Internet Voting

Jordi Barrat i Esteve
Universitat Rovira i Virgili, Spain

Jordi Castellà-Roca
Universitat Rovira i Virgili, Spain

Josep Domingo-Ferrer
Universitat Rovira i Virgili, Spain

Josep Maria Reniu i Vilamala
Universitat de Barcelona, Spain

LEGAL REQUIREMENTS AND TECHNICAL SOLUTIONS

Internet voting denotes electronic voting (e-voting) systems that allow votes to be cast using the Internet. There are, however, other types of e-voting, like those based on optical ballots, those using computers without remote connection or those sent by phone (Kersting, 2004; Tula, 2005). All these systems can be used in political elections or private ones (binding examples of Internet voting: the 2000 Democratic primary in Arizona or an election in a chapter of the Institute of Electrical and Electronics Engineers in 1997).

Since Internet voting will be applied to a democratic framework, it should offer the same conditions required in traditional elections (Cranor, 1997; Gritzalis, 2003; Prosser, 2004; Trechsel, 2005). Therefore, the suffrage must be at least universal, free, equal, and anonymous (Mitrou, 2002).

Universal voting means that any person entitled to take part in an election should be able to cast a vote, and this in an authenticated manner to avoid impersonation by malicious third parties. An identification procedure is required to *authenticate* the voter, which entails more difficulties than the traditional exhibition of a paper identification (ID). There are at least three approaches to identifying the user of an Internet voting system: through something the user *knows*, the user *is* or the user *has* (Schneier, 1996).

Knowledge of a username and the corresponding password is the most widely used identification procedure ("something the user knows"). It has the advantage of simplicity and usability by a vast majority of users. Nevertheless, it has two major problems. This system makes vote selling very easy, since the voter only needs to send his or her username and password to the buyer. The second problem is the trade-off between security and usability. Reasonable security requires long passwords, which increases the risk of typing errors by voters.

The second approach is to use a public key infrastructure (PKI) (Adams, 1999). In this case, every voter has a key pair of a public-key cryptosystem ("something the user has") and that public key is certified, for instance, by the electoral authority. Since the voter is authenticated with his or her digital signature, this system requires a high protection of the voter's private key to avoid its unauthorized use by another citizen. A user-held cryptographic token or smart card is a good solution to store and operate the user's private key, because such hardware devices can be regarded as being tamperproof in most practical situations.

Biometric identification is the third approach to identification ("something the voter is"). It is the oldest form, because physical recognition is a biometric procedure used not only by humans but also by animals. The voter uses a device that obtains a biometric measurement; for instance, a fingerprint. This measurement or pattern is sent to the authentication service that verifies whether it matches the data previously stored about the voter. Important issues when using biometrics to authenticate a voter are: (1) to ensure that the biometric pattern came from the right person at the time of the verification; and (2) to ensure that the collected pattern matches the one stored for the voter (both patterns are likely to be slightly different due to measurement errors or variable biological conditions, so exact matching is unlikely even if both patterns correspond to the same person).

A combination of several of these three identification approaches is a sensible solution.

Freedom is another important requirement that may be jeopardized if the voter receives inaccurate information

during the voting procedure. It should be realized that information technologies greatly facilitate these kinds of inputs (i.e., political pop-ups). The voter should also receive complete, accurate and understandable information about the operation of the Internet voting system. Therefore, training campaigns and on-site assistance are required.

Internet voting, although it can also be used in controlled polling stations, is particularly attractive in a distributed scenario where the vote is allowed from any computer (i.e., from home). However, a distributed scenario entails additional dangers because it becomes possible to create a voting market, even a massive one, or to practice extortion upon some citizens (i.e., the employer upon employees). An Internet voting system not used in official polling stations can hardly eliminate these problems, and the solutions—criminal protection or a reduced application to some specific groups of voters (i.e., citizens living abroad)—may not be enough from a democratic point of view. This is, therefore, one of the key problems of Internet voting (Jefferson, 2004). However, some countries currently admit postal voting, which is subject to similar dangers; thus, Internet voting could also be acceptable to those countries. It is actually a social and cultural problem.

Additionally, freedom in voting requires adapting to the electoral tradition of each country. An electronic vote should not reduce or eliminate the idiosyncrasy of an electoral system. For instance, blank votes and especially null votes cannot always be analyzed as voter's errors. They are part of political behavior and, if they are allowed in traditional systems, they must also be included in any Internet voting procedure (Barrat, 2004).

An *equal* vote requires that voters and the candidates receive a correct treatment. Therefore, the voting system screen should be designed to avoid any discrimination. The order of the political parties and their logos must be carefully established. It is also compulsory to have a simultaneous exhibition of all candidates, since using multiple screens would benefit the first ones. On the other hand, the system must avoid multiple votes by the same voter and should not exclude a citizen legally entitled to vote. Finally, equality requires a system that can guarantee the accuracy of the results; in particular, it should be impossible to change or delete a vote already cast. While perfect accuracy will avoid these situations or, at least, will detect and solve them, a system is said to provide partial accuracy if it is able to detect manipulation, but unable to solve it.

