THE
CARTER CENTER

Expert Study Mission Report
The Carter Center
Internet Voting Pilot: Norway's 2013 Parliamentary Elections

19 March 2014*

Executive Summary

The Carter Center was invited to observe the Internet voting trials of the Norwegian Parliamentary Elections of 2013. In response to the invitation, the Center decided to deploy a one-person Expert Study Mission in close coordination with a separate mission deployed by the Organization for Security and Cooperation in Europe/ Office for Democratic Institutions and Human Rights (OSCE/ODIHR).[1] As part of this collaboration, the Carter Center's expert participated in several joint meetings organized by ODIHR with election officials during the months of July and September.

Internet voting continues to be controversial both within and beyond Norway. With the "I-voting" trials of 2011 and 2013, the Kingdom of Norway joined a small group of countries (including Switzerland, Canada, and Estonia) that have allowed binding votes submitted via the Internet. Advocates argue that they enfranchise citizens with heretofore less access on Election Day, including the disabled, the elderly, expatriates, and military members serving abroad. In addition, some have also argued that Internet voting may increase political participation among apathetic and younger voting demographics.[2] Critics of Internet voting on the other hand believe both the insecurity of the technology

* A version of this report was issued on 18 February 2014; this final version includes small corrections and clarifications.

[1] OSCE/ODIHR, "Norway - Parliamentary Elections 9 September 2013 - OSCE/ODIHR Election Assessment Mission Final Report," December 16, 2013.

[2] Although recent research in Switzerland shows this may not be the case, Alexander Trechsel and Urs Gasser, "Casting Votes on the Internet," *Harvard International Review*, April 17, 2013, http://hir.harvard.edu/the-future-of-democracy/casting-votes-on-the-internet.

and the uncontrolled environment in which votes are cast compromises the secrecy of the ballot, opening the door to coercion and other forms of manipulation such as vote buying or selling.

For the Norwegian Parliamentary Elections of 2013, a select group of voters were permitted to vote via the Internet from the location of their choice during the advance voting period, a time when qualified voters have traditionally been permitted to cast paper ballots in advance of election day. This year's "I-voting" trial between 12 August and 6 September was the second such for Norway: I-voting first took place in 2011 during the advance voting period as a supplement to conventional poll site voting. In 2013, the Ministry for Local Government and Regional Development attempted to address concerns that arose during the initial pilot. In addition, the scope was expanded from ten to twelve municipalities so that approximately 250,000 voters, or 7 percent of the electorate, could submit their votes from the computers and locations of their choice.

Using the Norwegian 2013 elections, this report attempts to address two separate but related issues:

1) the relationship between Internet voting in uncontrolled environments and generally accepted standards for genuine democratic elections, and
2) the extent to which Internet voting is observable.

It is important to note that this study mission report does not and cannot make any conclusive statements about the 2013 Internet voting trials themselves. In addition, this report will not attempt to draw any conclusions about Internet voting overall. Rather, the main objective is to outline difficult issues related to observation techniques and methodology -- many of which have been well considered and discussed, and even specifically for the Norwegian context.[3] The meaning of observation in the context of the Internet demands more consideration, and the main goal of this report is to layout some challenges that Internet voting poses to election observation.

The Carter Center wishes to thank the Ministry for Local Government and Regional Development for its invitation to observe the Internet voting trials in spite of the specialized nature of the study. The generous openness and availability of its staff to questions before, during, and after the elections has furthered the Carter Center's understanding of key issues related to Internet voting.

The Carter Center also wishes to thank OSCE/ODIHR and the members of their Norway 2013 team, whose experience and knowledge were invaluable. Although the Carter

[3] Jordi Barrat i Esteve, Ben Goldsmith, and Nick Turner, *International Experience with E-Voting: Norwegian E-Vote Project* (IFES, June 2012), http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf.

Center expert participated in joint meetings with the Ministry and other election representatives, both Carter Center and OSCE/ODIHR organizations maintained institutional independence in their assessments and report writing. The contents and analysis of this report belong to the Carter Center alone.

This report contains the following sections:

Abbreviations

CoE	Council of Europe
E2E	End-to-End Verification
EVA	*Elektronisk Valgadministrativt*, or the Electronic Vote Administration, *System*
E-voting	Electronic Voting
IEC	Internet Election Committee, *Internettvalgstyret*[4]
I-voting	Internet Voting
KRD	*Kommunal- og Regionaldepartementet*, Norway's Ministry of Local Government and Regional Development
NIZKP	Non-Interactive Zero Knowledge Proof
OSCE/ODIHR	Organization for Security and Cooperation in Europe/ Office for Democratic Institutions and Human Rights
QA	Quality Assurance
SMS	Short Message Service
ZKP	Zero Knowledge Proof

[4] Literally *Internet Voting Board*, but IEC is used in Ministry document translations.

Context: the Electorate and the System

Before addressing the issues and challenges that Internet voting ("I-voting") presented in the Norwegian example as well as more broadly, an explanation about legal framework and the I-voting system itself is necessary. The section on the I-voting system does not offer a comprehensive review, but enough high-level understanding so that Internet voting issues are more clearly understood.

Obligations for democratic elections and Norway's legal framework

International obligations for democratic elections, which emerge out of a body of human rights treaties and commitments, form a firm basis upon which aspects of the election process can be assessed.[5] And regardless of the medium used, whether paper or electronic, obligations for genuine democratic elections such as the equal suffrage or freedom of movement apply equally. A number of obligations are particularly relevant for the context of e-voting, including:

- the *right to vote*,
- the *right to be elected*,
- the *right to participate in public affairs*,
- *secrecy of the ballot*,
- *equal suffrage*.[6]

In addition to the set of international laws and commitments to uphold democratic elections undertaken by Norway, the Election Act provides the Kingdom's general election framework. As defined in the Act's very first paragraph, elections in Norway are to be free and secret.[7] There is no national election management body; rather, overall responsibility for administering the elections lies with the Ministry of Local Government and Development.

[5] The Democratic Election Standards (DES) project at the Carter Center aims to build consensus on twenty-one such obligations for democratic elections and on common criteria for assessing elections, "Election Standards at The Carter Center | Election Observation Best Practices," accessed February 1, 2014, http://electionstandards.cartercenter.org/; more about international obligations for democratic elections is explained by Carter Center experts David J. Carroll and Avery Davis-Roberts, "The Carter Center and Election Observation: An Obligations-Based Approach for Assessing Elections," *Election Law Journal* 12, no. 1 (2013): 87–93; Avery Davis-Roberts and David J. Carroll, "Using International Law to Assess Elections," *Democratization* 17, no. 3 (June 2010): 416–441, doi:10.1080/13510341003700253.

[6] Carter Center, *The Carter Center Handbook on Observing Electronic Voting*, 2nd ed, 2012, 22, https://cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf.

[7] "The purpose of this Act is to establish such conditions that citizens shall be able to elect their representatives to the Storting, county councils and municipal councils ***by means of a secret ballot in free and direct elections***," *Representation of the People Act (the Election Act)*, accessed October 15, 2013, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf §1-1, emphasis from Ministry presentation in September 2013.

For the purposes of the 2013 Internet trials, the Ministry also laid down additional specific regulations to supplement the Election Act. The "Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities" outlined requirements, relevant electoral bodies, and specific details related to how decryption should take place.[8] First and foremost among the principles in the Regulations is that Internet voting is only a supplement to paper ballot voting; another way of understanding this is that in Norway, Internet voting is not designed to "work" without the standard voting system in place.

These more specific regulations reflected and incorporated key aspects of the Council of Europe's 2004 Recommendation on legal, operational, and technical e-voting [Recommendation 2004(11)]. Because Norway's regulations took little exception to the Recommendation, a number of its important guidelines have special relevance with regard to areas like *secrecy of the ballot* and election observation:

> 10. The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection […]
> 12. The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting. […]
> 17. The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter. […]
> 51. A remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast. […]
> 83. E-voting systems shall generate reliable and sufficiently detailed observation data so that election observation can be carried out. The time at which an event generated observation data shall be reliably determinable. The authenticity, availability and integrity of the data shall be maintained.[9]

Norway's Election Act also covers postal voting. With regards to Internet voting, postal voting is an area of particular interest because it seems to provide the most analogous comparison – voting from a remote uncontrolled environment. For countries that have allowances for postal voting in law, this has enabled them to more easily consider Internet voting. Postal voting as an analogy has been used in the Council of Europe's

[8] Kommunal- og Regionaldepartementet, *Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities*, 2013.

[9] Committee of Ministers - Council of Europe, *Legal, Operational and Technical Standards for E-Voting*, Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum (Strasbourg: Council of Europe Publishing, 2005).

Recommendation 2004(11), numerous academic papers, and the Carter Center's *Handbook on Observing Electronic Voting*.[10]

Postal voting is covered in §8 of the Election Act, which establishes a high bar for invalidating a vote.[11] Typically, while abroad, a voter would request the appropriate ballot and envelope from the nearest embassy and then mail it in. However there are no real procedures with regards to the checking of stamps, and in the end, one can still submit a ballot using one's own paper/envelope.[12] In general, it should be noted that the numbers of postal votes are very low, and that in Norway because postal voting fraud is considered to be a negligible threat, it does not require much consideration.

