Trust, secrecy and accuracy in voting systems

Roberto Casati

Trust, secrecy and accuracy in voting systems

Draft/Version of November 28, 2007-11-28

Roberto Casati
Institut Nicod,
Pavillon Jardin, Ecole Normale Supérieure,
29 rue d'Ulm, 75005 Paris, France
roberto.casati@ens.fr, casati@ehess.fr

Abstract: If voting systems are to be trusted, they not only need to preserve both secrecy (if requested) and accuracy, but the mechanisms that presenrve these features should be transparent, in the sense of being both understandable and accessible.

Secrecy and accuracy are desiderata of most voting systems. Sure enough, not all voting systems are bound to secrecy. Overt votes are possible or even requested in many circumstances, as happens with votes by raising hands. The rational for secrecy is oftentimes the necessity of freeing voters from external conditionings and blackmailing, and of preventing the exchange or sale of votes. On the other hand, all voting systems aim arguably at accuracy. In order for votes to count, they must be counted in a reliable way. Accuracy breaks down in a number of different elements, from making sure that everyone who has the power to vote is actually allowed to express their vote, that those who are not entitled cannot cast a vote, that no one votes twice, that it is possible to tell valid from non valid votes, and that each valid vote figures in the sum total.

Now, accuracy and secrecy do not coexist easily in a voting system. Intuitively, each individual voter can assess accuracy of the system if she can track her vote. But so being able to track one's vote means, in the norm, giving up secrecy. Raising hands in a small assembly allows each voter to make sure that all

votes, including hers, are counted: One can see one's voting token (the raised hand) in a population of other tokens. If, however, tokens are no longer connected with voters, so as to ensure secrecy, accuracy is delegated to counting agents, and is no longer assessable by the individual voter.

Voting systems that are to win the trust of the voting body are therefore faced with a dilemma. On the one hand, reinforcing secrecy means delegating accuracy. Trust in the secrecy of the system is accompanied in potential mistrust in its accuracy. On the other hand, trust in accuracy can be improved, but then secrecy will have to be given up.

Trust in accuracy has dominated some of the most spectacular debates about voting systems. The contested Florida results of the American Presidential Election of 2000 are a case in point. Most likely, the difference between the two candidates was below the error margin of the voting system. The recount made it apparent that the system was widely inaccurate. Even individual ballots were subject to dispute on some of their physical properties (a hole having been punched according to some specifications).

Indeed, voting systems can be inaccurate at many levels: at the level of the admission of registered voters at the poll (some voters may be erroneously excluded or included; others can be allowed to vote more than once), at the level of the recording of the individual intention (the ballot can be interpreted in different ways), at the level of data transmission to a central system, and at the level of adding votes (both in local constituencies and at the central server). Weaknesses in accuracy are, of course, open doors to frauds of various types. These can occur, however, even if each step of the system is in itself accurate. On top of the accuracy of the various steps (local accuracy), a system should be globally accurate, in that all steps should be implemented.

Electronic voting systems (EVS) promise to put an end to the accuracy issue, at least in principle. All steps of the systems are dealt with algorithmically by a machine, and the whole system is but a complex machine implementing a comprehensive algorithm. Provided the algorithm is built to count all votes expressed, and input is fed correctly into the machine, the EVS is accurate. In principle, the algorithm is just a sum with a large number of addends. Provided addends are entered properly, the result is relatively straightforward. In particular, such a simple principle is understandable by the voters.

What about secrecy? Secrecy is dealt with in EVS by requiring that only the machine knows the voter's intention, which is not transmitted to anyone else. For instance, voting may be encrypted; voters may get a receipt that their vote has been cast correctly (one that does not report the voter's choice, of course).

Now, no matter what the specific implements for dealing with secrecy and accuracy, issues of trust are exacerbated by EVS. How can the individual voter *know* that her voting intention is not kept by the system in close association with her identity, or that her validly expressed intention is counted by the system?

