

Challenging an e-voting system in court

An experience report

Richard Hill

Hill & Associates, Geneva, Switzerland
rhill@hill-a.ch

Abstract. The Swiss political system is decentralized, and this includes voting operations. Several cantons have implemented Internet-based e-voting systems. The system used until recently in Geneva was a simple Internet voting system which assumed that the voter's personal computer had not been compromised. This was considered risky already at the time and various counter-measures were considered. The one that was implemented in practice was to limit the proportion of voters that could vote via Internet. At present, there is consensus amongst experts that such systems are unsafe and should be improved, in particular by implementing verification. In order to stimulate improvements in the system, the author challenged the use of the Geneva system in court, arguing that it was not compliant with constitutional principles and cantonal law on voting rights. At the end of a long and complex legal process, the Swiss Federal Tribunal (supreme court) ruled that the complaints could not be heard on their merits, because they did not allege that weaknesses had actually been exploited in a specific vote. This decision differs from those taken in other jurisdictions and highlights the difficulties of bringing scientific arguments into the court system.

Keywords. E-voting. Internet voting. Court challenges to e-voting.

1 Introduction and Background

Switzerland is a federal state: the subdivisions are called cantons and communes. Although most laws in Switzerland are federal and apply throughout the country, that is not the case for many administrative matters such as taxation and voting. Fundamental voting principles are specified in the Federal Constitution and in the federal act on political rights. Lower level measures are included in the federal ordinance on political rights. Federal provisions apply throughout the country. But, within the limits specified by those principles, cantons are free to organize and administer elections as they think best. A detailed explanation of this complex situation is given in [1].

E-voting was introduced gradually and in a controlled manner (that is, with restrictions on its use), since the early 2000's. Internet voting has been used for federal votes since 2003. A comprehensive overview is given in [2]. The proportion of Internet voters is limited to 30% of the cantonal electorate and 10% of the federal electorate. About half of the 26 cantons use Internet voting systems and most of them are not

close to reaching the authorized limits [1]. In Geneva, about 20% of the voters who have the possibility to use Internet voting do so and the introduction of Internet voting did not increase the rate of participation [3].

The introduction of Internet voting was greatly facilitated by the fact that correspondence voting is widely used in Switzerland, and Internet voting was viewed as a natural extension of correspondence voting [1, 4].

The canton of Geneva started to use Internet voting in 2003 in trials at the communal level, and used it for a federal vote in 2004 [1]. During the early stages of the development process, computer experts identified the risks associated with Internet voting and recommended measures such as the development of a dedicated operating system that would be distributed on CD ROMs and uploaded by voters on their personal computers for the vote, but such measures were rejected as being too complex: it was felt that they would discourage use of the Internet voting system [4]. For similar reasons, solutions involving coded voting [5] were not implemented.

The system that was implemented was basically an electronic version of the correspondence voting procedure. The system is not fully electronic: the voter needs the very same paper material used for correspondence voting. The identification codes that prevent voters from casting multiple votes are provided in the correspondence voting material. Proxy voting is not allowed in Geneva. In order to prevent (or at least discourage) proxy voting, the voter must sign the identification card used for correspondence voting: this card must be sent to the voting authorities, but it is of course separate from the actual ballot, so anonymity of the vote is preserved. In the case of Internet voting, voters must provide their birth date and commune of origin (each Swiss citizen is associated with one or more commune of origin). In families, family members typically know the birth date and commune of origin of other family members.

When a voter accessed the Geneva Internet voting system that the author challenged, Java applets were downloaded to the voter's PC (the system has been modified and continues to evolve). Various sophisticated encryption measures are used for the communications between the user's personal computer and the state's servers. A detailed description is given in [6]. But the system used in 2011 did not have any provisions for verifiability (see [7, 8, 9] for a discussion of that technique) nor were any particular measures foreseen to check whether a user's personal computer had been compromised by malware [5, 7]. In June 2013 a computer engineer demonstrated that it was relatively easy to insert in the voter's personal computer malware that could modify the voter's vote before it was encrypted and sent to the state's servers, and this without the voter being aware of the change [11].

