Why electronic voting?

Marco Prandini*, Laura Sartori**, Anne-Marie Oostveen***

** Università di Bologna, Department of Computer Science and Engineering, marco.prandini@unibo.it*

*** Università di Bologna, Department of Social and Political Sciences, l.sartori@unibo.it*

**** University of Oxford, Oxford Internet Institute, anne-marie.oostveen@oii.ox.ac.uk*

Abstract: *Scientists have been studying electronic voting for 30 years, and some countries have been using it for almost 20 years. Yet, arguments in favor of its adoption or against it usually take into account only a limited subset of the issues at stake. As we show in this paper, no study has ever tried to draw a comprehensive picture of the interplay between social and technical aspects of the voting process. We claim that this kind of interdisciplinary research is needed for the scientific community to be able to exert its positive influence on stakeholders. We propose some urgent research questions that to our knowledge have no clear answer.*

Keywords: e-Voting, security, trust, electoral process;

Acknowledgement: This research work has been supported by EINS, the Network of Excellence in Internet Science through EC's FP7 under Communications Networks, Content and Technologies, Grant n. 288021.

Electronic voting experiences already span a significant period of time. Computer scientists have been working on the subject of exploiting cryptography to secure elections for the past 30 years, and computer-aided real-world elections have been running for more than 20 years, since the deployment of DRE machines for binding national elections in the Netherlands in the late '80s. Even at the first look, there is an evident divergence between theory and practice over the critical issue of security. The academic literature proposes complex solutions to deal with the peculiar and often contradicting requirements of this application, whereas public bodies are barely taking into account the most basic design principles (Schryen & Rich, 2009; King & Hancock, 2012).

In addition to the technical gap, there is another issue that still requires investigation from a social sciences perspective: trust in e-voting system is a crucial element when it comes to the actual use of electronic system within the political process. There are very few analyses of the broader social implications of a technology-driven paradigm shift in the electoral process (Oostveen & van den Besselaar, 2004), and none about the effective awareness of voters about its possible consequences, especially if we acknowledge that technology is more than a set of neutral tools assisting the satisfaction of preexisting normative criteria (Witschge 2008, 79). Voting is a specific social practice, crucial in a democratic regime, because it represents a ritual expressing power relations and political values (Kerzter 1989). Changes in the ritual of voting (with its symbols and meanings) might lead to changes in the outcome of the electoral process, such as legitimization and accountability of the representative democracy. In the following sections, we review the available literature to the best of our knowledge, and we highlight some unanswered questions that we deem important to the adoption of electronic voting in political elections.

Security

> *"The will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures." (United Nations, 1948)*

Simplifying to the extreme, the two broad categories of technical requirements for a voting system come directly from the Universal Declaration of Human Rights. Universal and equal suffrage must be supported by *accessible* systems. Equality and freedom come from *security* measures guaranteeing that eligible voters are able to anonymously cast a single vote.

On the issue of accessibility, electronic voting is often waved by its supporters as the only way to reach the totality of voters, yet there are studies that confute this thesis (Oostveen & van den Besselaar, 2009). Better user-centric design processes and the progress in narrowing the digital divide could, in principle, lead to the solution of accessibility issues, since there are no contradicting requirements to satisfy at once. Thus, we will not discuss this aspect any longer.

Security issues are completely different. Equality can be guaranteed only if voters are properly identified to prevent unauthorized or double voting, and if cast votes cannot be modified without leaving traces or ignored in the count. Freedom can be guaranteed only when voters cannot be linked to their cast votes. For all practical purposes, the traceability and accountability processes that usually satisfy the former set of requirements clash against the latter.