The digital signature is a good tool to provide these accuracy and integrity properties (Fujioka, 1992). The digital signature yields proof that the vote has been cast by a valid voter and has not been modified afterwards. Specific storage devices that do not allow information to be erased once it has been written can also be used. Nonetheless, security properties of an Internet voting system are ultimately dependent on the software implementation; therefore, the security properties of a system must be auditable (*vid. infra*).

The *anonymity* of the vote means that nobody, not even the electoral board, can link the content of one vote with the person who cast it. The system should also avoid the disclosure of partial results. The traditional procedure achieves these goals in a very simple way: a ballot (with or without envelope) is inserted into a transparent urn that can be controlled by any voter until the final tally. An Internet voting system cannot offer a similar procedure, since anonymity depends on the software source code and a citizen without technical knowledge cannot check it.

The anonymity of the vote and the secrecy of the intermediate results are usually assured by the encryption of the vote with the public key of the electoral authority (Benaloh, 1986; Chaum, 1988). However, the private key used to decrypt the votes protected with the public key is a very sensitive piece of information. It is not desirable that this key be possessed by just one person because that person can be an easy target for coercion. A usual strategy is to split the knowledge of the key between the members of the electoral board using a cryptographic threshold scheme that requires a pre-set number of board members to recover the private key (Shamir, 1979). If the number of co-operating board members is less than the threshold previously fixed, they do not obtain any useful information about the private key.

On the other hand, there are two basic methods to guarantee privacy and anonymity in an electoral procedure: mixing (Chaum, 1981) and homomorphic encryption (Benaloh, 1986).

In the first one, the voter obtains an authorization token issued by an electoral authority. There are several methods for obtaining the token anonymously, so that the election authority cannot later link the token with a particular voter (Sako, 1995; Nurmi, 1991; Fujioka, 1992). In the second step, the voter sends his or her vote and the authorization token using an anonymous channel implemented with a set of servers—"mixing servers": each server receives the votes, permutes their order and re-encrypts and sends them to the next one. Once the last mixing server has sent the votes the tally process begins. Every vote is decrypted and the server verifies that the authorization token is valid. These mixing server operations are complex and current research focuses on obtaining a mixing method that can be efficiently and universally verified.

In the homomorphic protocol, the voter encrypts his or her vote and computes a proof that demonstrates the correct construction of the vote. The proof does not

reveal any information about the vote. The voter sends the encrypted vote and the proof to the election authority. All the encrypted votes are multiplied together, and decryption of the final result yields the sum that would have been obtained by adding votes in the clear. The key used to decrypt the vote is divided among several authorities that must co-operate in the decryption process to obtain the final result. There are methods to check the accuracy and correctness of the process so that, in this case, universal auditability is guaranteed. However, the computation of the proof to demonstrate the correct construction of the vote is complex, which can be a problem when the voter's computing device has restricted computational power (as is the case if the voter computes his or her vote using a smart card). A second drawback is that the ballot format is limited, so that it does not allow complex voting procedures (i.e., write-in candidates).

Technology is a key factor, but it is not the only matter of concern. We have already seen some legal aspects that must be addressed with the technological ones. Essential elements of any voting procedure, like the correct identification of the voter, the anonymity of the vote and the correctness of the tally, are not easy to verify in Internet voting, whereas they are straightforward in traditional systems. An effort to improve *auditability* in Internet voting is needed (Riera, 2002; Muralt, 2003). Nowadays, the only really accurate option is a complete software audit. Some systems give a receipt that could increase the voter's confidence. When the system is used in a polling station, there can be a paper receipt with several options: a receipt with only participation data, a receipt with the content of the vote that could be given to the voter so the voter can insert it in a traditional urn or, finally, a receipt with the content of the vote shown only to the voter. In the latter option, the voter sees the receipt, checks that its content is correct, confirms the vote and finally the machine itself puts this receipt in an internal urn. If the system is not used in a polling station, no receipt with the content of the vote can be issued because this solution could facilitate voter coercion. Some technical solutions give the voter a code for his or her vote, and afterwards the electoral board publishes them together with the tally.

However, the solutions based on receipts do not guarantee individual nor universal auditability. Paper receipts certainly allow a manual tally to be computed to confirm the electronic one; in practice, this option is seldom used, because it severely diminishes the speed attractiveness of electronic voting. In the case of a receipt with a vote code, the citizen must make confidence to electronic data that he cannot check. As said above, performing a complete audit of the voting software is the most rigorous approach. Therefore, at least from a legal point of view, the implementation of the voting system should be totally transparent to allow any citizen, and not only the electoral boards, to check the code.