Geneva cantonal law does not limit the proportion of Internet voters, but this has no practical effect for most votes, because cantonal votes are held in conjunction with federal votes, so the federal limits apply. That is, when there is a vote that concerns both federal and cantonal matters, the federal rules apply, and the proportion of Internet voters is limited.

However, the limits do not necessarily apply if a vote concerns only cantonal matters. The schedule of federal voting is fixed in advance by the government and there

are usually four votes per year, each involving several separate questions (typically a yes or no vote on a constitutional amendment or on a federal law).

In May 2011, there was no federal question. The Geneva government decided to allow 100% of the Geneva voters to use Internet voting for the cantonal questions. The same happened in November 2011.

The purpose of this paper is to present the outcome of an attempt to challenge the Geneva system in court. A comparative analysis of the case law regarding electronic voting in several countries, and also of the respective laws, is given in [13]. As we will see, the approach taken by the courts in Switzerland differs from that taken by the courts in other countries.

2 What the Appellant Did

The author of the present paper filed court challenges (called appeals in Switzerland) against the use of the Geneva system by all voters for the May and September 2011 votes. He requested the courts to find that the Geneva system did not conform to cantonal law and the Federal Constitution.

The reasons being that there was no guarantee that the vote sent to the state's server accurately reflects the voter's choices, that a family members can vote for another family member without that member's knowledge, and that the secrecy of the vote was not guaranteed.

The appeals were filed only against the votes where 100% of the Geneva voters were offered the possibility of voting via Internet because, as explained below, an appeal can only be successful if the appellant can show that an irregularity could have affected the outcome. It is highly unlikely that the federal outcome can be affected by an irregularity in an Internet voting system that is offered only to 30% of the voters. So an appeal against the use of the Internet voting system in a federal vote had lesser chance of being successful.

As we will see, the appeal was unsuccessful and this colors the present paper.

3 Why the Appellant Did It

The motivation behind the appeals was to stimulate improvements to the Geneva system, in particular the implementation of verifiability. In the author's view, the Geneva government (who had put into place the challenged Internet voting system) and the Geneva parliament (who had passed the law allowing the challenged system to be offered to all voters) did not know or understand that there has long been consensus amongst computer scientists that e-voting is risky [5, 12], that the rather simple Geneva system was inadequate, and that appropriate systems can be put into place.

4 The Appellant's Background

The appellant in these cases is not a lawyer and he did not mandate or consult lawyers regarding the cases. The complainant has degrees in mathematics and statistics from MIT and Harvard University, but he has mostly worked as a programmer, information systems manager, and telecommunications manager.

5 The Legal Process

Legal challenges to cantonal votes in Geneva must be filed with the cantonal court. The decision of the cantonal court can be appealed to the Federal Tribunal, which is the Swiss supreme court.

The deadline for filing the appeal at the cantonal level is rather short, 6 days. The deadline for filing the federal appeal is 30 days. At the cantonal level, the court will consider the receivability of the appeal before considering the arguments on the merits; it will consider both cantonal law and federal law, in particular the provisions of the Federal Constitution.

At the federal level the court will consider the receivability of the federal appeal, and the receivability of the cantonal appeal (but it will only consider whether the cantonal decision on receivability was arbitrary). Regarding the merits, it will freely review the application of both cantonal and federal law, but it will rely on the facts established by the cantonal court, unless the appellant can prove that the cantonal court established the facts in an arbitrary manner.

As we will see below, these technical legal procedural niceties were significant to the cases.

5.1 Receivability

In order to be receivable, an appeal must be filed within the deadline, by a person who has the right to file the appeal (in this case any voter). And it must respect formal rules regarding the format of the appeal, the language in which it is written, the number of copies to be submitted, etc.

There were no receivability issues at the federal level (even if the Geneva government did attempt to challenge the receivability of the federal appeals). On the other hand, there were significant issues regarding the receivability at the cantonal level. On the one hand, this might appear surprising: why should the court try to avoid considering the merits of the case? On the other hand, it is understandable: courts are not comfortable evaluating what is primarily a technical dispute [13].

5.2 Merits

The law applicable to the merits.

