Digital support for gathering administrative ideas from constituents of democratic bodies

Marius C. Silaghi and Ronald J. Bailey and Phil Bernhard and Phil K. Chan and Cem Kaner

February 17, 2004

Florida Institute of Technology
Computer Sciences Department

Technical Report
TR-2004-04
(draft)

Abstract

Digital systems have simplified the management, accounting, transfer, and dissemination of all types of information. However, they have not yet been often successfully applied to a very difficult and rewarding task of a democratic administration: facilitating the acquisition, evaluation and refinement of the ideas and opinions of large bodies of constituents. Consequently, administrative ideas from individuals, other than a predefined set of rule-makers are going to be lost, despite the fact that they may be substantial, novel, and provide solutions to significant economic, social or security problems. Some digital support already exists for assessing the opinion of the citizens:

- Classic polls on the Internet. The problem is that the formulation of the well advertised polls can be shaped by only a limited number of people and can therefore miss important issues and variations. As follows, new ideas cannot be collected but only verified.
- Comments sent to websites such as *www.regulations.gov*. The comments can only be directed toward a narrow topic that has been recently addressed. Also, some issues can draw hundreds of thousands of comments and there is no feasible way to score them.
- E-Mails and Phone Calls to representatives. The main drawbacks are that they cannot reliably convey the amount of popular support, and important ideas can still be lost in large heaps of requests received.

An enhanced way to support input from constituents in democratic organizations is via citizen-sourced & ranked polls and civic discourse, where debating participants can jointly formulate ideas. This article is concerned with investigation of techniques that will provide extensive digital support in gathering and refining ideas from citizens. The techniques developed will be applied and tested by obtaining administrative ideas and feedback at different levels of democratic bodies: student governments in high schools, committees in academic institutions, homeowner associations, and town administrations. We will investigate new levels of privacy that can be offered in the new framework, as well as techniques for fair management and presentation of large numbers of ideas. Each member of any democratic organization benefits if better feedback from citizens to administrations is set in place.

1 Status of the problem

Digital systems have simplified the management, accounting, transfer, and dissemination of all types of information. Unfortunately it has not yet been often successfully applied to a very difficult and rewarding tasks of democratic administrations: facilitating the acquisition and evaluation of the ideas of large bodies of constituents. Consequently, administrative ideas from individuals, other than a limited set of rulemakers are going to be lost, despite the fact that they may be substantial, novel, and provide solutions to significant economic, social or security problems.

Some digital support already exists for assessing the opinion of citizens:

- Polls on the Internet are a common way of assessing citizens' opinion. They are organized both by governments and independent institutions. The problems with existing polls include:
  - The formulation of well advertised polls can be shaped by only a limited number of people and therefore cannot serve for gathering new ideas from the large public.
  - Limited involvement (related to the fact that they are not discursive, having a very limited impact).
- E-Mails, Phone Calls to representatives, and comments to websites such as *www.regulations.gov* can have an important impact. The main drawbacks are that:

  - They cannot reliably convey the amount of popular support (vulnerability to manipulated response rates).
  - Important ideas can still be lost in large heaps of requests received (hundreds of thousands were reported for some narrow topics).
  - Comments to be submitted to www.regulations.gov can only follow narrow topics proposed as in the case of the classical polls.

- Intelligence analysis by government agencies can learn and transmit upward good ideas. However intelligence is meant mainly for security purposes and cannot guarantee the best backing of a proposal that doesn't emerge from within.

A powerful tool that can help promote new ideas from citizens and obtain the best public feedback is *citizen-sourced & ranked polls and civic discourse*. Currently, well intentioned citizens may have to abort well founded ideas for the simple reason that they do not have time and energy to bring them before representatives. Citizens may also be unable to point out unforeseen complex side-effects that they detect for discussed proposals.

An important issue that must be addressed when citizens are enabled to present their ideas, is that huge amounts of proposals may flood the administration. A solution is required, which on one side could give all citizens opportunities and support to present their administrative ideas, and on the other side should allow evaluators to easily spot high quality proposals. A scalable solution we propose is to let the citizens filter each other's proposals via citizen-sourced & ranked pools and civic discourse. The introduced challenges are:

- the high costs of subsequent evaluation procedures,
- the useless involvement of the whole democratic body with unpopular issues proposed and supported only by relatively small minorities,
- the need of potentially requiring citizens to study texts that are inconsistent, incomplete, presented poorly or, in general, of low quality.