The system should be audited before, during and after the election. Before the election, the devices and the software used must be audited and sealed so that it will be detected if they are tampered with. The use of open source code should be viewed as a good practice, because security experts and the entire community could help to detect and correct errors. During the election, all actions must be logged, because this information will help to find and repair any errors. Finally, the seals and the information recorded must be verified after the election to make sure that no abnormal circumstance happened.

SOCIO-POLITICAL FRAMEWORK

From a socio-political perspective, the use of Internet voting raises several issues for debate. We can differentiate those arguments against the use of Internet voting from those in favor of it.

Among the former, three main arguments are discussed: first, criticisms about the security and reliability of the Internet; second, problems that arise connected to the digital and social divide; and third, arguments related to the changes in the process for casting the vote itself.

The digital and social divide stands out as the most important issue (Norris, 2001). It focuses on the differences of technology use among citizens. So it is not just about how many citizens could have Internet access or which is the percentage of citizens that use computers (Demunter, 2005). The digital and social divide goes further: Internet voting assumes that citizens are not only able to use the Internet for voting, but also to become instructed and informed on the options/candidates they can choose from. Comparative data from various surveys shows a well-known picture where men have greater access to the Internet that women; younger people than older; richer than poorer; highly educated than those with lower levels of education and so forth. Thus, the concept might be widened, involving not only technological issues but socio-economic, cultural, educational and legal aspects.

Beyond the digital divide, there exist other arguments against Internet voting related to social perception. From that point of view, it is said that people are afraid of using new technologies. Some scholars argue that *off-line* people—those excluded or self-excluded from information and communications technologies (ICT)—do not feel confident enough to use Internet not just for voting, but also for anything else (e.g., using credit cards or shopping online). Such a *technophobia* may seem a bit

irrational, but is the consequence of most people being unable to understand how ICT work. In other words, people know *the existence* of those technologies, but do not know *how* they really work. For instance, while in traditional voting systems citizens can *see* both the ballot and the urn and can in principle attend the counting process, using Internet voting prevents them from doing so (Reniu, 2005; Barrat, 2004a).

For a significant number of citizens, the moment when votes are cast is still a strongly symbolic moment. Such citizens are reluctant to surrender the possibility of social interaction with other people in exchange for a number of alleged advantages inherent to casting the vote from home. Indeed, the moment of casting the vote is understood as a way of reinforcing socio-political identification with the community and implicitly renew the *res publica* social contract. In this respect, Internet voting is blamed for promoting strictly private behaviors, whereas the ultimate goal of elections is to elicit the general will.

On the other hand, arguments in favor of Internet voting are not limited to comfort for voters. The main positive reasons refer to increased participation enabled by information technologies both in terms of quantity and quality (Braun, 2005). On one side it is said that Internet voting provides more possibilities for citizens to take part in elections, especially for those living abroad, in isolated areas or experiencing difficulty to reach a polling station due to illness. Moreover, Internet voting stimulates people to participate because its update effect on the electoral process will result in a more informed citizenship. On the other side, the quality of participation will increase thanks to the vast amount of information available on the Internet that will help voters attain a well-informed opinion.

Last but not least, we have to take into account the economic and political benefits. Using Internet voting will not only reduce the cost of traditional elections—which require a substantial human and logistic deployment—but also will help environmental sustainability by reducing the use of paper. In addition, Internet voting allows quicker tallies that result in a reduction of uncertainty in electoral processes and thus reinforce the democratic legitimacy of the system. In conclusion, as several public opinion surveys point out, Internet voting will provide citizens with a fast, comfortable and easy-to-use way to take part in the governing process (Trechsel, 2005a).

REFERENCES

Adams, C., & Lloyd, S. (1999). *Understanding public-key infrastructure. Concepts, standards and deployment considerations.* Indianapolis: New Riders.

Barrat i Esteve, J., & Reniu i Vilamala, J. M. (2004). Legal and social issues in electronic voting. Report on the Catalan Essays during the elections of November 2003. In J. Padget, R. Neira, & J. L. Díaz de León (Eds.), *E-government and e-democracy* (pp. 129-137). Mexico DF: Instituto Politécnico Nacional.

Barrat i Esteve, J., & Reniu i Vilamala, J. M. (2004a). *Electronic democracy and citizen participation. A sociological and legal report about the citizen consultation "MadridParticipa."* Madrid: Ayuntamiento de Madrid.

Benaloh, J. C., & Yung, M. (1986). Distributing the power of a government to enhance the privacy of voters. *Proceedings of the 5th Annual ACM Symposium on Principles of Distributed Computing* (pp. 52-62).

Braun, N. (2005). E-voting—worldwide developements, opportunities, risks and challenges. *Reflections on the future of democracy in Europe* (pp. 115-119). Strasburg: Council of Europe.