According to federal law (art. 34 of the Swiss Constitution and the resulting case law of the Federal Tribunal), the results of a vote must faithfully reflect the voter's

intent, the vote must be secret (with some exceptions which are not relevant for the cases at hand), and one person can vote only once. It is not necessary for a complainant to prove that irregularities actually affected the result of a vote: it suffices to show that irregularities could have affected the result. [14]

According to cantonal law (art. 60 of the Loi sur l'exercice des droits politiques), a voter must use equipment that is sufficiently secure, the government publishes security rules, and the government can suspend the use of e-voting systems if it believes that security is insufficient. In this context, "security" does not refer merely to security of the information technology used in the e-voting systems, it also refers to the reliability and security of all other aspects of the e-voting system, including manual operations.

The substantive arguments.

The appellant alleged that the Geneva system did not comply with the law because the personal computers used by voters are vulnerable to malware that can change a vote without the voter's knowledge (for example, man-in-the-browser attack), that a man-in-the-middle attack was possible, that the state's server could also be compromised, that massive fraud could not be detected, that the secrecy of the vote could not be guaranteed, and that a family member could – easily and without risk of detection – impersonate and vote in place of another family member (also a risk in old persons' homes).

Further, the appellant alleged that the Geneva government had not produced the security requirements called for by cantonal law, and that the government should suspend the use of Internet voting until those security requirements were published.

The appeal was directed against the specific system (software) implemented and used in Geneva and the allegedly missing detailed regulation of security, and not against the principle of e-voting, nor against the provisions of the Geneva Constitution or of the cantonal law authorizing Internet voting. Indeed, appeals against those provisions per se would have been time-barred: an explicit challenge of the provisions of the Constitution or the cantonal law would have had to be filed within 30 days of their promulgation. On the other hand, the provisions can be challenged implicitly in the context of an appeal against a specific vote. The appellant attempted to do this but, as we will see below, the appeal was not accepted because the appellant could not present evidence showing that specific weaknesses had been exploited in a specific vote.

The appeal included the following figures. Figure 1 shows how malware could be introduced so as to change what the voter entered and send the falsified vote to the state's server. Figure 2 shows how a man-in-the-middle attack would be possible if the voter's personal computer were compromised, for example by replacing its X.509 certificates. Figure 3 shows the results of the Internet vote compared to the correspondence vote for the May 2011 vote for each of the five questions considered in that vote. As can be seen, the Internet vote differed systematically from the correspondence vote, which is not usually the case [15]. And the difference for question 5 was statistically significant and it actually affected the result of the vote for that particular question.