Consider simple paper voting, by using a procedure that allows registration and ensures ballot accuracy (i.e., each entitled voter can vote once at most, and voter's intentions can be expressed unambiguously on the token). What typically happens is that once the identity of the voter is ascertained, and her right to vote is confirmed, it is *the voter herself* who takes an anonymous ballot to the cabin, votes on it, and drops it into the urn. That is, the *link* between registration accuracy (which requires an id check) and the subsequent steps of the voting process is *broken by the voter herself* – the act of breaking it is literally taken by her in her hands. Trust in this step is hence a trivial, transparent issue, insofar as the mechanism implementing secrecy it is both easily understandable and actually accessible to the voter: the voter has only to trust herself. (It can be alleged that paper (or physical in general) ballots are not exempt from traceability, as each ballot could be identified by traces imperceptible to the naked eye. However, this problem can be solved by allowing voters to randomly choose their ballot from a pile.)

At the next step of the voting process, ballots are dropped into an urn and get mixed with anyone else's ballots; this is the final guarantee that secrecy will be kept. Trust in secrecy depends on the fact that the voter has an implicit knowledge of the working of the urn. She knows that unless everyone votes like her, or unless she is the only voter, it will be impossible to know what she have voted for. She also knows that it will be near impossible to figure out the order of ballots from the pile inside the urn. Easy to figure out statistical facts, and physical properties of the urn's content, are perfectly accessible to the voter.

At the further steps of the voting process, that involve counting, voters, or their party representatives, can be present at the count. Discussions can of course ensue, and disputed votes be reported, but the highly intersubjective procedure is within the grasp of the participants. Once the local count is over, the results are made available to the central system. When the final results are published, the local results are printed alongside with the local ones, so that each constituency can verify that their results are accurately reflected in the list of addends for the sum total. Checking the final result, at this point, is only a matter of checking a large sum.

Furthermore, should doubts arise, records for each poll are kept and votes can be, under certain circumstances, recounted.

The key point here is not simply that the whole process guarantees, in principle, both accuracy and secrecy. It is rather that the factors that ensure accuracy and secrecy are perfectly transparent to anyone willing to reflect on them.

EVS can be protected against fraud and errors in many ways. However, it is obvious that understanding the mechanisms for the protection, whatever they are, requires specialized knowledge, and not just the willingness to reflect upon the different phases of the process. No matter what the sophistication of the mechanism – indeed, because of that very sophistication – the preservation of privacy and the accuracy of the count will be not assessable by the lay person. Understanding of electronics, of data transmission, of encryption will prove crucial to accepting the ESV as reliable, hence to trusting it.

The accuracy of EVS can be, to a point, tested by lay people. For instance, spot checks, or parallel shadow voting can be run on the system, possibly during an election, so that accuracy is tested on the fly, as if it were. But the point remains that all those tests presuppose insider understanding of the system, and a complex organization to run them. Besides, were such checks routinized in EVS, the whole point of delegating voting to machines would become rather moot. As to secrecy, its testability is, to my knowledge, beyond lay access.

There are general objections against electronic voting. One is that voting, at least on certain issues, should not become an "effortless" procedure: a difference should be kept between voting and just expressing an opinion, and votes are not opinion polls. EVS should then be rejected because they would narrow the gap between voting and opinion polling. Another objection is that the costs of counting votes manually are not so high, and that the accuracy of manual systems is largely underestimated (for instance, manual counts in Switzerland are performed very quickly, within hours of the closure of the polls). Much as these objections evoke important points, the main reason for keeping manual voting is related to its intrinsic open structure, which can be checked simply and effectively at all crucial junctions by every voter, thereby enhancing trust. No matter what the benefits of electronic voting, these will never be enough to overcome the wide gap between them and manual voting on the issue of trust.

The main result of this discussion is it is not sufficient that a voting system effectively protects both secrecy (if requested) and accuracy. *Transparency* of the mechanisms that ensure secrecy and accuracy is a desideratum as well. Transparency means here that the key steps of the mechanisms be both *easily understandable* and *in principle accessible* to each individual voter.