Trust

Trust is an essential element of the democratic process especially regarding the secrecy and freedom to express a vote that will legitimate the choice of rulers for a whole country. Trust is also inherently linked to the idea of delegating power in a healthy representative democracy. Studies dealing with the key issue of measuring the "correct amount of trust" that e-voting systems deserve are progressing (Volkamer et al., 2011) although it is clear that technology is not a remedy for broken institutions, as the Brazilian case showed (Avgerou et al. 2013). Still, taking trust into account might lead to further improvements in the knowledge of barriers or drivers for users' acceptance of e-voting systems. In this domain, trust has a twofold meaning: it is a property of a technology and it is an attitude of the citizens. As we previously saw, it relates to the security of the system preventing frauds and guaranteeing the secrecy of ballots and the privacy of vote; it also relates to the amount of confidence citizens store in the electronic system. Trust as an attitude relates to the overall political and electoral process as well as to the trust towards institutions that guarantee fairness in the execution of the electoral process (Xenakis & Macintosh 2005). Another important factor affecting users' perception of e-voting systems is the confidence with ICT and the related culture (eg. the symbolic and practical meanings of ICT). Summing up we can state that trustworthiness as a property of the system is influenced by ease of use, accuracy, and convenience conveyed by a certain level of perceived usefulness of the e-voting system (Schaupp and Carter 2005). On the other hand, trust as an attitude relies on the general confidence in the political system and in the national ICT culture (Leidner and Kayworth 2006). How the properties of a technology and the attitudes of citizens interact in building a robust and trusted e-voting machine is an open topic.

The computer science approach vs. real-world experiences

Cryptography provides the mathematical foundations for secure communication, processing, and storage of data. Over the last 30 years, scientists have proposed various cryptographic protocols (too many to cite), some with excellent features, but all with a common weakness: the system is a black box that has to be blindly trusted by the users. More recently, there has been a strong interest in solutions providing *end-to-end verifiability*, in which cryptography is cleverly used to allow voters to verify that their vote has been correctly recorded, and even correctly tallied, without harming privacy. The most successful proposals are Helios, Scantegrity, and Prêt à voter. While not completely devoid of weaknesses (Prandini & Ramilli, 2012), they represent the state of the art in security. However, their actual level of security is directly linked to the effective voters' will to verify the correct execution of the electoral process. Is this an acceptable technical trade-off? Up to now, it seems this trade-off has not even been taken into account. Many countries started to test or even to massively deploy e-voting solutions, mainly based on two paradigms: Direct Recording Electronic (DRE), or online systems. DRE is the epitome of the black box approach, and has shown serious issues in almost every place it was used (Balzarotti et al., 2008; Oostveen, 2010, Gonggrijp and Hengeveld, 2007), leading to massive decertification in the U.S. and to their dismissal in The Netherlands[1] and in Germany[2]. Online systems have been used for political elections in various countries in Europe, again showing various vulnerabilities (Schryen & Rich, 2009), caused by such issues as designs conceived under unrealistic adversarial models and poor coding. Furthermore, pure online voting systems are intrinsically vulnerable to vote selling, family voting and coercion threats, which among other concerns convinced Norway to abandon online voting (Nestas & Hole, 2012).

The peculiarity of electronic voting in political elections

Less-than-perfect technologies are routinely used for important tasks. It is a sensible choice especially when their negative effects can be somewhat easily reversed (e.g. financial transactions) or when there is no better alternative anyway (e.g. modern surgery).

As for any other social and technical process, not every deliberation calls for the same level of security. Evaluating risks and benefits, it is easy to imagine scenarios where electronic voting is an appropriate tool for decision making: for example when frequency and timeliness are fundamental, and/or the results of the deliberation have limited effects or can be easily reversed.

Political elections, however, present a very different situation. We claim that the conditions to deploy electronic voting do not hold. Risk is proportional to opportunity, motivation and damage inflicted by an attack. We believe that each of these factors is present.

- *Opportunity*: many elections are won by narrow margins[3]. It is not necessary to take control of a large number of votes to completely overturn the results. While with paper ballots this must be done vote by vote, complex systems where traceability must be limited to ensure vote secrecy are the perfect environment to mount a stealth attack, which could prey on the (relatively few) easiest targets and the most effective vulnerabilities, with no need for ultra-high impact actions.

[1] http://wijvertrouwenstemcomputersniet.nl/images/c/c5/KST118412.pdf.

[2] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-019en.html

[3] http://en.wikipedia.org/wiki/List_of_close_election_results

- *Motivation*: even taking into account the difference between campaign promises and post-elections actions, some economic effects of having one party win over the other are quite easy to foresee (e.g. the attitude towards public spending in big infrastructures). With less-than-perfect systems, cybercriminals will be able to achieve almost any objective, given the right budget.
- *Damage*: the effects of a hijacked election are long lasting and affect a whole population. Reverting them could require decades; it could be outright impossible.

