in e-government adoption," *The Journal of Strategic Information Systems*, vol. 17, pp. 165–176, 2008.

[7] smartvote, Available at: http://www.smartvote.ch, accessed 29 April, 2015. [Online]. Available: http://www.smartvote.ch/

[8] A. Ladner and J. Pianzola, *Do voting advice applications have an effect electoral participation and voterturnout? Evidence from the 2007 Swiss federal elections*, ser. Lecture Notes in Computer Science. Springer, Berlin, 2010, vol. 6229, pp. 211–224.

[9] S. Marschall and S. M., "Voting advice applications and their effect on voter turnout: The case of the german wahl-o-mat," *International Journal of Electronic Governance*, vol. 5, no. 3, pp. 349–366, 2012.

[10] F. Mendez, *Matching Voters with Parties and Candidates Voting Advice Applications in Comparative Perspective*. ECPR Press, 2014, ch. What's behind a matching algorithm: A critical assessment of how VAAs produce voting recommendations, pp. 49–66.

[11] I. Katakis, N. Tsapatsoulis, V. Triga, C. Tziouvas, and F. Mendez, "Clustering online poll data: towards a voting assistance system," in *Semantic and Social Media Adaptation and Personalization*, IEEE, Ed., 2012, pp. 54–59.

[12] A. F. Westin, "Privacy and freedom," *Washington and Lee Law Review*, vol. 25, no. 1, p. 166, 1968.

[13] E. Aïmeur, S. Gambs, and A. H, "Upp: User privacy policy for social networking sites," in *2009 Fourth International Conference on Internet and Web Applications and Services*, 2009.

[14] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th international conference on World wide web*, 2010.

[15] M. Johnson, S. Egelman, and S. M. Bellovin, "Facebook and privacy: it's complicated," in *Proceedings of the eighth symposium on usable privacy and security*, 2012.

[16] F. Stutzman, R. Gross, and A. Acquisti, "Silent listeners: The evolution of privacy and disclosure on facebook," *Journal of privacy and confidentiality*, vol. 4, no. 2, 2012.

[17] L. Palen and P. Dourish, "Unpacking privacy for a networked world," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2003.

[18] A. Ladner and A. Meier, "Digitale politische Partizipation-Spannungsfeld zwischen MyPolitics und OurPolitics," *HMD Praxis der Wirtschaftsinformatik*, vol. 51, no. 6, pp. 867–882, 2014.

[19] B. P. Knijnenburg and A. Kobsa, "Making decisions about privacy: Information disclosure in context-aware recommneder systems," *ACM Tramsactions on Interactive Intelligent Systems*, vol. 3, no. 3, 2013.

[20] A. Meier, *eDemocracy and eGovernment: Stages of a Democratic Knowledge Society*. Springer-Verlag Berlin Heidelberg, 2012.

[21] I. Altman, "Privacy regulation: Culturally universal or cuturally specific?" *Journal of Social Issues*, vol. 33, no. 3, 1977.

[22] L. Zadeh, "Fuzzy sets," *Information and control*, vol. 8, no. 3, pp. 338–353, 1965.

[23] J. C. Bezdek, R. Ehrlich, and W. Full, "Fcm: The fuzzy c-means clustering algorithm," *Computers and Geosciences*, vol. 10, no. 2-3, pp. 191–203, 1984.

[24] F. Ricci, L. Rokach, B. Shapira, and P.B.Kantor, Eds., *Recommender systems handbook*. Springer US, 2011.