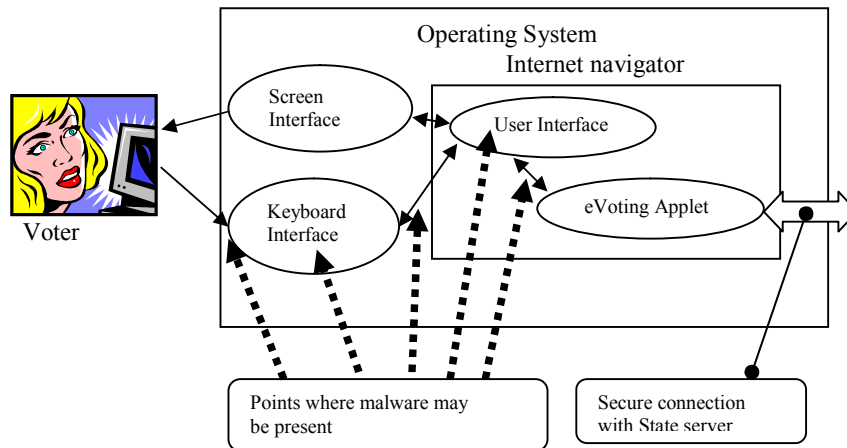


Fig. 1. Vulnerabilities to malware

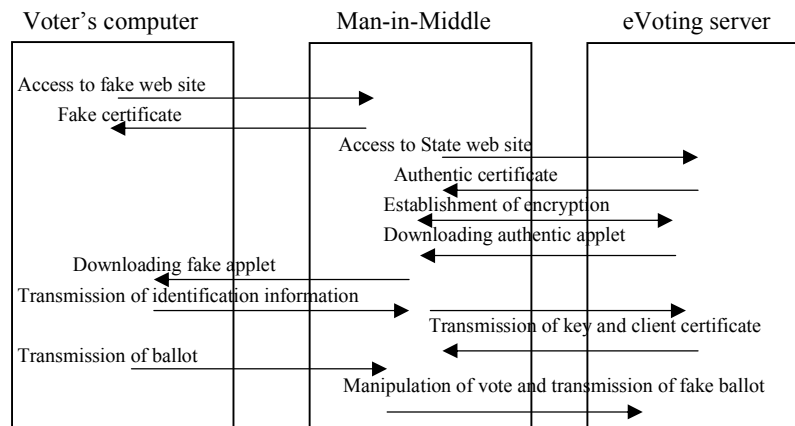


Fig. 2. Vulnerabilities to man-in-the-middle

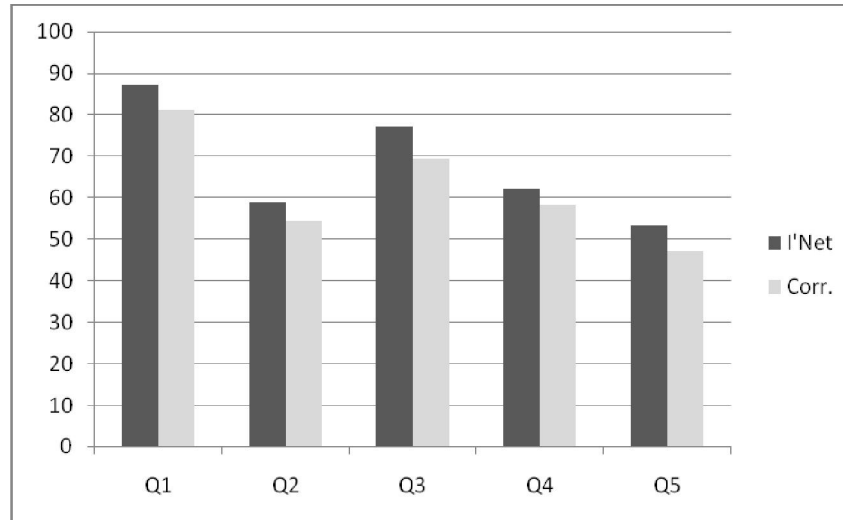


Fig. 3. Differences between Internet vote and correspondence vote for May 2011 vote

The appeals pointed out that a computer engineer had actually shown how easy it was to insert malware that would modify a vote, without the voter being aware of it [11]. And it stressed the fact that the 2013 report of the Federal government called for not allowing more than 30% of voters to use the existing systems, and for the development and implementation of verifiable systems [2]. The appellant argued that the federal restriction of 30% on the proportion of voters allowed to use the Geneva Internet voting system should apply also to cantonal votes.

The cantonal court's judgment provided a good summary of all the arguments outlined above [16].

6 The Actual Procedures

The complainant filed six separate legal actions. In four of them he appealed to the Federal Tribunal against the cantonal decision. The six separate actions were:

1. Against the voting method used for the May 2011 vote. This complaint was mistakenly filed too late, so it was irreceivable. There was no appeal to the Federal Tribunal. The total cost of this action was CHF 500.
2. Against the result of the May 2011 vote. This was declared time barred and thus irreceivable at the cantonal level because the cantonal court held that the complaint was in reality directed against the voting method, not against the result of the vote [17]. The complainant appealed to the Federal Tribunal: the appeal was rejected [18]. It should be noted here that, with respect to cantonal procedural law (in this case the deadline for filing the cantonal complaint), the Federal Tribunal will only overturn the cantonal decision if it finds it to be arbitrary. The Federal Tribunal's

judgment did not explicitly deal with the fact, put forward in both the cantonal complaint and the federal appeal, that there was an unusual difference between the results of the correspondence vote and the Internet vote, see Figure 3 above. So the complainant filed a request for revision, on the grounds that the Federal Tribunal had overlooked a significant fact. The Federal Tribunal rejected this request [19]. The cost for this action was CHF 500 at the cantonal level, and CHF 1000 for each stage at the federal level, so the total was CHF 2500.