In this research we propose to investigate web-based techniques that can be used to solve the just mentioned problems with citizen-sourced & ranked polls. The specific problems that we plan to address are:

- The development and analysis of fair criteria to organize the dissemination of large amounts of administrative proposals, such that novel and high quality ideas get the appropriate visibility.
- The development and analysis of methods for managing proposals as they mature and age.
- Identify interesting levels of security and acceptable trade-offs with needs of scalability, mobility and convenience. Offering security technologies for proposers, commenters, and evaluators.
- Techniques that allow for cooperation between several persons editing proposals without an explosion in the number of proposal versions.
- Customization of each citizen's access web-page facilitating usage and security.
- Techniques for archiving ideas and easy retrieval.

- Automatic verification of submitted proposals for consistency.
- Automatic identification of conflicts between new ideas and existing norms, i.e. rules, authoritative standards, models and types.

The techniques developed will be evaluated on different levels of democratic bodies:

1. student governments
2. committees in academic institutions
3. homeowner associations and town administrations

We have found that several of the techniques we have developed to date can be applied to solve some of the aforementioned challenges. As part of the proposed research, we plan to also disseminate our results to attract input from other researchers.

2 State of the Art

Modern polls are a valuable tool that with very limited effort can produce information of high reliability. Polls can be organized by governments but also by other independent institutions, e.g. newspapers. Many of these polls are conducted via the Internet. Some of their limitations are that they:

- cannot help elicit new ideas or variations of ideas,
- do not encourage participation, since each separate action is limited to a small impact,
- are not organized such that users could easily search for them.

We plan to approach polling with technologies that relate to ones studied for electronic election systems. There exists extensive research into secure electronic election systems [20, 2, 23]. Several desirable properties of such systems that have been identified and analyzed include: *Accuracy, Democracy, universal Convenience, Scalability, Mobility, Flexibility, Verifiability*, and *Privacy*. Currently there exists no election protocol to simultaneously offer the highest levels of all of these. Following is a list with the classical definitions for the desired properties of a voting system.

- Accuracy A system is accurate if *it is not possible* for a vote to be altered, *it is not possible* for a validated vote not to be included in, and *it is not possible* for an invalid vote to be counted in the final tally.
- **Democracy** A system is democratic if it *permits* only eligible voters to vote and it *ensures* that each eligible voter can vote, but only once.
- **Privacy** A system is private if neither election authorities nor anyone else can link any ballot to the voter who cast it and no voter can prove that he or she voted in a particular way (also called receipt-free or non-coercible voting).

- **Verifiability** A system is verifiable if anyone can verify that all votes have been counted correctly.

  A weaker form of verifiability which we still find acceptable is when a system allows voters to verify their own votes and correct any mistakes they might find without sacrificing privacy.

  Even weaker forms are, when mistakes may be pointed out but not corrected or when mistakes are detected by party/administration representatives, not individual voters.

- **Convenience** A system is convenient if it allows voters to cast votes quickly, in one session, and with minimal equipment or special skills.

- **Scalability** A system is scalable if it can be used with many voters and votes.

- **Flexible** A system is flexible if it allows a variety of ballot question formats, including open ended questions.

- **Mobility** A system is mobile if there are no restrictions on the location from which a voter can cast a vote.

3 Example of our Proposed System in the Curricula Committee Setting

In this section we describe a very small example of how a few features of our proposed system, the Administrative-Feedback Website (AFW), will be used. For this discussion, assume that user Alice gets a new idea: *"The PhD program of the school could be improved by waiving tuition fees for the PhD students "*. To promote this idea using the AFW, she performs the following:

1. Alice formulates the idea as a proposal: *"FIT should waive the tuition fees for all PhD students!"*

2. Alice goes to the AFW of the curricula committee, opens the submission module for ideas, and types in her proposal.

3. If Alice was able to type in her whole proposal it means that the module for checking the consistency of proposals validated the text as being legal.

4. Simultaneously Alice can specify an explanation in a separate field: *"The PhD program of the school could be improved since more good students will be able to afford to study. Their research could help attract funding that compensates for the lack of fees"*. This comment undergoes similar semantic filtering like the proposal.

5. Alice pushes a button to effectuate the submission, and her locally stored credentials are used for completing the task with the level of privacy supported by the AFW. The proposed idea is published on AFW together with a first *pass* score referring Alice's comment.