Context: 2013 Parliamentary Elections Snapshot

Overall, approximately 3.6 million Norwegians were eligible to vote for the 2013 parliamentary elections. 30 percent of this electorate were 60-years-old and above, while 18- to 19-year-olds (first-time voters) made up 3.4 percent. In addition, the number of immigrant and second-generation immigrant voters increased to 5.9 percent of the total, up from 3.6 percent in 2005.[13]

[10] In addition to works already cited in this paper, see also Council of Europe Venice Commission (European Commission for Democracy Through Law, *Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe, Adopted by the Venice Commission at Its 58th Plenary Session (Venice, 12-13 March 2004)*, Study no. 260/2003 (Strasbourg: Council of Europe, March 2004), http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx; Ben Goldsmith, IFES - Internet Voting: Past, Present and Future, accessed September 7, 2013, http://www.ifes.org/Content/Publications/Interviews/2013/Internet%20Voting%20Past%20Present%20and%20Future; *Introducing Electronic Voting: Essential Considerations*, Policy Paper, International IDEA Resources on Electoral Processes (International IDEA, December 2011), http://www.idea.int/publications/introducing-electronic-voting/upload/PP_e-voting.pdf; US Election Assistance Commission, *A Survey of Internet Voting*, Testing and Certification Technical Paper (US Election Assistance Commission), accessed July 6, 2013, http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf; Carter Center, *The Carter Center Handbook on Observing Electronic Voting*.

[11] Siri Dolven, Follow-up discussion, interview by Connie Moon Sehat, September 8, 2013; *Representation of the People Act (the Election Act)*; Kommunal- og Regionaldepartementet, "Election Manual: Overview of Election Rules" (Ministry of Local Government and Regional Development, Norway, August 26, 2013), §11, http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/valgmedarbeidere/Valghandbok/Valghandbok_2013_engelsk.pdf.

[12] Dolven, Follow-up discussion; Ingrid Trømborg, Anne Skau, and Marit Hexeberg, Municipality of Frederikstad preparations for I-voting trials and EVA, July 2013.

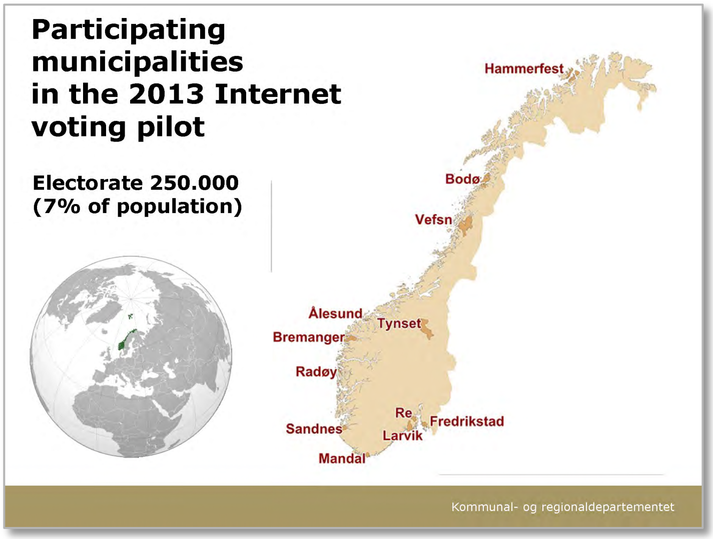
[13] Statistik sentralbryå, "Storting Election, Persons Entitled to Vote, 9 September 2013," *Statistik Sentralbryå - Statistics Norway*, September 3, 2013, http://www.ssb.no/en/valg/statistikker/stemmerettst.

This election saw an increase in participation compared to the 2011 local elections: in 2011, 64.5 percent of those eligible cast their votes while 78.2 percent turned out in 2013.[14]

Within the twelve Internet voting participating municipalities – which included 250,000 voters or 7 percent of the electorate – interesting trends were visible. 28 percent participated in the Internet voting pilot, representing an increase of 8 points from 2011.

This is noteworthy considering that overall in Norway, 23 percent of the population casted their vote in the advance voting period. Thus, through Internet voting alone, voters from the pilot municipalities proportionally registered their votes much earlier than the rest of the country. As expected, the greatest influx of advance votes took place during the final days before the end of the Internet voting period. Finally, with regards to age: the popularity of electronic votes compared to paper votes was quite high among those younger than 60, with the tipping point occurring towards paper voting first in the late-60s bracket. Internet votes seem to have been cast by a handful of voters in their late 90s, though whether or not they were assisted in this effort is another, significant question addressed later in this report.[15]

Figure 1, KRD[16]



Participating municipalities in the 2013 Internet voting pilot

Electorate 250.000 (7% of population)

Kommunal- og regionaldepartementet

[14] Kommunal- og Regionaldepartementet, "Valg 2013 - Stortingsprognose - Grafisk," *Stortingsvalget*, September 9, 2013, http://www.valgresultat.no/bs7g.html.

[15] Henrik Nore and Christian Bull, "An Observable Internet Election," September 8, 2013, http://www.regjeringen.no/pages/38377245/2_an_observable_internet_election.pdf.

[16] Ibid.

Explanation of the I-voting System[17]

Building upon logic used in previous I-voting elections (such as in 2005 Estonia) and academic research, Norway's I-voting system involved *cryptography* and voter self-*verification* to secure the system against external tampering.[18] A joint project between Norway's Ministry of Local Government and Regional Development (Kommunal- og Regionaldepartementet or KRD) and the Spanish-based corporation Scytl, the system tried to ensure vote integrity and verification – by allowing voters or proxy voters to individually and independently verify that the votes cast were the only ones counted in the final tally of election results – while also preserving the secrecy of the vote as much as possible.

Put another way, the system tried to live up to the argument that "cryptographic voting protocols offer the promise of verifiable voting without needing to trust the integrity of any software in the system."[19]

A key part of this system is that it allowed voters to recast their vote via the Internet multiple times, with only the final vote counting as valid. The theory behind *vote updating* or *repeat voting* is that it reduces the likelihood that a vote can be bought or forced, since votes can be changed at the very last minute. In addition, paper ballots cast in polling booths during the advance voting period or on election day – from controlled voting environments – override any Internet vote. Thus the supplementary role of Internet voting is reinforced given the option to cast a paper ballot on election day within a controlled environment, which acts as a kind of system override.

The Ministry I-voting team tried to accomplish the twin goals of integrity and secrecy of the vote through a number of steps:

[17] For this section, references include Kommunal- og Regionaldepartementet, "Election Manual: Overview of Election Rules"; Kommunal- og Regionaldepartementet, "How to Vote via the Internet in the Parliamentary Election 2013," September 2013, http://www.regjeringen.no/pages/597658/how_to_vote_internet.pdf; Jordi Barrat et al., "Internet Voting and Individual Verifiability: The Norwegian Return Codes," in *Electronic Voting*, 2012, 35–45, http://www.e-voting.cc/wp-content/plugins/download-monitor/download.php?id=210; "IFES Election Guide | Elections: Norway Parl Sept 2013," accessed October 8, 2013, http://www.electionguide.org/election.php?ID=2076; OSCE/ODIHR, *Norway Parliamentary Elections - 9 September 2013 - Needs Assessment Mission Report* (Warsaw, Poland, July 12, 2013); Barrat i Esteve, Goldsmith, and Turner, *International Experience with E-Voting: Norwegian E-Vote Project*.

[18] In particular, especially with regards to the generation of return codes and a bulletin board hash, see Ben Adida and C. Andrew Neff, "Ballot Casting Assurance," in *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*, 2006, 7–7, http://www.usenix.org/event/evt06/tech/full_papers/adida/adida.pdf.

[19] Chris Karlof, Naveen Sastry, and David Wagner, "Cryptographic Voting Protocols: A Systems Perspective," in *USENIX Security Symposium*, vol. 12, 2005, 39, http://www.usenix.org/event/sec05/tech/full_papers/karlof/karlof.pdf.

1) Voters would be able to gain *enough of a sufficient receipt* – some level of verification to show that their vote was cast as intended, but not exact copies of their ballots. Providing an exact copy of the ballot, which would have conflicted with CoE Recommendation 2004 (11) nr. 51 that a "remote e-voting system shall not enable the voter to be in possession of a proof of the content of the vote cast," is problematic for maintaining secrecy of the ballot.
2) Through encryption, the vote and its receipt were never available in the system as plain text.
3) The encryptions resulted from algorithms that were employed across a distributed architecture of servers and server ownership designed with a "separation of duty" protocol. No single server/function was supposed to have direct access to the relationship among voter, party ballots, and votes cast.
4) To reduce the chances of vote buying or coercion, the system implemented repeat voting as described above.
5) But because of repeat voting, linkages between voter and votes cast had to exist until the official election; so, as soon as possible, links between vote and voter would be dissolved on servers and using software that would sufficiently "mix" the results.
6) In addition, as soon as the Internet voting phase was completed, the electronic ballot box was to be taken offline and handled on an airgapped server (one without Internet connection and therefore not susceptible to outside attack during this phase).