In short, we believe that before considering electronic voting systems for political elections, they should exhibit a set of security features not currently available in any existing proposal. Current efforts seem to be directed towards the development and adoption of metrics to evaluate the adherence of voting systems to the basic democratic principles (Neumann & Volkamer, 2014), so that public trust is based on scientific data rather than emotional factors (e.g. biased media campaigns) (Volkamer & al., 2011). But what if scientific measurements prove, as it would currently happen, that perfect security is not achievable? Should we stick with technical trade-offs between security and usability or should we consider social trade-offs before anything? By social trade-off we mean the autonomy for different actors (voters, politicians, policy makers, etc.) to state whether a voting system is acceptable. Different actors may have different imaginaries and agendas for using an e-voting system. Yet, there is a moral obligation to guarantee the democratic process, and again this moral attitude may differ from actor to actor. The role of the scientific community is to support an informed discussion taking into account the different positions and to make a decision on the democratic process considering both technical and social trade-offs .

Open questions

Some questions that could drive future research are stated here.

Is electronic voting inevitable?

While pencil and paper voting has its own long record of vote fraud, it continues to provide a solution which is hard to compromise on a massive scale without anyone noticing, and easy to verify without any particular skill or tool. Moreover, real-world experiences have contradicted the claimed usefulness of e-voting in terms of addressing declining voter turnout, exclusion of some social groups, and high cost (Simons & Jones 2012);

Is e-vote different from other social processes related to new technologies?

Commerce and payments are two processes profoundly changed by technologies (e.g. credit and debit card, online bank transfer) that are often compared to e-voting. Although confidentiality is also fundamental in the consumer decision of finalizing an Internet transaction, it is substantially different from an e-voting context (Choi and Kim 2012). Economic transactions require disclosing selected information in precise moments; political vote requires secrecy and total privacy.

Does e-voting lower the perceived importance of voting?

Voting via SMS or mobiles has been proved to be perceived as less urgent and important (Local Government Association 2002) but the population's growing ease with ICT (especially among younger citizens) with online public consultations or e-petitions cannot be ignored, paving the way for the next generation of e-voting systems.

Do citizen perceive the link between elections and their own lives?

If political disaffection is a feature of contemporary democracies, can e-voting reverse it? The young participate less and less in the political life but are said to be those who benefit the most from ICTs, especially when it comes to political and electoral participation. Yet, there is little evidence to substantiate this claim (Local Government Association 2002; Payne et al. 2007). On the other hand, older generation have higher levels of trust in political and democratic institutions, leading to higher confidence in e-voting systems. Should we fear that both disaffection and trust could lead citizens to underestimate the risks associated with the hasty adoption of e-voting?

Is an "open box" verifiable process more valuable than a black-box-based one?

From a user perspective, an extensive survey combined with more fine-grained qualitative work is required to understand whether an open or black box process is more valued and trusted and what the implications are for democracy. Should the technical evaluations show that the only viable solution is one that requires strong user cooperation, how do we ensure that citizens understand and appreciate it? Trust has to be cultivated both at the technology's security level and at the citizens' level. A first move is to understand that a voting technique is a socio-technical system that has to be designed taking into account specific technology features as well as users' perceptions and needs. A second step could be to adopt a social constructivist approach in order to grasp how power relations expressed and exploited within the traditional electoral process are affected by e-voting and their implications for the political rituals and social structures.

References

Avgerou, C. & Ganzaroli, A. & Poulymenakou, A. & Reinhard, N. (2007). ICT and citizens' trust in government: lessons from electronic voting in Brazil. 9th International Conference on Social Implications of Computers in Developing Countries, São Paulo, Brazil

Balzarotti, D. & Banks, G. & Cova, M. & Felmetsger, V. & Kemmerer, R. & Robertson, W. & Valeur, F. & Vigna, G. (2008). Are your votes really counted?: testing the security of real-world electronic voting systems. 2008 international symposium on Software testing and analysis (ISSTA '08). (pp. 237-248). ACM, New York, NY, USA.

Choi, S. O. & Kim, B. C. (2012). Voter Intention to Use E-Voting Technologies: Security, Technology Acceptance, Election Type, and Political Ideology. *Journal of Information Technology & Politics*, 9, 433–452.

Gonggrijp, R., and W. Hengeveld. 2007. "Studying the Nedap/Groenendaal ES3B Voting Computer: A Computer Security Perspective." *Proceedings of the Usenix/Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop* (Boston, MA). USENIX Association, Berkeley, CA.

Kertzer, D. (1989). *Ritual, Politics and Power*, Yale University Press.