6. The new proposal appears at the top of the list of new proposals, and Bob sees it. It also appears in the tail of the list of proposals ordered by the number of supports in the last week, but that is not what was visible to Bob. Bob likes the idea and its comment and scores it

with *pass*. This new score on AFW supports the idea and refers the initial comment, which is tagged 2 (the number of grades referring it).

7. Carol does not like the idea and submits a *fail* grade associated with a comment showing weaknesses of Alice's comment. Carol's comment is shown separately in a list of failing comments for Alice's proposal and is threaded to Alice's comment.

8. Dave likes Alice's proposal and submits a *pass* score with a comment that answers Carol's critique. His comment appears after Alice's comment since it is so far referred to by only one grade. However, Carol's comment also receives a link threading it towards Dave's comment. Other comments answering Carol will be added to Carol's comment, ordered by the grades referring to them.

9. If Alice returns and reads the continuation of the discussion, she can abandon her own initial comment and refer to Dave's more complete comment for her scoring. Then the score of Dave's comment is higher and is ordered before the initial comment of Alice, referred to now only by Bob. Alice could not submit a second grade while still having a previous grade valid for that idea.

4 Overview of Citizen Sourced & Ranked polls

As part of the proposed research, we will address the issue of enabling all eligible participants to easily publish new ideas that pass an appropriateness filter, as well as to evaluate and grade any of the existing ideas. This is somewhat related to some forums [12, 28]. The grades that we will support initially are: *pass*, *fail*, and *borderline*. For enabling advanced feedback on existing ideas, we plan to also let participants submit/confirm one comment in association with their grade.

The major modules that are required for the system that we envisage are: module for the submission of ideas, module for submission of grades, module for submission of comments, module for checking the consistency of proposals, module for visualization, module for verification of the tally, and module for citizen data management.

There are several new customized techniques which will be required for the different modules. A special cryptographic technique is required for each module (except visualization and proposal consistency). We will develop and employ *verifiable private credentials* and new techniques for secure tallying and verification of the tally. Semantic language filtering of inappropriate texts is required for the submission of both proposals and comments. New techniques for cooperation in text development and web intelligence techniques for presenting ideas are important for assuring the usability of the system. Learning interests of the users will be needed to improve the visualization module.

The minimal desirable properties for consideration of a support/rejection evaluation technique are: Accuracy, Democracy, Convenience, Scalability, Mobility. We currently assume that Flexibility should be offered in an independent way from the grading/tallying procedure. However we also plan to offer acceptable: Verifiability, Privacy. These priorities come from our intention to conform as much as possible to classical expectations from polling systems.

It should be noted that the currently used methods for polling offer very limited guarantees of *privacy* and offer only limited *democracy* (i.e. not all people are guaranteed an opportunity to evaluate each pol), while *verification* is also difficult (i.e. not everybody can ask and recount the validity of the evaluations). Therefore the type of system we propose will also improve democratic

characteristics in the evaluation methodology for polls, namely permitting all eligible citizens to give feedback. Everybody has access to the Internet via the public library infrastructure. A certain amount of privacy can also be proposed given the new framework.

Our vision is to develop a standardized tool that can be used by any administration wanting to support feedback from constituents: student government, academic committee, homeowners associations, cities. For democratic institutions (organizations striving for democratic administration) a dedicated Administrative-Feedback Website can be designed according to an accepted standard (a final goal of this work). A dedicated AFW should be known to all participants.

While there exist techniques with guaranteed non-coercibility (typically based on a voting booth [2, 22]), our system has only a statistically informative value and does not need such complex techniques.

4.1 System Modules

4.1.1 Module for the Submission of Ideas

If a participant has an idea for a poll, he can publish it on AFW. Any given participant can publish up to a certain number of such proposals per month (e.g. 1 proposal per month). By answering a poll, the evaluators also grade the interest of the ideas.

By supporting on-line evaluations for citizen-sourced & ranked polls and civic discourses published on AFW, one can easily manage aging, and deal with spam or a large number of comments (e.g. for large organizations like cities or counties). For example, proposals can be accessed by different indexes:

- Proposals where at least one support was signed in the last 7 days, listed according to the decreasing number of supporting evaluations (this helps to discriminate serious proposals from spam).
- Petitions listed in the reverse order of submission time (this gives a chance of visibility to new proposals).