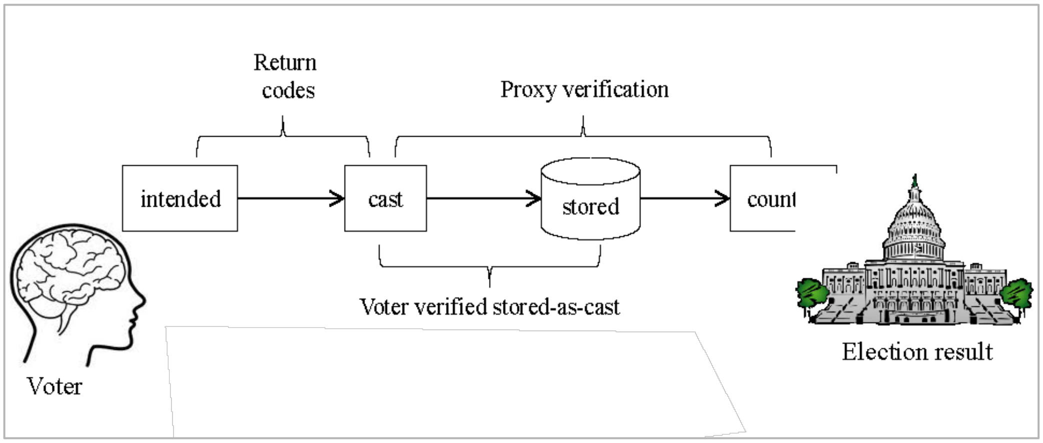


Figure 2 - Verification chain for Internet voting, provided by KRD.[20]

In order to implement these steps, Norway has worked since 2011 in close collaboration with the academic community, inviting members to analyze the system and to publish mathematical proofs related to its security and functioning.

[20] Christian Bull, "Safety First! Verifiability in the Norwegian E-Voting System" (presented at the Seminar on Internet Voting, Oslo, Norway, September 8, 2013).

The system was clearly complex. As a result, many significant parts to the process happened well in advance of Election Day. Norway's 2013 Internet voting trials involved at least four distinct phases: Phase I: *Software Development and Project Approval Phase* (initial 2011 pilot through early May 2013), Phase II: *Verifiability Setup Phase* (July and early August 2013), Phase III: *Internet Voting Phase* (August 2013), Phase IV: *Final Election Phase* (September 2013). What follows is an overview of the intended workings of the system from Phase II through IV. A large part of the development of this software was accomplished in Phase I, but alterations and additions were made during Summer 2013.

Phase II: Receipt and Verifiability Setup Phase

In order to vote, a voter had to register their mobile phone with a centralized government register (one could do so online while the voting was underway). The voter should have also received a special card, printed at the end of July and delivered through the postal service, with personalized numeric *return codes*. These cards provided the voter a list of four-digit numbers corresponding to each party running for election. The four-digit numbers were randomly assigned for every voter so that, for example, any two voters who wanted to cast their vote for Labour would unlikely have the same return codes associated to the Labour party.

In order to print these return codes, advance work was necessary to establish the link between voters and possible ballots in a secure way. An encrypted key framework was built so that any electronic information associating voter and vote content could only occur with the appropriate decryption key.

Establishing the keys was a critical part of 2013's preparation process, and in contrast to 2011, this process involved a new election committee. The nine-member Internet Election Committee (IEC) was formed specifically to ensure that the secrecy of the vote was not compromised – the bulk of its responsibilities was specifically related to voter information and cryptography. In order to do this, the Committee was granted the power to halt the Internet trials if necessary, and also to decide whether votes submitted via the Internet should be discarded. The committee included a balance of voters, county electoral committees, and technical experts including specifically a representative of the Norwegian Data Protection Authority, one election researcher, and one cryptographer.[21]

In addition, or as part of these duties, the Internet Election Committee corporately became owners of the decryption key: in order to decrypt the votes after the polls closed, at least 6 of the 9 members of the committee would have to provide smartcards that,

[21] Kommunal- og Regionaldepartementet, *FOR 2013-06-19 Nr 669*.

taken together, would create the decryption key.[22] The smartcards – as well as the servers important to this process -- were set up and generated during Phase II.

Finally, the IEC subcontracted Quality AS, a consulting firm with electoral, technological, and mathematical expertise to conduct various checks with regards to secrecy of the vote. In the invitation to tender, IEC sought external confirmation of the following:

- the destruction of information regarding the interpretation of the return codes post-printing.
- the secure handling of cryptographic keys,
- and a verification of the Internet voting system by an independent third party through mathematical proof application.[23]

Phase III: Internet Voting Phase

Internet voting took place from 12 August to 6 September. When ready to vote, the voter accessed a Javascript-based voting website (evalg.stat.no) from the browser of their choice. After confirming that computer and browser setup was sufficient to run the program, the voter was presented with the option of using one of several existing authentication services to confirm their identity (banking, smartcard, or the government MinID issued service). The idea behind this authentication step was that because these services provide access to highly sensitive information, it reduced the likelihood that one would want to voluntarily share these passwords with any other person.

The Norwegian parliamentary electoral system is open list proportional representation. Voters choose a party list, which has a ranked order of candidates; the higher the rank of the candidate, the more likely they will win a seat. Seats per party are awarded proportionally according to a modified Sainte-Laguë distribution method. Voters are permitted to propose a reordering of the candidates – in order to express their preference for specific representatives. However, unless their reordering is matched by more than 50 percent of those who also voted for the same list, a different candidate ranking is unlikely. The Internet voting program allowed for voters to easily opt for the party list of their choice as well as to rank or to delete candidates from the list.

As the following graphic shows, once the voter's ballot was submitted, then the choice was accepted in the Vote Collection Server (VCS). Two things happened at that point from the voter's perspective:

- she received a SMS that should have helped her verify that her vote was *cast as intended (as explained below)*

[22] Shamir secret sharing algorithm; encryption scheme was El Gamal.

[23] Kåre Vollan, *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys, Version 0.1 DRAFT*, The Internet Voting Board Representative: Internet Voting Trial 2013, August 26, 2013.

- she was presented with a hash of her encrypted vote (a fixed length string resulting from an algorithm) that could be used to verify the storage of her vote – or that it was *stored as cast*.

The concepts *cast as intended* and *stored as cast* -- reference Figure 2 on page 10 -- are specific links in a verification chain.

Cast as intended. In order to indicate receipt of a party ballot, the Vote Collection Server communicated with the Return Code Generator Server, which sent an SMS text to the voter with the appropriate personalized return code. The voter then could have taken the numeric return code and matched it against the list of codes received in the mail. If, for example, one voted for the Pirate Party and then received a four digit text of "1234," there should have been a match between "1234" and "Pirate Party" on the voter card. This match was supposed to verify that the vote was "cast as [the voter] intended."

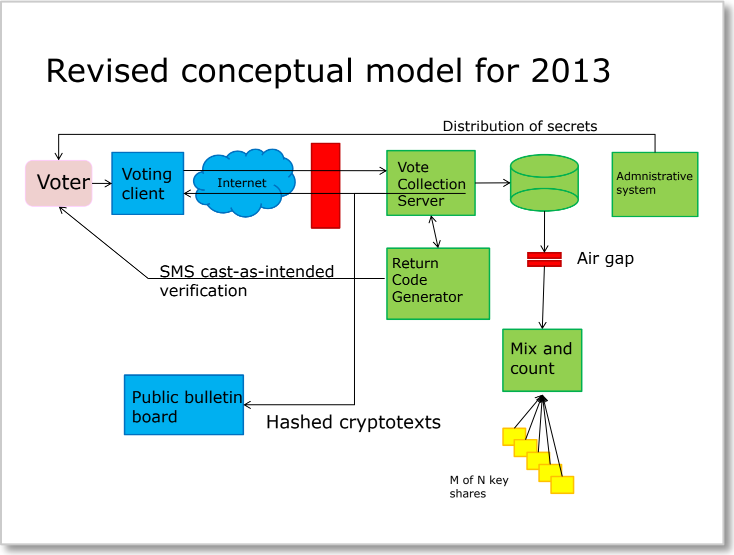

Revised conceptual model for 2013

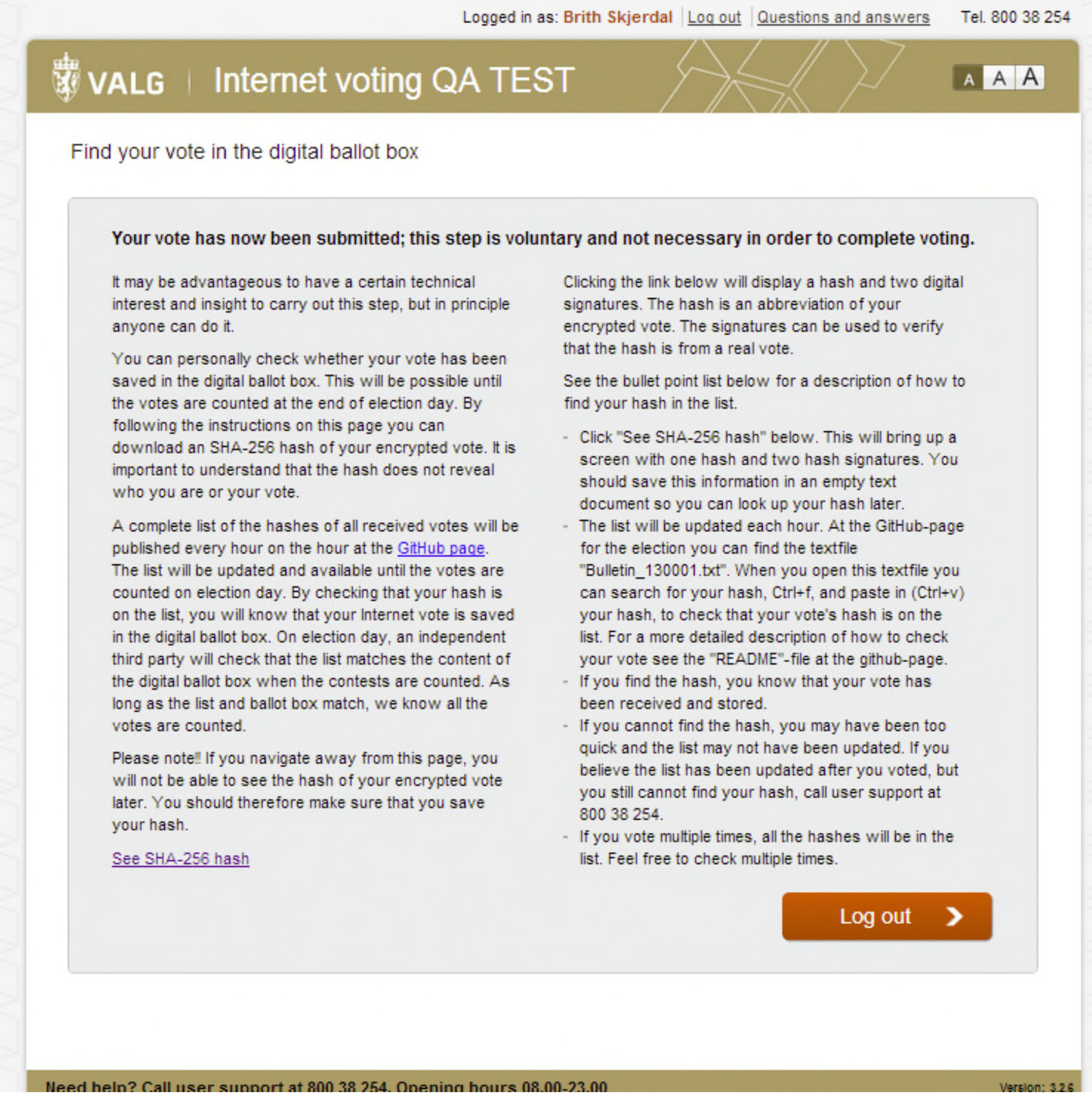
Figure 3 – High-level view of internet voting flow, courtesy KRD.[24]