3. Against the refusal of the Geneva government to suspend e-voting as requested by letter. The cantonal court held that there was no appealable decision: the mere refusal to comply with the request in a letter was not a formal decision. There was no appeal to the Federal Tribunal. The total cost of this action was CHF 500.
4. Against the voting method used for the 27 November 2011 vote. The cantonal court held that the appeal was irreceivable because the arguments were abstract, general, and directed against the principle of e-voting and not against the Geneva system [16]. On appeal, the Federal Tribunal quashed this judgement and remanded the case to the cantonal court for a new decision, on the grounds that the arguments put forward by the cantonal court concerned the merits, not the receivability of the appeal [20]. In accordance with the procedural rules regarding deadlines, the appeal was filed before the results of the vote were known. Once the results were published, it became obvious that they could not have been affected by a defect in the Internet voting system (the proportion of voters using the Internet system was too small to affect the outcome). Therefore the appellant withdrew his request to annul the vote, but he persisted with his request that the method be found illegal. The withdrawal of the request to annul the vote could have resulted in the case being declared moot, but the Federal Tribunal ruled that it was not, because the case raised a question of principle which should be examined by the courts [20]. There was no cost for this case because the appellant prevailed.
5. Recusal of the cantonal judges who involved in the judgment mentioned above, on the grounds that they had already evaluated the merits of the case, because they had held that the arguments were abstract, general, and directed against the principle of e-voting and not against the Geneva system. The request was refused both by the cantonal court and by the Federal Tribunal [21]. The cost was CHF 350 at the cantonal level and CHF 2000 at the federal level, so the total cost was CHF 2350.
6. Second cantonal judgment regarding the 27 November 2011, the case having been declared receivable by the Federal Tribunal. The cantonal court rejected the appeal on the grounds that the arguments were abstract, general, and directed against the principle of e-voting and not against the Geneva system [22]. On appeal, the Federal Tribunal agreed [23]. Since this judgment ended the process, it will be discussed in more detail below. The cost was CHF 1500 at the cantonal level and CHF 1000 at the federal level, so the total was CHF 2500.

7 The Federal Court's reasons

In essence, the Federal Tribunal [23] held that an appeal can only be lodged if weaknesses have been actually exploited during a specific vote. The fact that a weakness exists, and that it could be exploited in a way that cannot be detected, is not sufficient, and this even if the appeal is directed against the procedures used and not against the outcome of the vote. According to the Tribunal, arguments of that nature must be decided at the political level. Thus in practice one cannot appeal to the courts against the characteristics of an electronic voting system. The Tribunal, in so ruling, distances itself from the case law of other jurisdictions.

It should be noted that the Tribunal rejected (for the reasons mentioned above), the following claims regarding the Geneva system:

1. A voter can vote more than once using the electronic system, and this in a way that cannot be detected. This is not due to the computerized system properly speaking: the weakness is in the method used to identify voters when they are voting electronically.
2. A virus or other malware could have changed the results of the vote.
3. The secrecy of the vote cannot be guaranteed, because malware could compromise the secrecy.
4. The regulations at the cantonal level are not consistent with cantonal law because they do not contain the required level of detailed requirements regarding the security of the voters' computers.
5. Because the federal law does not allow use of a system such as the Geneva system for all voters, and this precisely for the reasons set forth by the appellant, making such a system available to all voters for cantonal votes violates the Federal Constitution.

Regarding the case law of other jurisdictions, claims similar to those put forward by the appellant have been evaluated on their merits by courts in Austria, Germany and India [13]. In those cases the courts ruled that the electronic systems in question did not conform to the law and could not be used without changes. The German judgment is particularly broad and some commentators are of the view that it essentially prohibits e-voting [26].