Proposals that do not receive any new positive comment during a contiguous period (e.g. 1 month) can be automatically moved to an archive. However, they can also be revived at any time, along with whatever support applied when archieving took place. Participants should also be able to modify their evaluation for a proposal, in case they change mind. Techniques will be used that allow users to compute statistical estimates of the relevance of the poll. Proposals whose degree of acceptance estimated statistically using the poll is highly probable over 50%, will be linked on a separate Website that the administration can use as potentially supported suggestions.

4.1.2 Module for submission of grades

For grading evaluators will submit, via the anonymous channel, both a support and a rejection grade that can be 0 or 1. If both are 0, or if one of them has any other value, then the evaluation is withdrawn. If both are 1 then the grade is counted as *borderline* but interesting.

Some Web forums use scoring and allow a larger range of grading choices. Currently, they typically allow scoring of comments rather than scoring articles. A larger set of numbers were used in the past on SlashDot [28] and on Kuro5hin [12] with scores -1 to 5, etc. Now SlashDot uses string

scores: Terrible, Bad, Neutral, Positive, Good, and Excellent. However, it was noted in [12] that the variety of grades is often used for steering rather then for fair evaluation, namely encouraging some users to give higher weights to their score for compensating others' scores.

However, we also want to equally highlight comments with each alternative opinion, and currently suspect that some users' comment would subjectively get a higher weight than others.

4.1.3 Module for submission of comments

For enabling advanced feedback on existing ideas, we plan to also let participants submit/confirm one comment in association with their grading. Like the proposals, the comments must be verified for appropriateness in language and semantics. There is also a need to ensure fair visibility of both favorable and unfavorable comments.

4.1.4 Module for checking the consistency of proposals

The texts that different users submit as proposals or comments may have inappropriate language or semantics. A strong grammar will also be automatically enforced by the editing tools that will be made available to users. The module can also help spot conflicts with a predefined database of norms, and advise/force the user to reference or conform to them.

4.1.5 Module for visualization

The system should allow participants to easily retrieve ideas of high quality, and also to easily retrieve ideas in an area of interest to the user. All this should be done without leaking private data and without being biased based on criteria that are not essential (such as submission date).

4.1.6 Module for verification of the tally

We want to allow the user to check that his grade for a proposal was correctly accounted. Together with a proof that only eligible evaluations were considered, this can be considered as sufficient guarantee of the fairness of the system, which is needed for providing incentives to participants. When errors are found, participants should be able to prove the faulty agency without revealing their identity or their grading. If an agency is found faulty, one should be able to redo the tally with minimal involvement of the participants.

4.1.7 Module for citizen data management

For achieving all the functions described above, an AFW server should maintain a set of databases. A possible set of databases that achieve the previously discussed functions is (see Figure 1):

- An authority that can be outside the AFW maintains a database of eligible participants (ID, names, addresses, birthdays, public key of digital signature, signed request for credentials)
- Database of all accepted private credentials.
- Database of existing norms (eventually with their already processed logic form).
- Database with active proposals (ID, description, credential of author, date of creation, reference to related versions, number of supports, number of rejections, date of last support)

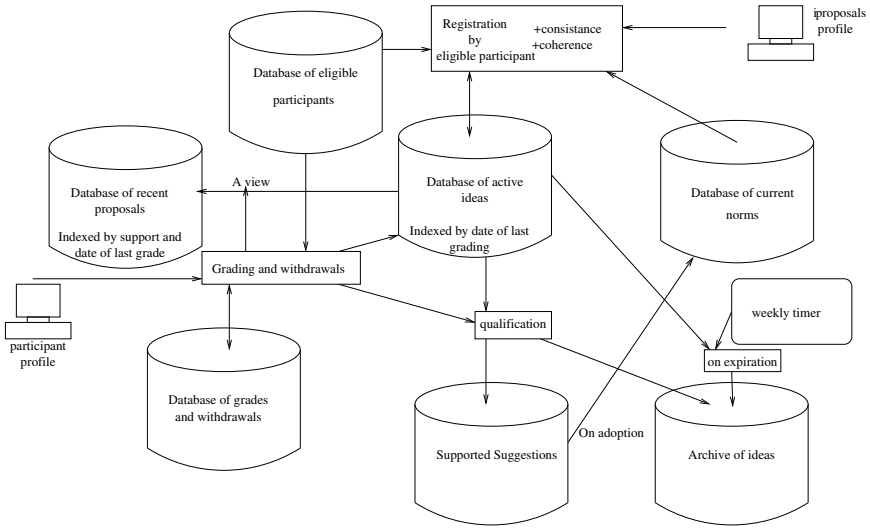

Figure 1: An AFW architecture.