Stored as cast. In addition, the 2013 trials introduced a new layer of verification to demonstrate the votes were also "stored as cast" – in other words, that the system not only received the votes correctly, but also stored them appropriately. In order to accomplish this, the Internet voting team used GitHub – a web-based repository sharing service based in San Francisco – to act as a kind of external third-party vote tracker.

[24] Bull, "Safety First! Verifiability in the Norwegian E-Voting System."

To make this work, upon submitting her vote, the voter also received an invitation to participate in additional verification. Although the vote was not in plaintext form, voters had access via the Vote Collection Server to their *hashes* as well as the *hash signatures* – the special alphanumeric strings that result from encryption algorithms. To voters familiar with SHA-256 is and what cryptographic hash functions do, the verification process made more sense but any voter could have performed the actions nevertheless.

Figure 4 – Hash verification, screen 1



Find your vote in the digital ballot box

Your vote has now been submitted; this step is voluntary and not necessary in order to complete voting.

It may be advantageous to have a certain technical interest and insight to carry out this step, but in principle anyone can do it.

You can personally check whether your vote has been saved in the digital ballot box. This will be possible until the votes are counted at the end of election day. By following the instructions on this page you can download an SHA-256 hash of your encrypted vote. It is important to understand that the hash does not reveal who you are or your vote.

A complete list of the hashes of all received votes will be published every hour on the hour at the GitHub page. The list will be updated and available until the votes are counted on election day. By checking that your hash is on the list, you will know that your Internet vote is saved in the digital ballot box. On election day, an independent third party will check that the list matches the content of the digital ballot box when the contests are counted. As long as the list and ballot box match, we know all the votes are counted.

Please note!! If you navigate away from this page, you will not be able to see the hash of your encrypted vote later. You should therefore make sure that you save your hash.

See SHA-256 hash

Clicking the link below will display a hash and two digital signatures. The hash is an abbreviation of your encrypted vote. The signatures can be used to verify that the hash is from a real vote.

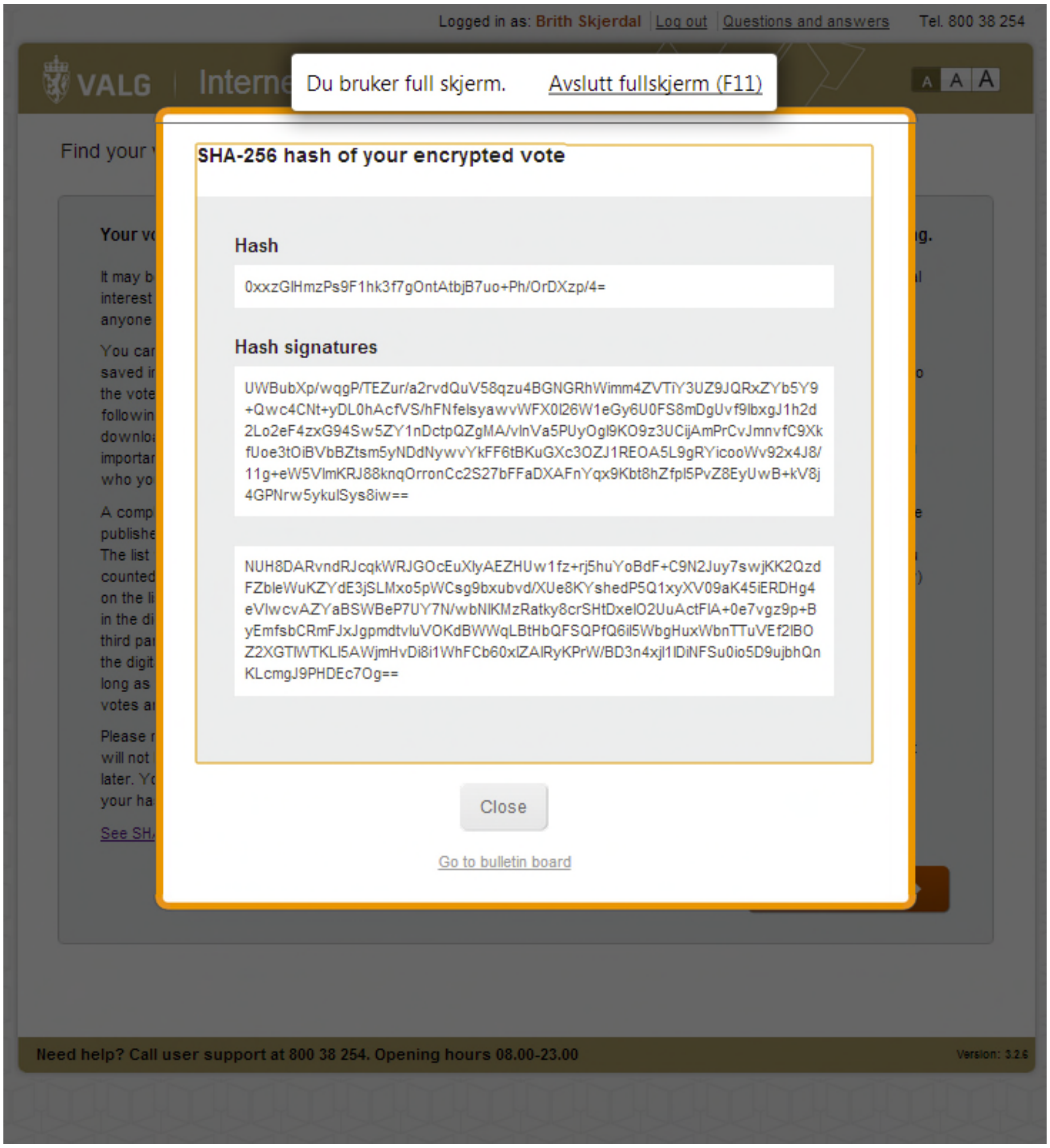
See the bullet point list below for a description of how to find your hash in the list.

- Click "See SHA-256 hash" below. This will bring up a screen with one hash and two hash signatures. You should save this information in an empty text document so you can look up your hash later.
- The list will be updated each hour. At the GitHub-page for the election you can find the textfile "Bulletin_130001.txt". When you open this textfile you can search for your hash, Ctrl+f, and paste in (Ctrl+v) your hash, to check that your vote's hash is on the list. For a more detailed description of how to check your vote see the "README"-file at the github-page.
- If you find the hash, you know that your vote has been received and stored.
- If you cannot find the hash, you may have been too quick and the list may not have been updated. If you believe the list has been updated after you voted, but you still cannot find your hash, call user support at 800 38 254.
- If you vote multiple times, all the hashes will be in the list. Feel free to check multiple times.

Need help? Call user support at 800 38 254. Opening hours 08.00-23.00

Voters could have located the hash string within the public, hourly updated file of all hashes/hash signatures on the Ministry's GitHub page. Should she vote numerous times, the voter would be able to match the hashes received against every vote she submitted. Because of the way that GitHub works, it is highly difficult and unlikely that the repository's files and history can be manipulated or rewritten.[25] However, this verification process still required trust that the Vote Collection Server reportout indeed reflected the ballots used in the final counting.