King, M. S. & Hancock, B. (2012). Electronic Voting Security 10 Years after the Help America Vote Act. *IEEE Security and Privacy*, *10(5)*, 50-52

Leidner, D. E., and Kayworth, T. (2006). A review of culture in information systems research: toward a theory of information technology culture. *MIS Quarterly* 30(2), 357-399.

Local Government Association (2002) *The Implementation of Electronic Voting in the UK*. London: LGA publications. Retrieved August 6, 2014, from http://www.dca.gov.uk/elections/e-voting/pdf/e-summary.pdf

Neumann, S. & Volkamer, M. (2014). A Holistic Framework for the Evaluation of Internet Voting Systems. In D. Zissis & D. Lekkas (eds) *Design, Development, and Use of Secure Electronic Voting Systems.* (pp. 76-91). IGI Global pub.

Oostveen, A. & van den Besselaar, P. (2004). Security as Belief. Users Perceptions on the Security of Electronic Voting Systems. In A. Prosser and R. Krimmer (Eds.) *Electronic Voting in Europe: Technology, Law, Politics and Society. Lecture Notes in Informatics.* Vol.47, pp 73-82. Bonn: Gesellschaft fur Informatik.

Oostveen, A. & van den Besselaar, P. (2009). Users' experiences with e-voting: A comparative case study. *International Journal of Electronic Governance (IJEG). Special issue "Users and uses of electronic governance", 2(4),* 357 -377

Oostveen, A. (2010). Outsourcing Democracy: Losing Control of e-Voting in the Netherlands. *Policy and Internet* 2 (4) pp. 201– 220

Nestas, L. & Hole, K. J. (2012). Building and Maintaining Trust in Internet Voting. *Computer* , 45(5), 74-80

Prandini, M. & Ramilli, M. (2012). Internet voting: fatally torn between conflicting goals?. In J. Ramon Gil-Garcia, Natalie Helbig, and Adegboyega Ojo (Eds.). *Proceedings of the 6th International Conference on Theory and Practice of Electronic Governance (ICEGOV '12)*. (pp. 58-61) ACM, New York, NY, USA.

Payne, J. G. & Hanlon, J. P. & Twomey, D. P. (2007). Celebrity spectacle influence on young voters in the 2004 presidential campaign: What to expect in 2008. *American Behavioral Scientist*, 50(9), 1239–1246.

Schaupp C. & Carter, L. (2005). E-voting: from apathy to adoption. *The Journal of Enterprise Information Management 18(5)*, 586-601

Simons, B. & Jones, D. W. (2012). Internet voting in the U.S.. *Commun. ACM 55(10)*, 68-77.

Schryen, G. & Rich, E. (2009). Security in Large-Scale Elections: A Retrospective Analysis of Elections in Estonia, The Netherlands, and Switzerland. *IEEE Transactions on Information Forensics and Security, 4(4)*, 729-743

United Nations (1948). *Universal declaration of human rights.*

Volkamer, M. & Spycher, O. & Dubuis, E. (2011). Measures to Establish Trust in Internet Voting. In *Proceedings of ICEGOV 2011.* ACM Press, New York, NY, USA.

Witschge, T. (2008). Examining Online Public Discourse in Context: A Mixed Method Approach. *Javnost: The Public 15(2)*, 75-92.

Xenakis, A. & Macintosh, A. (2005). Trust Analysis of the U.K. E-Voting Pilots. *Social Sci. Computer Rev.* 23(3)

About the Authors

Marco Prandini works as an Assistant Professor at the University of Bologna (Italy), where he obtained a Ph.D. in year 2000 in the field of Electronic and Information Engineering. He teaches system administration. His research interests include systems security models, ranging from PKIs – with special regard to authentication and verification mechanisms – to operating systems and network protection, secure administration paradigms, privacy-protection technologies and e-voting.

Laura Sartori has a Ph.D. in Sociology and Social research (University of Trento 2002) and is Associate Professor in the Political and Social Sciences Department of the University of Bologna. She teaches methodology for social research and information society. Currently, she is carrying out research on political participation (online and offline behaviour, consultation and deliberation via electronic platforms), open government and sustainable Internet (consumer awareness and behaviour).

Anne-Marie Oostveen is a Research Fellow at the University of Oxford. Her work focuses on the interdisciplinary study of the design, uses and consequences of ICTs taking into account their interaction with institutional and cultural context.