- View of the database with active proposals, selecting those proposals that had a support registered recently (e.g. during the last 7 days)
- Database archive of inactivated proposals (rejected, qualified, or with no new support for some time - e.g. 2 months). Also database of grades for inactivated proposals.

The profile that should be stored by each participant consists in his current private credential keys and the random numbers associated with its grades. A participant that loses his credentials cannot get involved until a next setup replay.

4.2 Research issues

If the AFW systems will desire to publish the identity of the supporters of each citizen-sourced & ranked poll or civic discourse, then standard digital signatures schemes are sufficient for controlling the evaluation submissions as well as proposal submission steps. Each transaction would simply be authenticated based on the known digital signature public keys of each eligible participant. However, we will also study solutions allowing for the privacy of participants.

4.2.1 Verifiable Private Credentials

There exists a technique allowing a trusted authority to generate private credentials proving that its owner has a certain characteristics (e.g. is member of a certain organization, has a certain age) [14]. However, the verifiers in [14] need to trust the authority for not introducing false credentials. We propose to develop new techniques for *private credentials*, such that any third party can verify that a given credential belongs to an authorized person out of a predefined group and that each such person has exactly one pseudonym [25].

These techniques allow for a certain amount of privacy, limited in the sense that citizens can be coerced to reveal their pseudonyms. We actually develop a technique that is a pseudonym digital signature. It requires all the members of the group to sign the list of pseudonyms, to certify that

their own pseudonym is listed there. If the number of signers equals the number of pseudonyms, any third party can be convinced that no false participant was introduced. There are several techniques for generating pseudonyms of certified users [5, 7, 19, 14, 24].

Given the fact that currently polls evaluation gathering is public, we do not foresee that a very high level of privacy (and specially non-coercibility) would be often preferred over other properties: democracy, accuracy, scalability, flexibility, mobility, convenience. Most of the recent effort in the community developing election techniques was looking for high levels of privacy. Some techniques mainly based on blind signatures, anonymous channels, mix networks, also concentrate on scalability [4, 20, 6, 23, 9, 8, 15] but are meant for classic one round polling.

The problem of support/rejection gathering for ideas is of a different type than usually addressed elections, needing a homogeneous process. Namely, classical techniques with stages (e.g. authorization stage, voting stage, claiming stage, counting stage) do not fit well. In the techniques shown further the authority can reconstruct the identity of the participants (with a certain effort). The techniques we would apply in a first development only try to increase the complexity of the effort a single person in the authority should need to illegally break privacy. We hope that future research could lead to even more complete solutions. The techniques we propose combine versions of anonymous channels, with secret sharing, digital signatures and blind signatures.

For robustness, and as a deterrent from breaking of the privacy by individual persons in AFW administrations, we propose to first investigate the alternative of having the evaluation grades submitted using (t,n) Shamir secret sharing. Then, n distinct physical AFW sharing servers can be used for shared storing of the grades: pairs of support-rejection (0 or 1, where the sum for support and rejection is 1). Once the sum of the grades is computed with a secure multi-party computation [32, 2], it can be verified that any t of them lead to the reconstruction of the same result, which is the current pol's result.

Periodically (since some citizens die, lose/acquire rights, errors are detected: e.g. more credentials than eligible participants), the setup procedure is repeated semi-automatically between registered software agents of the eligible users, the authority and AFW sharing servers. The process is not fully automatic since human involvement is needed to avoid involvement from computer viruses. A citizen should be able to erase the history of the evaluations associated with his credential, which can be done automatically when he chooses a new credential.

4.2.2 Secure Tallying

Both support and rejection grades will be submitted as encrypted (t,n) Shamir shares and associated with:

- the private credentials of the evaluator,
- the ID of the evaluated idea,
- an encrypted number used for ordering changes of decision, as well as
- an encrypted semi-randomly generated number (number whose first part is generated with a pseudo random generator, while the second part is input manually by the user) which will be published on the appropriate list: support, reject, undecided,
- a digitally signed message for each AFW (shares and ID of evaluated idea), and

- optionally, a withdrawal status.

The AFWs receive the ballot, check the credential of the evaluator and register the credential and the ID of the evaluated proposal in a database (respectively remove them if the withdrawal status specifies so). The submission, after removing the citizen credential, will then be shuffled with other ballots for the same proposal (e.g. by using shuffling techniques for Paillier-encrypted secret shares as we did in [27]). In the end, each AFW decrypts the random number and its share.