Figure 5 - Hash verification, screen 2



SHA-256 hash of your encrypted vote

Hash

```
0xxzGlHmzPs9F1hk3f7gOntAtbjB7uo+Ph/OrDXzp/4=
```

Hash signatures

```
UWBubXp/wqgP/TEZur/a2rvdQuV58qzu4BGNGRhWimm4ZVTiY3UZ9JQRxZYb5Y9
+Qwc4CNt+yDL0hAcfVS/hFNfelsyawvWFX0l26W1eGy6U0FS8mDgUvf9lbxgJ1h2d
2Lo2eF4zxG94Sw5ZY1nDctpQZgMA/vlnVa5PUyOgl9KO9z3UCijAmPrCvJmnvfC9Xk
fUoe3tOiBVbBZtsm5yNDdNywvYkFF6tBKuGXc3OZJ1REOA5L9gRYicooWv92x4J8/
11g+eW5VlmKRJ88knqOrronCc2S27bFFaDXAFnYqx9Kbt8hZfpl5PvZ8EyUwB+kV8j
4GPNrw5ykulSys8iw==
```

```
NUH8DARvndRJcqkWRJGOcEuXlyAEZHUw1fz+rj5huYoBdF+C9N2Juy7swjKK2Qzd
FZbleWuKZYdE3jSLMxo5pWCsg9bxubvd/XUe8KYshedP5Q1xyXV09aK45iERDHg4
eVlwcvAZYaBSWBeP7UY7N/wbNlKMzRatky8crSHtDxelO2UuActFlA+0e7vgz9p+B
yEmfsbCRmFJxJgpmdtvluVOKdBWWqLBtHbQFSQPfQ6il5WbgHuxWbnTTuVEf2lBO
Z2XGTlWTKLl5AWjmHvDi8i1WhFCb60xlZAlRyKPrW/BD3n4xjl1lDiNFSu0io5D9ujbhQn
KLcmgJ9PHDEc7Og==
```

The hash verification process in fact played an important part in events during the final week of Internet voting, and is discussed later below.

[25] Completely rewriting the history requires that the repository hasn't been downloaded or forked – a repository that anyone can openly and easily copy -- and also requires coordinated effort among all actors. This works for the Ministry in this aspect, but is also a possible concern should the hash encryption not be truly random.

Phase IV: Final Election Phase

As the Internet voting came to a close on 6 September in advance of the actual Election Day (9 September), several steps took place. These next steps, on separate airgapped servers, included:

- *Cleansing*: a process to ensure that only the last Internet vote per voter would be counted during advance voting, and then only one vote per voter for the entire election would be counted: any paper ballots cast during the advance voting period or election day would override the Internet vote.
- *Mixing*: a process to destroy the connection between voter and votes.
- *Counting*: a process to decrypt the votes and count them, and finally to submit the final count to the central election administration system.

As an additional step, as mentioned before, the nine members of the Internet Election Committee came together equipped with their smartcards on election night. Before a public audience and livestream broadcast, they provided their cards upon random selection, and the decryption key was created – again before the public and only after polls had closed.[26] With the decryption key, preliminary counts for the Election were then able to be generated.

A little more in depth: End-to-End Verifiability ("E2E")

Before dealing with issues that arose in the implementation of the system, the importance of *cast as intended* and *stored as cast* needs to be clarified; they are tied to the concept of end-to-end verifiability.

End-to-End Verifiability Voting Systems or "E2E" are electronic systems that attempt to ensure that votes *cast as intended* are those included in the final count, and counted appropriately. Furthermore, some receipt is issued during the process that allows various confirmations:

- *Ballot Casting Assurance*: an individual voter can have "*direct verification* that *her vote* was properly cast and recorded into [the final] tally"
- *Universal Verifiability*: "any observer can verify that only registered voters cast ballots and that cast ballots are tallied correctly"
- *Possibility of Failure Recovery*: should it be determined that votes have not been properly recorded, complaints can lead to the possibility of a revote or recount.[27]

[26] *Decryption and counting ceremony of the Internet votes, English language*, http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-trial/news-about-the-e-vote-2011-project/year/2013/decryption-and-counting-ceremony-of-the-.html?id=735366

[27] Original emphasis, Adida and Neff, "Ballot Casting Assurance."

Though Norway's Regulations did not specifically require the implementation of an E2E system, they clearly required E2E aspects like ballot casting assurance through the return code SMS.[28]

Although systems like Ben Adida's HELIOS – a recognized standard in Internet voting verifiability but importantly, explicitly not intended for binding country elections – are designed accordingly, it is not clear that an E2E system necessarily possesses all three hallmarks. At least in practice, it is an open question as to what degree the average citizen should be able to audit or verify aspects of an Internet-voting process.[29]

The Norwegian I-voting team did not attempt to make every part of the chain one that average voters would be able to audit or verify. Instead, they created a hybrid model where individual and proxy verification were both in play. Earlier parts of the process involved individual actions; checking the SMS return code or the hash signatures were, according to design, processes in which voters can themselves verify information. With this verification, they might have Ballot Casting Assurance that their vote was *cast as intended* and *stored as cast*. At the same time, the receipt was not sufficient to be used as a recount mechanism or as proof to a vote buyer or coercer (since a voter can vote multiple times, there is no telling when a receipt is truly final). When it came to the final mix and count of electronic votes, or the latter half of the E2E chain, the Norwegian case relied on an interesting form of proxy verification. One of the ways that Quality AS, the consulting firm with electoral and technological expertise commissioned by the Internet Election Committee, verified the integrity of the vote was through mathematical zero knowledge proofs.

[28] Kommunal- og Regionaldepartementet, *FOR 2013-06-19 Nr 669*, §5.

[29] The absence of universal verifiability is a problem fundamental to computer-based election systems, but electronic systems are not uncommon; the issue of trust is reflected on later in this report.

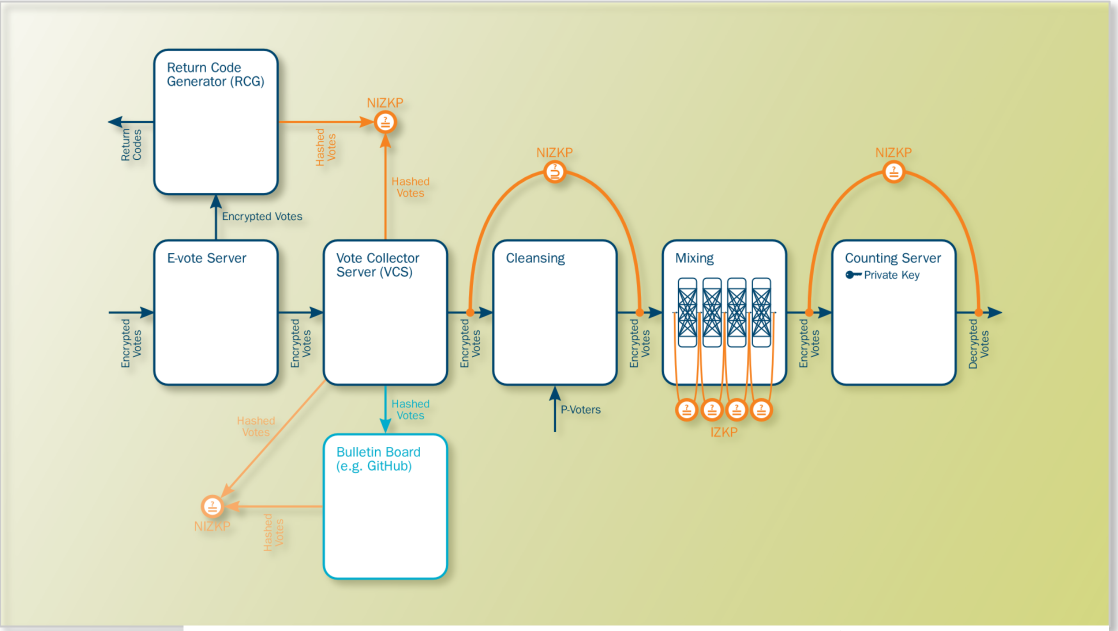


Figure 6 - Verifications via Quality AS Zero Knowledge Proof

Zero knowledge proofs are black-box proofs, in which a verifier can prove that a particular statement is true without having to know the content of the statement itself. In the case of voting, zero knowledge proofs or ZKPs are supposed to allow verifiers to demonstrate that the votes that came into the system are the same as the ones that came out, but without having to know the exact contents of each ballot. The diagram provided by Quality AS above shows orange Non-Interactive Zero Knowledge Proof (NIZKP) vectors, which represent the points at which Quality AS ran Zero Knowledge Proofs on the data. Their proofs demonstrated, without knowing the contents of the data directly, that what was submitted to the system through appropriate channels resulted in a final count of legal votes.

Thus, in the combination of individual and proxy verification, the Norwegian team argued that it had created a complete end-to-end verification for the Internet voting process, from *cast as intended* to *counted as stored*.

In practice: vulnerabilities and implementation

Before getting into the details of how well the system worked in practice, there were a few areas of potential vulnerability concerning the requirements of secrecy in theory. Some of these issues did in fact surface in the actual implementation.

Potential vulnerabilities

The generation and printing of the return codes raised two possible problems related to secrecy. The first was the actual printing of the cards: voter names and addresses were required on one side of the cardstock for postal delivery, while the verification codes were printed on the other side. This very paper therefore physically linked voter and vote cast. Without the printing process being handled in a way to prevent the viewing or linking of those two sides of paper, the advantage (and the work) of having *separation of duty* such as separate servers with encryptions could be lost.

During the 2011 trials, the Ministry set a high bar in order to protect against this possibility: two different machines were set up to handle the printing of the cards. The first printer printed the return codes associated with a random identifier. Then the second printer interpreted the random identifier and printed voter information on the other side of the card. Unfortunately, as documented during the 2011 trials, there were errors and mismatches in this printing process that pointed to the need for better design, testing, and implementation.[30]

For 2013, they decided to simplify everything by printing from a single printer that would automatically fold the cards, thus hiding the connection between voter and codes from view. How this plan fared is discussed in the next section.