A case judged in Estonia is worth mentioning because it creates a catch-22, that is, a situation from which an individual cannot escape because of contradictory rules [24]. At the time, Estonia was using an Internet voting scheme that shared the main characteristics of the Geneva system described above: it assumed that the voter's personal computer had not been compromised. A computer specialist deliberately infected his own personal computer with a virus that tampered with his vote, and then challenged the voting process in court, using as evidence what had happened in his own personal computer. The court dismissed the case, holding that the situation was analogous to that of a user who deliberately casts an invalid ballot. But the computer

specialist would have committed a criminal offense if he had tampered with the computer of another voter without that voter's consent. So, in effect, there was no legal way for the computer specialist to present to the court evidence regarding how easy it was to tamper with the Internet voting system by tampering with voters' personal computers. [27]

As Driza Maurer and Barrat put the matter [28], absence of proof of tampering is not proof of absence of tampering. We will discuss this point in more detail in the next section.

8 Next Steps

On the one hand, the judgment of the Federal Tribunal might seem surprising because, having first ruled that the appellant raised matters of principle that should be evaluated by the courts, it subsequently ruled that the matters in question were better left to the political system. On the other hand, the judgment must be seen in light of the evolution of the Swiss federal rules regarding e-voting systems. While the case was progressing through the courts, the Federal Council tightened the requirements for e-voting significantly, mandating the use of verifiable systems if more than 30% of the voters are allowed to use an e-voting system [25]. While this change in federal law does not directly prevent the use of non-verifiable systems for cantonal-only votes, in practice it has resulted in the implementation of verifiable systems in the cantons. Thus the court cases discussed above may have influenced the actual implementation of e-voting systems in Switzerland, even if they were thrown out by the courts [28, 29].

Nevertheless, one might take the view that the situation in Switzerland is not satisfactory, because there is no way to ask for judicial review of a cantonal government's implementation of the federal rules regarding e-voting systems. For sure the systems are subject to review and approval by the federal government, but that is not the same as review and approval by an impartial and independent judiciary.

And indeed a group of federal parliamentarians has proposed to change the federal law so that the courts would have to evaluate on their merits arguments such as the ones outlined above [30]. That is, courts would evaluate whether a specific implementation of an e-voting system complies with the applicable federal and cantonal laws and regulations, and this independently of whether or not an appellant can prove that specific weaknesses were exploited in the course of a specific vote.

Further, it seems reasonable to conclude that parliaments need to take greater responsibility for the security of the systems that are actually implemented, and that they should be more involved in the tradeoffs between verifiability versus secrecy, usability versus coded voting or dedicated operating systems, and low costs versus dedicated hardware. All those topics warrant considerable further inter-disciplinary discussions, because they relate to legal, technical, and social matters [28].