In the citizen-sourced & ranked polls with civic discourses support framework, AFWs can daily (or in chunks) rebuild the secrets checking that several/all combinations of t shares reveal the same grading and classify the corresponding random number on the appropriate list as: support, rejection, or borderline. For several evaluations with identical random numbers, only the one with the highest ordering number is taken into account.

The system can be used with one-shot polling, namely where partial results are not officially revealed before the end of the process. There, the shares will be secrets of individual physic AFWs until the closure of the polling.

4.2.3 Verification of the tally

Part of the security verification, each user can have a profile where she keeps track of proposals she evaluated, as well as withdrawals. Users can also have agents that automatically check for them the consistency of the grading they have made with the data currently published on the AFW.

A simple technique for achieving accuracy, democracy, convenience, and verifiability consists in assigning each participant a private credential (an authorized digital signature, a big number generated randomly). The credential can be used for verification by publishing those used for either supporting or rejecting each given proposal (mixing grades for support and rejection). By separately publishing all user credentials, one can make sure that no illegitimate grading is introduced. Each participant can check that his own grade is counted correctly by associating each grade with a new semi-randomly generated code that is listed on AFW either as support, rejection, or undecided. Each participant can keep a copy of each proposal it graded, to make sure that no modification is illegally performed on it by the AFW administration.

This simple technique can even achieve acceptable privacy (except the fact that proof/receipts can be generated by revealing one's secret keys for credentials).

If an eligible participant finds that his grade is not published correctly on the AFW (even after eventual repeated resubmissions), he can add a TRACE mark to his resubmitted evaluation. All servers shuffling the evaluation (except for the anonymous channel) will have to store all permutations and transformations performed on that ballot. Later inspection can then reveal the faulty agency, or correction to the evaluation is done. All tracing information stored for evaluations requiring it will be published on AFW such that the author can study it anonymously, and everybody can detect errors. If data on a required traced evaluation does not appear on the AFW, the user can suspect the anonymous channel. Alternative anonymous channels (mix nets) can be provided for these cases.

If the number of posted grades for a given idea is higher than the number of credentials registered as having submitted a grade, then the AFW are faulty and they should just replay the mix-net for redistributing the shares and recomputing the tally for the corresponding idea. Due to its properties of ensuring correct tally with verification, our techniques can also be used for gathering signatures for supporting popular initiatives petitions, as they exist in some democratic organizations.

4.2.4 Semantic language filtering and automated consistency checking

One issue that has to be solved is to avoid spam messages, and a large amount of research focuses on spam in Internet [18]. For our application, when submissions can be made only by verified eligible participants then the spam can be reduced. Spam can be completely removed when it is well defined. (e.g advertisements of products, use of offensive vocabulary, illogic constructs). In fact, AFW can provide some degree of automated verification of submitted proposals, and identified proposers using predefined inappropriate language can be temporarily blocked from submitting additional proposals or comments.

A degree of acceptability of texts can be automatically enforced/verified, e.g. enforcing a certain grammar, or alternatively using techniques that translate English legal text into logic knowledge representation [31]. This way, some illogic or incoherent proposals can be automatically filtered out, and the author can receive feedback such that he can correct his errors. Moreover, given additional research advances, the system may automatically detect articles of other applicable norms that conflict with the new proposals and can thereby help/force authors in specifying better the implications of their proposals. Several people worked already on related issues [21, 29, 30] and there is place for many future contributions to improve automation of this step and to require only reasonable human effort for treatment of complex proposals.

Automatic analysis of natural language is difficult. Therefore, to define a consistent framework for allowing fair mass submission of proposals while avoiding spam, in the beginning we will restrict formulations to a strict grammar based on a consistent ontology [31]. This grammar is expected to be too poor for expressing all needed proposals, and we are designing a way to let people help in expanding the grammar. A scalable way is to use a special submissions channel dedicated to extending grammar where support from a large fraction of the users would suggest priorities for add the new terms and structures to the allowed grammar.

Techniques to offer advanced graphical user interfaces that detect grammar conflicts "as you type" and then intuitively guide users through possible alternative formulations are already available.