Another small vulnerability in the system existed simply through the receipt of the cards themselves. Members of the same household, for example, would easily be able to intercept another's mail and in theory be able to verify votes cast for a given party, thereby enabling coercion. However, the return code card was only meaningful with access to the voter's SMS messages; the vulnerability is limited by the difficulty of having access to the voter's mobile phone. In addition, constant access would have been necessary, as another, later vote and SMS could cancel out any earlier submissions – not to mention the fact of paper voting in polling stations either in advance or on the day of the election. However unlikely, it is worth noting that the possibility remained.

It is worth noting because the possibility of coercion, though addressed in the I-voting design, was not completely mitigated, and in ways that had nothing to do with the system but through the uncontrolled context. As discussed earlier, voters had to verify their identities through one of several systems, based upon the idea that access to these systems was sensitive and unlikely to be shared. At the same time, one of the proposed advantages of Internet voting is increased accessibility of voting to the disabled and elderly. Indeed, results from this year's Internet voting indicated higher participation by persons in the 90-year percentile. But it is conceivable that the votes of some 90-year-olds were cast by, for example, a younger grandchild. In other words, best construed,

[30] Oliver Spycher, Melanie Volkamer, and Reto Koenig, "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting," in *E-Voting and Identity*, ed. Aggelos Kiayias and Helger Lipmaa, Lecture Notes in Computer Science 7187 (Springer Berlin Heidelberg, 2012), 19–35, http://link.springer.com/chapter/10.1007/978-3-642-32747-6_2; OSCE/ODIHR, *Internet Voting Pilot Project Local Government Elections 12 September 2011: OSCE/ODIHR Election Expert Team Report*, accessed July 11, 2013, http://www.osce.org/odihr/88577.

there are situations of dependency such as elderly or disabled parents who desire to relinquish all control of online presence including voting to designated proxies. There are, however, less ideal scenarios. The nature of coercion is further explored towards the end of this report.

Problems encountered in practice: printing and cryptography

Printing

For 2013, in addition to the changes to the printing process, the KRD transferred the printing from an external vendor to one in another branch of the government and within walking distance. As documented by the verifier Quality AS, there remained problems with the printing process that sometimes demanded human involvement to facilitate folding. But the problems overall do not appear to have resulted in the errors or difficulties experienced during 2011. In addition, Quality AS served a critical function in ensuring the destruction of anything that would "disclose the connection between return keys and individual voters during the printing process."[31]

A point of interest is that during the observation in July, it became clear that a certain PC with USB stick contained all the information related to voters and return codes in plaintext format. Through conversation, procedures had been put in place in order to require the combined participation of three units -- KRD personnel, Quality AS personnel, and printing department personnel – to gain access to the laptop and computer used in the printing. These procedures, which were good ones, were however not documented in any way that observers had access to and were seemingly laid out through practice.

Cryptography

During the final days of the Internet voting period, a bug in the software was discovered that posed a serious threat to the secrecy of the ballot. During a verification of the integrity of the cleansing process, Quality AS discovered that some of the El Gamal encrypted ballot strings were identical. Such an occurrence is impossible in a truly random encryption process. Upon investigation, it was discovered that due to a simple error in the code, the random number generator function was in fact generating fixed numbers. In the opinion of the cryptographer on the Internet Election Committee, Håvard Raddum, the encryption was so weak that ballots could be considered virtually the same as plaintext, or entirely non-encrypted.[32] By the point that the bug was discovered, some 29,000 votes fell into this "weakly" encrypted category.

[31] Vollan, *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys, Version 0.1 DRAFT*.

[32] Håvard Raddum, interview by Connie Moon Sehat, September 9, 2013.

The IEC was informed of the encryption problem on Tuesday 3 September. The I-voting team immediately fixed the code that evening, added additional encryption, and severely limited access to relevant servers. The suggestion to continue with Internet voting with the extra security measures was presented to the IEC, which was informed on Wednesday 4 September that they had until the morning of the next day to decide what to do.

During this period, Raddum communicated concerns about this solution via email first to the chair of the committee, and then when it became clear that decisions to move forward were about to be made, also with the broader group. From the standpoint of a cryptographer, he explained that the votes were practically unencrypted and endangered the secrecy of the vote, the specific purview of the IEC. From his perspective, he would have felt better if the votes were discarded and all 29,000 voters were notified via SMS of the need to revote. He expressed understanding about why this course, by potentially disenfranchising any number of voters who did not know or were unable to submit their re-vote, may have been ultimately unacceptable. However, as a cryptographer, Raddum also felt compelled to stress that a fundamental framework of the system had failed.[33]

In informing the electorate, the Ministry posted a statement to the website on 5 September (Thursday), that explained that an “error in the encryption of the Internet votes cast” was discovered, but that it “had been corrected and has no effects on the election results. All Internet votes are correctly cast and will be correctly counted.” The Ministry confirmed that “some of the Internet votes are now less encrypted than planned” but explained the tightening of the system that occurred since. In addition to explaining that access had been restricted and that activity logs were being reviewed, the post mentioned that the IEC had “has taken the Ministry’s reviews into account.”[34] The IEC did not issue its own statement.

Unpacking the problem

With regards to this cryptography problem, several points can be made. First, it was an unfortunate mistake in the code, but one that was not completely unforeseen. From July, it was clear to those familiar with software coding practices that the I-voting team’s rapid development was going to make errors more likely. In response to a question put to the Team in advance of the July observation, KRD indicated that there would not be a true date at which the code would be frozen (when no additions to the code would be made). In later communications specifically around the erroneous line of code, it became clear that safeguards such as code review had been discontinued.[35] Any development –

[33] Ibid.

[34] Ministry of Local Government and Regional Development, “Protection of the Internet Votes,” Redaksjonell artikkel, September 6, 2013, http://www.regjeringen.no/en/dep/krd/information-campaigns/election_portal/nytt-om-valg/2013/protection-of-internet-votes.html?id=735145.

[35] Christian Bull to Connie Moon Sehat, “SV: Timetable/calendar for I-Voting Trials, Esp. July Timeframe,” June 24, 2013.

especially rapid – will result in overlooked critical bugs, which is why rules of thumb exist to estimate the likely number of coding errors per lines of code. Hence, stable code is necessary for adequate regression testing and review. The overall rapid development practice may have reflected a decision that the venture should be considered a "true pilot" – one in which the boundaries of Internet voting should be pushed and tried. Though there is tension between a true pilot and the requirements of binding election votes, pilots can still preserve some safeguards. However, the decisions to bypass processes such as code freeze and review were not careless ones, but made in the belief that the verification built into the system itself offered security. Because E2E verification assumes distrust, advocates argue that any particular issues or workings in the system will bear out in the sum of the whole.[36] This contention will be addressed later.

A second point is that the Internet Election Committee did not appear to be prepared to make the kind of decision that they were called to make. Despite the presence of a cryptographer, it is unclear to what extent the rest of the committee understood his recommendation. Instead making a decision about encryption content, it is more likely that the Committee made a choice between two assumedly *trusted* sources of information: the cryptographer or the (alternative posed by the) Ministry. Beyond this, defined procedures that may have mitigated the circumstance, allowing adequate time or space as a body in which to deliberate decisions, did not exist. It is difficult to know exactly how long and how much information those committee members, dispersed across the country, had to consider the issue.

Thirdly, though the Ministry team was ultimately completely transparent about the problem, its initial website communication was a little opaque. While explaining that a problem was discovered, the site did not explain how, for example, secrecy of the vote may have been compromised.[37] To be sure, in successive days after the posting and in their own webcast around the decryption ceremonies, KRD representatives were absolutely open and straightforward about the problem. IEC members such as Raddum were also free to give interviews about cryptographic problem.

But a final, important point is that the Ministry's own verification protocols in fact led to the discovery of the problem. Thus, an aspect of the system "worked" well in spite of the bug. Via Quality AS verifications, safeguards put in place to verify their work on a very complicated and not well-understood technology did their job.

Challenges and Reflections

Both the printing scenario as well as the cryptography problem point to two very practical themes for these trials: the relationship between system design and implementation, and

[36] This point is also made in the design of the Helios system.

[37] Ministry of Local Government and Regional Development, "Protection of the Internet Votes."

the lack of documented procedures. There are also some higher conceptual challenges that Internet voting poses including a tradeoff between vote integrity and secrecy.

Integrity versus Secrecy

A key challenge of encrypted electronic voting overall, let alone Internet voting, is that there is a tension between two requirements: integrity and secrecy of the vote. Both are requirements but they are in conflict with one another. To insure that the final tally only includes legitimate votes, you need to have some connection in the system with the voter. But maintaining the connection to the voter is what lessens the likelihood of secrecy, and this is compounded in a long voting period on an insecure platform or open system such as the Internet. In general, the system can provide either unconditional integrity or unconditional secrecy, but not both.

In the Norway system, as with many other systems, the property that is regarded as more important is unconditional integrity.[38] Information Risk Professor Wolter Pieters and Philosophy of Ethics Professor Marcel J. Becker have argued, "for Internet voting, the need for transparency (through verifiability) supersedes the need for absolute vote secrecy, especially as people are voting from unsupervised environments anyway. They accept the failure in vote secrecy as necessary to implement verifiable Internet voting."[39] But where does the decision of integrity versus security lie: with information and computer experts, state employees, or by the people of the nation?

End-to-end encryption, ideally, attempts to solve both the problem of integrity and secrecy. But its ability to do this really depends on two things: the implementation of the system and also a certain amount of trust.[40] Furthermore, as demonstrated in the Norwegian case, the proxy verification as part of the E2E requires a bit more clarification: who is qualified to be a proxy for the people in such a verification scheme?