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

Chaum, D. (1988). Elections with unconditionally-secret ballots and disruption equivalent to breaking RSA. *Lecture Notes in Computer Science, 220,* 177-182.

Cranor, L. F., & Cytron, R. K. (1997). Sensus: A security-conscious electronic polling system for the Internet. *Proceedings of the Hawaii International Conference on System Sciences*. Retrieved December 17, 2005, from http://lorrie.cranor.org/pubs/hicss/hicss.html

Demunter, C. (2005). *The digital divide in Europe*. Statistics in focus. 38/2005. Luxemburg: Eurostat. Retrieved December 15, 2005, from http://epp.eurostat.cec.eu.int/cache/ITY_OFFPUB/KS-NP-05-038/EN/KS-NP-05-038-EN.PDF

Fujioka, A., Okamoto, T., & Ohta, K. (1992). A practical secret voting scheme for large scale elections. *Lecture Notes in Computer Science, 718,* 244-251.

Gritzalis, D. A. (Ed.). (2003). *Secure electronic voting*. Boston: Kluwer.

Jefferson, D., Rubin, A.D., Simons, B., & Wagner, D. (2004). *A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE)*. Retrieved December 17, 2005, from http://servesecurityreport.org/paper.pdf

Kersting, N., & Baldershein, H. (Eds.). (2004). *Electronic voting and democracy: A comparative analysis*. Basingstoke: Palgrave Macmillan.

Mitrou, L., Gritzalis, D., Donos, P., & Georgaroudi, G. (2002). *Legal and regulatory issues on e-voting and data protection in Europe* (e-vote project). Mytilene: University of the Aegean. Retrieved December 17, 2005, from http://www.instore.gr/evote/evote_end/htm/3public/doc3/public/public_deliverables/d_3_4/e_vote_D_3_4_v22_20_02_02.doc

Muralt Müller, H., Auer, A., & Koller, Th. (Eds.). (2003). *E-voting*. Berne: Stæmpfli Editions.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty and Internet worldwide*. Cambridge: Cambridge University Press.

Nurmi, H., Salomaa, A., & Santean, L. (1991). Secret ballot elections in computer networks. *Computers & Security, 10*, 553-560.

Prosser, A., & Krimmer, R. (2004). *Electronic voting in Europe. Technology, law, politics and society*. Bonn: Gesellschaft für Informatik.

Reniu i Vilamala, J. M. (2005). *Improving citizen participation through the use of electronic voting. A sociological report regarding the Citizen Consultation on the "Huerta de la Salud" Park in the Hortaleza district.* Madrid: Ayuntamiento de Madrid.

Riera, A., Sànchez, J., & Torras, L. (2002). Internet voting: Embracing technology in electoral processes. In Åke Grönlund (Ed.), *Electronic Government: Design, Applications and Management* (pp. 78-98). London: Idea Publishing Group.

Sako, K., & Kilian, J. (1995). Receipt-free mix-type voting scheme—A practical solution to the implementation of a voting booth. *Lecture Notes in Computer Science, 921*, 393-403.

Schneier, B. (1996). *Applied cryptography, protocols, algorithms and source code in C* (second edition). New York: John Wiley & Sons.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*, 612-613.

Trechsel, A. H. (2005a). Curing democracy's ills? Modern technology and democratic procedures. *Reflections on the future of democracy in Europe* (pp. 45-50). Strasburg: Council of Europe.

Trechsel, A. H., & Méndez, F. (2005b). *The European Union and e-voting. Addressing the European Parliament's Internet voting challenge*. London: Routledge.

Tula, M. I. (coord.). (2005). *Voto electrónico. Entre votos y máquinas. Las nuevas tecnologías en los procesos electorales*. Barcelona: Ariel.

KEY TERMS

Blank Vote: A valid vote that does not choose any candidate or, in case of a referendum, any of the offered options.

Client Voting Platform: Electronic device used by the voter to cast a vote. It can consist of hardware only or both hardware and software.

Digital Divide: Sociological concept that underlines the different approaches of the population to the ICT. Both the access to these technologies and the know-how for using them emerge as key elements of a new social gap that depends on several factors such as country, economic status, age or gender.

Individual Auditability: The property whereby every voter can check that his or her own vote has been correctly cast and managed.

Manager Voting Platform: Electronic devices that manage the election and offer three basic functionalities: the reception of the votes, their tally and, finally, their publication.

Null Vote: A vote cast in an incorrect way (i.e., by introducing two different ballots in the envelope, introducing a non-official ballot, etc.). This vote can be cast inadvertently, but sometimes there are citizens who wish to cast an invalid vote to protest against something.

Universal Auditability: The property whereby anyone can check the whole electoral procedure and confirm the correctness of the final tally.