Research will focus on enabling automatic detection of simple inconsistencies of the proposal with existing norms:

Example 1 *If a citizen of a city proposes the next proposal on the AFW of the city:* "Let all the benches in the parks of the city be painted red, white and blue". *If the database of norms of the city contains a norm of the type:* "A bench in the parks of the city may be colored only in a single color"*, then logic formulations of the norms with an established ontology could help to automatically signal the conflict.*

Such conflicts can appear dynamically if new norms are adopted which conflict with on-going proposals. In theory, conflicts can be detected using logic inference (e.g. resolution), or different constraint processing techniques.

4.2.5 Cooperation in proposal text development

If an idea has already been shown on AFW for a while and has gathered significant support but a modification would improve it, it is desirable to avoid dealing with the modification as with a new proposal. Therefore, when somebody suggests a modification/reformulation to an existing proposal, the modification can be linked on AFW from the original proposal. All evaluators of the original idea can learn of the existence of a discussion on a modification (e.g. a star can be appended on their web page to the proposal that they have graded).

Participants could then submit different evaluations for all alternative formulations of an idea and can also submit relations of the type (proposal i can be abandoned for proposal j). A partial order between proposals can then be defined so: Proposal i is abandonable for proposal j if all evaluators that support the proposal i marked that it can be abandoned for proposal j. One can then remove/disable proposals that are abandonable for some other proposal.

4.2.6 Web Intelligence for presenting ideas

The research field of web intelligence focuses on analyzing and developing techniques for optimizing the visibility and usability of the information on the Web. There is a need to ensure fair visibility of both favorable and unfavorable comments. Some researchers lay efforts for improving the selectivity in browsing web forums, but the nature of such forums reduces the possibilities to scoring to probabilistic criteria [1], which are not acceptable for the level of fairness expected from our system.

In our case, we are concerned about the visibility of ideas as well as the visibility of comments and we need an objective scoring. Fortunately, the identifications we will implement in our application allowed us to devise a much nicer solution [26]. Available comments will be presented to readers in two classes, namely favorable/unfavorable, and in the decreasing order of the number of associated support/rejection grades. This will lower the chances that a favorable comment is passed as unfavorable or vice-versa. To give opportunities for civic discourses, and to help find replies, threading will be enabled. Namely, each comment will be allowed one main link to another comment which the source comment claims to respond to, as in standard forums. Each comment will be displayed with the list of comments claiming to respond to it, listed in the decreasing order of the evaluations confirming those comments. The technique used by [10] to retrieve ideas appreciated by participants with similar opinions will also be evaluated. The agents of the users can extract such informations based on the partial reuse of credentials.

The privacy of the ideas that a user chooses to view can be ensured in a variety of ways. Some vendors even provide anonymization techniques, where a user should trust the vendor [17, 13, 11].

4.2.7 User adaptation

In active and vocal communities citizens could face large numbers of proposals, many of which could be of little interest to the majority. Allowing individuals to efficiently identifying worthwhile proposals is crucial in gathering public opinions. One usual method is to organize the proposals hierarchically based on some ontology and provide a search engine for easy navigation—this still requires the participant to do most of the work in identifying relevant proposals. A more sophisticated method asks the user to specify keywords of interest into her profile and proposals with matching keywords are recommended to the user. Though the second method can help the user focus on proposals that match her interests, the user needs to manually build the profile. Furthermore, changes in the interests of the user require manual changes to the user profile. We propose machine learning techniques that can identify a user's interests by observing her past behavior: in which proposals she chose to read or not and which proposals she selected to grade or not. This has the advantage of building the user profile in an automated manner as well as the ability of the profile to adapt to changes in the user's interests.

Our previous work in using machine learning techniques for constructing user profiles in the context of web documents mainly relies on features in the documents. In [3] we investigate individual words and automatically constructed phrases as features for the user profiles. To construct phrases,

we proposed AEMI (Augmented Expected Mutual Information) to not only gather evidence of correlation between two events (word pair in our case), but also discount counter-evidence of correlation. In [16] we investigate profiles that can characterize general to specific interests in a hierarchy. A hierarchical profile allows a more refined characterization of interests and different levels of matching in interests. For example, documents matching more general interests receive lower scores than those matching more specific interests.

Features other than words in the proposals could be beneficial for identifying relevant proposals for individual citizens. These features include the address of residence, age, and other information that is required to establish eligibility for grading a proposal. Though user profiles could contain personal information as features, privacy is maintained since the profiles are not revealed to the public, are not directly related to values of grades, and are as protected as the personal information used for registration. Also, the profiles are only used to generate relevancy scores for ranking the proposals and only ranking information could be exposed to possible sniffing during communication on the network.