Turning our attention to the role of Quality AS, it seems that the vendor was sometimes meant to serve as a proxy for the voter: in their ZKP activities, for example. Yet another proxy group gave this role: the Internet Election Committee. However, Quality AS's ability to meet the demands of this task was complicated by the fact that at the same time, it served also as a kind of *internal* Quality Assurance (QA) function. During our

[38] Ben Adida, "Helios: Web-Based Open-Audit Voting.," in *USENIX Security Symposium*, vol. 17, 2008, 335–348, https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf.

[39] (Pieters and Becker (2005):11) according to Barrat i Esteve et al, 2013, p 34.

[40] Recent argument that encryption solves integrity and secrecy, see Jeremy Clark, "Democracy Enhancing Technologies: Toward Deployable and Incoercible E2E Elections" (University of Waterloo, 2011), http://www.uwspace.uwaterloo.ca/handle/10012/5992; Example of systems-based analysis, beyond cryptography, Karlof, Sastry, and Wagner, "Cryptographic Voting Protocols"; On the issue of trust, David Wagner to Connie Moon Sehat, "Norway Internet Voting System and Election Observation," August 7, 2013.

observation, the relationship between testing, software development, and verification were at times closely entwined. Even during the printing of the voting cards – Quality AS seemed also to be providing technical assistance in order to fulfill requirements of secrecy. Finally, although Quality AS was hired by the IEC through a formal bid process and responsible to the needs of the IEC – not the Ministry – it seemed to at least one committee member that Quality AS was presented to them by the Ministry as the advisable choice.[41] Thus, the meaning and degree to which a verifier, such as Quality AS, may serve as a proxy for the voter requires more reflection.

Electronic versus paper voting

For the purposes of the Norwegian trials, there were several important considerations when comparing the electronic voting with the paper ballot standard: a new electronically centralized election system, paper ballots in polling stations on election day, and the advance remote postal vote.

With this election, the Ministry introduced a new level of centralized electronic administration (Elektronisk Valgadministrativt System, or EVA). The system had several functions. It handled the complete electoral rolls, allowing voters to vote from any polling station in the country. Related to this was handling the possibility of multiple voting: it recorded whether the eligible had voted, so that for example an Internet vote could be thrown out if a paper vote was received. It also introduced new software for scanning, used in the automatic tallying of votes, so that paper ballots scanned into the system were automatically evaluated for the party choice as well as any edits to the presented party platform.[42] In its vote counting aspect, EVA required that humans evaluated any problem ballots, either the virtual scanned copy or original paper ballots that were kept in case of a recount. On Election Day, informal visits to a few polling and counting stations demonstrated how election officials handled the EVA system.

The visits to polling and counting stations also served as a helpful reminder of the paper standard to which Internet voting is supposed be held. Of the three polling stations the OSCE/ODIHR and The Carter Center visited, one had a noteworthy failing: the lack of any securing device (locks or zipties) of the ballot boxes. These were not present anywhere in the materials received for the polling station. In addition, the head of the polling station confessed that the boxes had been set up in advance of her arrival, that she had no idea whether the ballot boxes were empty at the beginning of the day – she trusted that they had been. In all the stations we visited, moreover, there seemed to be no procedure or understanding of what the codes on each ziptie might signify. These few and anecdotal observations cannot lead to any conclusions about polling procedure in Norway. However, it is worth noting that Norwegian Broadcasting (NRK) and the

[41] Interview with Sehat, 26 July 2013.

[42] The scanning process was not new, but the software was.

Norwegian Helsinki Committee/European Platform for Democratic Elections also reported unsealed ballot boxes, the latter going so far as to say "in many places the ballot boxes were not sealed."[43]

Finally, as mentioned earlier, advance remote postal voting seemed to offer the closest paper-based comparison to Internet voting scenarios. Due to the unclear procedures around the verification of postal ballots in addition to the disinclination to throw any out, and thereby disenfranchise some voters, one might assume the possibility of a small batch of extra votes being counted. However, this may not have been the case: because of EVA's reconciliation, counting multiple ballots via post or electronically may have been handled correctly – one vote per voter. More research would be required to know definitively. Paper-ballot advance voting, too, depends on the appropriate actions of the officials or procedures as well; for example, Norwegian Broadcasting (NRK) reported that some 400 advance voting paper ballots in some counties were not delivered in time for the count, the responsibility of which was attributed both to the postal service and to late submissions from election officials.[44]

In the end, just as with electronic voting, paper voting requires correct implementation of the system as defined or designed.

However, there are limits to the association between postal and Internet voting. Though they share the context of uncontrolled environments, any further comparison must take into account all the preconditions as well as the impact of potential failures. One might be tempted to say that Internet voting standards in Norway are at least more rigorous than current postal voting standards, including stronger requirements for voter authentication, and aspects of individual verification – something not possible for postal votes today. But Norway's frame for postal voting and its corresponding laxity is related to the fact that only a small number of votes will be submitted via post.[45] This means that any

[43] "Election Observers Find Some Faults," *NewsinEnglish.no*, September 9, 2013, http://www.newsinenglish.no/2013/09/09/election-observers-find-some-faults/; Norwegian Helsinki Committee and European Platform for Democratic Elections, *Parliamentary Elections 9 September 2013 Kingdom of Norway Press Release: Fair Elections with Potential for Improvement*, September 10, 2013, http://www.epde.org/tl_files/Newsletter%20Norway/Press%20Release_fair%20el%20with%20potential%20for%20improvement.pdf.

[44] As reported by "Probe Launched into Ballot 'scandal,'" *NewsinEnglish.no*, September 13, 2013, http://www.newsinenglish.no/2013/09/13/probe-launched-into-ballot-scandal/.

[45] Procedures for postal voting validity are clearer in Geneva, where a reported 95% of voters cast their ballots by mail, though opportunities for abuse are just as clear, "E-Voting - The Geneva Internet Voting System," accessed October 16, 2013, http://www.geneve.ch/evoting/english/presentation_projet.asp; State Chancellery, Republic and Canton of Geneva, *State Council's Report to the Grand Council on the Geneva Electronic Voting Project*, June 2006, http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf; State Chancellery, Republic and Canton of Geneva, *Comparison of OSCE Observations and Recommendations with the Genevia*

coordinated effort to manipulate, alter, or coerce either the votes will have negligible impact.[46] Internet voting possibilities, should they be opened to a large proportion of the population – large enough to impact election day results – and should they no longer be seen as a supplement to voting, should require a thorough reconsideration of the assumptions and framework to see how well the similarity with postal voting bears up.[47]

Vote Buying and Coercion

Perhaps the most important concern regarding Internet voting from home, or outside of a controlled environment, is the potential for vote buying and coercion. The secrecy of the ballot booth no longer exists, and therefore, we cannot know if voters were either forced or bribed into casting their vote for a candidate they would have otherwise not elected. The key method that the Norwegian system uses to mitigate this problem is through the allowance of repeat voting.

Representatives of both the KRD and the Internet voting team repeated this argument during their presentations of the Internet-voting system to the public on 8 September. In the overview of the Electoral System, members of the Ministry indicate that repeat voting is: "A possibility for e-voters to vote again as many times as they wish to prevent undue influence and coercion."[48]

Specifically among the challenges of "remote e-voting" that the KRD attempted to address were both vote selling and "coercion/family voting," which had been highlighted as a particular area of concern in Norway. The repeat voting system, in their option, mitigates the situation:

> The coerced can re-vote...Votes submitted from a polling station will supersede any vote cast remotely, The system will never divulge that a previous vote has already [sic] been recorded, If you accept that bastards are evenly distributed across the political spectrum, that doesn't really scale either.[49]

Internet Voting Procedures, March 7, 2012, http://www.ge.ch/evoting/doc/rapports/OSCE_final_report_w_comments_E.pdf.

[46] Including Geneva, there are instances where postal voting makes up the majority of the vote, and the possibility of large-scale postal voting fraud is something that needs more researching. A recent example on the local level of coordinated postal voting fraud (and the problems of coercion), occurred in "Judge Upholds Vote-Rigging Claims," *BBC*, April 4, 2005, sec. West Midlands, http://news.bbc.co.uk/2/hi/uk_news/england/west_midlands/4406575.stm.

[47] Assumptions about Internet voting and scalability that went into the design in Norway were articulated in a presentation on verifiability, Bull, "Safety First! Verifiability in the Norwegian E-Voting System."

[48] Marianne Riise, Dolven, and Mjøsund, "Information Session on the Norwegian Electoral System," September 8, 2013, http://www.regjeringen.no/pages/38377245/1_information_session_election_observers.pdf.

[49] Bull, "Safety First! Verifiability in the Norwegian E-Voting System," Slide 19.

With regards to coercion, the argument is two-fold: that a victim of coercion has many opportunities to escape an oppressive context and re-vote and that, in any case, the impact of any real coercion will not be significant enough upon the final result – thereby perhaps lessening the attractiveness of the option for coercers.