9 References

1. A. Driza Maurer: Internet Voting and Federalism: The Swiss Case. *Revista General de Derecho Público Comparado*, No. 13, 2013; and in J. Barrat (ed.): *El voto electronico y sus dimensiones juridicas: entre la ingenua complacencia y el rechazo precipitado*, Iustel, Madrid, Spain, 2015
2. Swiss Federal Chancellery: Vote électronique
<http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=fr>
3. Commission externe d'évaluation des politiques publiques: Voter par Internet: évaluation des effets du vote électronique à Genève, Geneva, Switzerland, 2013
<http://goo.gl/BZpFn4>
4. M. Chevalier: Internet Voting: Status, Perspectives, and Issues, Chancellery of the canton of Geneva, ITU-T Workshop on e-Government, 2003
<http://www.itu.int/itudoc/itu-t/workshop/e-gov/e-gov010.html>
5. R. Oppliger: Traitement du problème de la sécurité des plate-formes pour le vote par Internet à Genève, Chancellerie du canton de Genève, Geneva, Switzerland, 2002
<http://goo.gl/t8o9gG>
6. M. Chevalier: La solution genevoise de vote électronique à cœur ouvert, *Direktdemokratie*, *Flash Informatique* No. 6 (2011) <http://goo.gl/9HUZXx>
7. E. Dubuis, R. Haenni, and R. Koenig: Konzept und implicationen eines verifizierbaren Vote Elektronique Systems. Berner Fachhochschule, Bern, Switzerland, 2012
<http://goo.gl/pj7Gyl>
8. E. Dubuis, S. Fischli, R. Haenni, U. Serdült, and O. Spycher: A Verifiable Internet Voting System, in *CeDEM'11*, Conference for E-Democracy and Open Government, pages 301-312, Krems, Austria, 2011
9. J. Barrat, M. Chevallier, B. Goldsmith, D. Jandura, J. Turner, and R. Sharma: Internet Voting and Individual Verifiability: The Norwegian Return Codes, in *EVOTE2012*, pages 35-45, Bregenz, Austria, 2012
10. Swiss Federal Council: Rapport sur le vote électronique, 2013
<http://www.admin.ch/opc/fr/federal-gazette/2013/4519.pdf>
11. S. Andrivet: Attacking E-Voting: A Concrete Case, in *Nuit du Hack 2013*, Advtools, 2013
<http://goo.gl/1FamYU>
12. Jones, Douglas W. and Simons, Barbara: *Broken Ballots: Will Your Vote Count?*, University of Chicago Press, Chicago, USA, 2012
13. A. Driza Maurer and J. Barrat (eds.): *E-Voting Case Law: A Comparative Analysis*, Ashgate, Farnham, UK, 2015
14. A. Auer, G. Malinverni, and M. Hottelier: *Droit constitutionnel suisse*, Staempfli, Bern, Switzerland, 2006
15. T. Christin and A. S. Trechsel: Analyse du scrutin du 26 septembre 2004 dans quatre communes genevoises, E-Democracy Center, University of Geneva, Geneva, Switzerland, 2005 <http://goo.gl/4YqhFz>
16. Chambre administrative, Cour de Justice de Genève: ATA/533/2012, 21 August 2012
<http://justice.geneve.ch/tdb/Decis/TA/ata.tdb?F=ATA/533/2012>
17. Chambre administrative, Cour de Justice de Genève, ATA/414/2011, 28 June 2011
<http://justice.geneve.ch/tdb/Decis/TA/ata.tdb?F=ATA/414/2011>
18. Federal Tribunal: IC_329/2014, 22 July 2014
http://relevancy.bger.ch/php/aza/http/index.php?type=highlight_simple_query&highlight_docid=aza%3A%2F%2F22-12-2011-1C_329-2011

19. Federal Tribunal: 1F_5/2012, 19 March 2012
http://relevancy.bger.ch/php/aza/http/index.php?type=highlight_simple_query&highlight_docid=aza%3A%2F%2F19-04-2012-1F_5-2012
20. Federal Tribunal: 1C_477/2012, 27 March 2013
http://relevancy.bger.ch/php/aza/http/index.php?type=highlight_simple_query&highlight_docid=aza%3A%2F%2F27-03-2013-1C_477-2012
21. Federal Tribunal: ATF 1C_563, 29 August 2013
http://relevancy.bger.ch/php/aza/http/index.php?type=highlight_simple_query&highlight_docid=aza%3A%2F%2F29-08-2013-1C_563-2013
22. Chambre administrative, Cour de Justice de Genève, ATA 118/2014, 25 February 2014
http://justice.geneve.ch/tdb/Decis/TA/FichierWord/2014/0001/ATA_000118_2014_A_3506_2011.pdf
23. Federal Tribunal: 1C_136, 22 July 2014
http://relevancy.bger.ch/php/aza/http/index.php?type=highlight_simple_query&highlight_docid=aza%3A%2F%2F22-07-2014-1C_136-2014
24. Wikipedia: Catch-22 (logic) [http://en.wikipedia.org/wiki/Catch-22_\(logic\)](http://en.wikipedia.org/wiki/Catch-22_(logic))
25. Swiss Federal Chancellery: Des nouvelles dispositions régissent le vote électronique
<http://www.bk.admin.ch/themen/pore/evoting/index.html?lang=fr>
26. S. Seedorf: Germany: The public nature of elections and its consequences on e-voting, in [13]
27. U. Madise and P. Vinkel: A Judicial Approach to Internet Voting in Estonia, in [13]
28. A. Driza Mauer and J. Barrat: Conclusions, in [13]
29. B. Kuoni: Case Law on E-Voting – A Swiss Perspective, in [13]
30. Swiss Parliament: Zulassung einer rechtlichen Prüfung der Modalitäten der elektronischen Stimmabgabe, Curia Vista 15.412
http://www.parlament.ch/d/suche/Seiten/geschaefte.aspx?gesch_id=20150412