References

[1] Andrew Arnt and Shlomo Zilberstein. Learning to perform moderation in online forums. In *Web Intelligence*, October 2003. NSF, Information and Data Management Program.

[2] Josh Benaloh and D. Tuinstra. Receipt-free secret ballot elections. In *26th ACM Symposium on Theory of Computing*, pages 544–533, 1994.

[3] P. Chan. Constructing web user profiles: A non-invasive learning approach. In B. Masand and M. Spiliopoulou, editors, *Advances in Web Usage Mining and User Profiling*, pages 39–55. Springer Verlag, 2000. LNAI 1836.

[4] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, 1981.

[5] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, October 1985.

[6] D. Chaum. The dining cryptographers problem: Unconditional sender and recipient untraceability. *Journal of Cryptology*, 1(1):65–75, 1988.

[7] L. Chen. Access with pseudonyms. In *Cryptography: Policy and Algorithms*, number 1029 in LNCS, pages 232–243, 1995.

[8] W. Dai. Pipenet 1.1. www.eskimo.com/ weidai/pipenet.txt, 2000.

[9] D. Goldschlag, M. Reed, and P. Syverson. Hiding routing information. In *Information Hiding*, number 1174 in LNCS, pages 137–150, 1996.

[10] Amazon.com Inc. Amazon. http://www.amazon.com, 2004.

[11] Anonymizer Inc. Privacy is your right. http://www.anonymizer.com/.

[12] Kuro5hin.org Inc. Kuro5hin. http://www.kuro5hin.org/special/faq.

[13] Somebody Inc. Somebody. www.somebody.net.

[14] Zero-Knowledge Systems Inc. Private credentials. http://www.zeroknowledge.com/media/credsnew.pdf, 2000.

[15] M. Jakobsson, A. Juels, and R. Rivest. Making mix nets robust for electronic voting by randomized partial checking. In *USENIX*, 2002.

[16] H. Kim and P. Chan. Learning implicit user interest hierarchy for context in personalization. In *Proc. Intl. Conf. on Intelligent User Interfaces*, pages 101–108, 2003.

[17] IDzap LLC. Idsecure anonymous browsing. www.idzap.com.

[18] T. Loder, M. Alstyne, and R. Wash. Information asymmetry and thwarting spam. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=488444, January 2004.

[19] A. Lysyanskaya, R. Rivest, and A. Sahai. Pseudonym systems. In *Selected Areas in Cryptography, SAC*, number 1758 in LNCS, pages 184–200, 1999.

[20] M. Merritt. *Cryptographic Protocols*. PhD thesis, Georgia Inst. of Tech., Feb 1983.

[21] Laurens Mommers. A knowledge-based ontology of the legal domain. In *Second International Workshop on Legal Ontologies*, 2001.

[22] C. Andrew Neff. Verifiable mixing (shuffling) of elgamal pairs. http://www.votehere.com/vhti/documentation/documentation.htm, December 2003. VoteHere.

[23] Tatsuaki Okamoto. Receipt-free electronic voting schemes for large scale elections. In *5th IW on Security Protocols*, Berlin, 1998.

[24] R. Samuels and E. Hawco. Untraceable nym creation on the freedom 2.0 network. http://www.zeroknowledge.com/media/Freedom-NymCreation.pdf, 2000.

[25] M. Silaghi. Verifiable private credentials. To be submitted, 2004.

[26] M. Silaghi and C. Kaner. Fair comment scoring for polling. To be submitted to WIAS, 2004.

[27] M.C. Silaghi. Solving a distributed CSP with cryptographic multi-party computations, without revealing constraints and without involving trusted servers. In *IJCAI-DCR*, 2003.

[28] Slashdot. Slashdot faq - comments and moderation. http://slashdot.org/faq/com-mod.shtml#cm703, December 2002.

[29] Robert van Kralingen. A conceptual frame-based ontology for the law, 1997.

[30] Pepijn R. S. Visser and Trevor J. M. Bench-Capon. A comparison of four ontologies for the design of legal knowledge systems. *Artificial Intellgence and Law*, 6(1):27–57, March 1998.

[31] Pepijn R. S. Visser, Robert W. van Kralingen, and Trevor J. M. Bench-Capon. A method for the development of legal knowledge systems. In *International Conference on Artificial Intelligence and Law*, pages 151–160, 1997.

[32] A. Yao. Protocols for secure computations. In *FOCS*, pages 160–164, 1982.