This system may mitigate against vote buying, but there is a significant problem with the assumptions regarding repeat voting and coercion. Electoral system expert Kåre Vollan has addressed the possibilities of paternalistic family structure and group pressure upon Internet voting. In addition to outright coercion, Vollan attempted to address the subtler problem of influence: in a non-secret, non-individual context – which Internet voting in an uncontrolled environment allows – it may be that especially younger people may not fully understand the significance of casting a secret ballot. Even in the case of repeat voting, Vollan notes

> By early Internet voting the voter may be given a possibility to change his or her vote either on the Internet or by casting a ballot in person on election day. That would offer a possibility to such voters who might have been under pressure by family members, community leaders or friends to cast a particular Internet vote to override the vote on election day in controlled environment[s]. This would only help in such cases where the voter ***is conscious enough to want to exercise the right to a secret ballot*** [emphasis added].[50]

In other words, repeat voting will not take care of the cases where the voter does not really understand the link between ballot secrecy and election integrity, and freely gives up their vote to a group of friends or to family members. In this case, the voter has lost or never understood their individual responsibility, and the significance of individual participation in the democratic system.

The study at hand makes a related but different point. In general, many current discussions and designs of e-voting systems are based upon a too limited understanding of coercion. At bottom, the supposition at work in the repeat voting scheme is that once a person is removed from the particular situation in which pressure is applied, then she or he would be able to register their true will at another computer during another time or even at the polling station. One assumption, not necessarily shared by all, that even runs through the I-voting literature is that an Internet voting scheme might one day be made to be "incoercible."[51]

But this belies what coercion is, and how it works. Social and political philosopher Scott A. Anderson has written at length in recent years about the concept. In a nutshell, he

[50] Kåre Vollan, "Voting in Uncontrolled Environment and the Secrecy of the Vote," in *Electronic Voting 2006*, ed. Robert Krimmer, Lecture Notes in Informatics (Gesellschaft für Informatik, 2006), 167.
[51] As an example of a work that "continues the more recent trend in the literature of building voter-verifiable systems that are both incoercible and practical," Clark, "Democracy Enhancing Technologies," 2.

notes that coercion "generally disables (or threatens to disable) its target from being able to take effective countermeasures, or renders him unlikely to succeed or dangerously imprudent."[52] It does this because the coercion is part of a relationship between more powerful and less powerful persons, where assessing the costs of behaving outside the sensed will of the more powerful begins to enter the realm of the psychological and not entirely conscious desires.[53]

Put more concretely, if a person is in a position of power over someone, enough to have access to their MinID or look over their shoulder and force a particular vote, then it is not necessarily the case that repeat voting provides a real option to a coerced voter.

To be sure, given this situation, it may be the case that this kind of relationship – this kind of coercion – can also affect actions within the polling booth.[54] But, Anderson's main point, which is not concerned with electoral law in particular, has to do with the protections that public spaces are supposed to afford: "a state's authority depends on its ability to monopolize and regulate coercion among its subjects, because individuals need protection and stability against unpredictable, private uses of such power."[55]

Allowing Internet voting not only increases the number of opportunities that the electorate may have to engage, it may also remove the legally protected space of the ballot booth. With the regulations related to the Internet voting trials, the Electoral Act's Section 8-4(1) "Voting shall take place in a secluded room and be unobserved," was specifically held not to apply. Instead, it was replaced with Regulations, §16-1 "Voters shall personally ensure that their Internet vote is cast in private."[56] Whatever the rewards, there is risk, and Anderson's final thoughts on this are worthy of consideration: "private, unauthorized uses of coercion constitute a failure of the state to protect its subjects in accord with the conditions of its authority, thus leaving them to engage in self-help, such as acceding to the demands made by those private coercers."[57]

[52] Scott A. Anderson, "The Enforcement Approach to Coercion," *J. Ethics & Soc. Phil.* 5 (2010): 28. In fact, Anderson has been trying to upend the particular notion that equates coercion with pressure, and thus coercion as epiphenomenal – a model more associated with philosopher Peter Nozick. Instead, Anderson stresses coercion as behavior enforcement and reintroduces the nature of power into the equation.

[53] Anderson, "The Enforcement Approach to Coercion."

[54] And if Josh Benaloh is right, the polling booth may not be so secure anymore either, Josh Benaloh, "Rethinking Voter Coercion: The Realities Imposed by Technology," *The USENIX Journal of Election Technology and Systems*, 2013, 82.

[55] Anderson, "The Enforcement Approach to Coercion," 31.

[56] Kommunal- og Regionaldepartementet, *FOR 2013-06-19 Nr 669.*

[57] Anderson, "The Enforcement Approach to Coercion," 31.

Trust in a complex world

When it comes to Internet voting, in the end, trust is required. Even with various levels of verifiability, there is a level of trust that must ultimately be present for any electronic voting system to work.[58] For example, although voters received their Return Codes via SMS and were able to verify hashes and hash signatures on a public bulletin board, they still had to trust that the servers used to receive votes, send SMSs, or post to GitHub, were in fact the ones used in the final tallies. And even if the bulletin board is an accurate reflection of the stored votes, in the case of multiple voting, she still has to trust that system will take the very last one submitted for the final count.[59]

Technically speaking, even in a system like Helios built upon the fundamental supposition of distrust, there was still a choice to be made: one does not have to trust the system for integrity given the auditability of the design. However, one still has to trust the system to protect privacy or secrecy (the tension between integrity and security previously mentioned).[60]

In the United States, there does not appear to be that level of trust in the potential for Internet voting to address these challenges. A number of US academics associated with the Verified Voting Foundation, a non-profit organization that advocates for auditable voting systems, for example, have endorsed a statement that they do not believe that Internet voting has been able so far to meet the challenge of being verifiably accurate, and until it is so, that it should not be adopted:

> - Election results must be *verifiably accurate* – that is, auditable with a permanent, voter-verified record that is independent of hardware or software. Several serious, potentially insurmountable, technical challenges must be met if elections conducted by transmitting votes over the internet are to be verifiable. There are also many less technical questions about internet voting, including whether voters have equal access to internet technology and whether ballot secrecy can be adequately preserved.
> - Internet voting should only be adopted after these technical challenges have been overcome, and after extensive and fully informed public discussion of the technical and non-technical issues has established that the people of the U.S. are comfortable embracing this radically new form of voting.[61]

[58] Melanie Volkamer, Oliver Spycher, and Eric Dubuis, "Measures to Establish Trust in Internet Voting," in *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, ICEGOV '11 (New York, NY, USA: ACM, 2011), 1–10, doi:10.1145/2072069.2072071.

[59] Spycher, Volkamer, and Koenig, "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting."

[60] Adida, "Helios."

[61] "Computer Technologists' Statement on Internet Voting | Verified Voting," accessed October 14, 2013, https://www.verifiedvoting.org/projects/internet-voting-statement/.

However, in Norway, trust in the government overall is high, such that for the Norwegian 2011 pilot, there have been no public debates about any of the weaknesses described by Professor David Wagner of UC Berkeley about the problems with Internet voting overall:

- There is no way for a voter to verify that their vote was cast/recorded as they intended (without trust in computer systems/software).
- There is no way for an interested citizen to verify that all of the recorded votes were counted as they were cast/recorded. The system doesn't have an audit process that is open to the public that would allow to verify this (without trust in computer systems/software).[62]

But for the moment, let us say that we sidestep the issue of trust, and assume that the system owners are well intentioned and that internal threats do not exist. Regardless of the intention of the designers, they may have not designed the system in a way to address all possible compromises. Effectiveness is not the same thing as trust. And simply put, the Norwegian I-voting is a highly technical and complicated system: the greater the complexity, the more avenues of risk and failure.

Speaking to the complexity of the system was the critique made – at the invitation of the Ministry – by Swiss academic Reto Koenig. His research is based on the security models used in Internet banking. In a presentation given just prior to election day, he pointed out two ways that adversaries could take over the SMS receipt channel, and thereby submit false votes to the system via email or phone clients without the voter realizing anything.[63]

Again, the fact that the Ministry team has continued to invite critique from members of the academic and election communities, and then openly shares this information speaks both to their transparency as well as their considerable understanding of the difficulties related to securing this system. And compared with the levels of transparency, sophistication, and interrogation available by electronic (not Internet) voting systems, the KRD has created an amazing model. They know very well that the only way that the system can hope to improve is through encouraging the discovery of potential issues by as many persons as possible. As the software progresses and related dependencies change – such as even browser software -- vulnerabilities for this complex system will continue to exist, and need to be addressed each time it is used.

Ultimately, systems cannot by themselves guard against collusion, oversight, or omission. In the case of the printing cards, or the keys, the Ministry attempted to show that only a

[62] Wagner to Sehat, "Norway Internet Voting System and Election Observation."

[63] Reto E. Koenig, "A Security Flaw in the Verification Code Mechanism of the Norwegian Internet Voting System" (presented at the Ministry of Regional of Local Government and Regional Development, Oslo, Norway, September 8, 2013), http://www.regjeringen.no/pages/38377245/4_a_security_flaw_koenig.pdf.

sophisticated conspiracy could manufacture or rewrite Internet votes, including processes such as always using new USB drives for ballot box data transfer to requiring multiple key holders for decryption. However, security hinges on specific preconditions or processes happening in a certain and consistent order or way. Because the secure implementation of technical systems are dependent upon a number of factors, well-documented procedures are critical to enabling adequate reflection about possible system weaknesses.

The Role of Observation

What exactly is possible for an election observation team to accomplish when it comes to Internet voting? Given that we are dealing with technical systems, it seems fitting to introduce technical standards and processes to consider. In 2005, Vollan's paper on *Observing Electronic Voting* did just that, offering definitions of *verification, validation, audit, observation,* and *certification* that are a useful springboard for further consideration.[64]

Although related, there is an important distinction between verification and validation. To clarify the difference, the technical notions of *Verification and Validation* (also known in shorthand as *V&V*) in software engineering are both helpful and apropos. The contrast between the terms is sometimes described as "are we doing the job right?" versus "are we doing the right job?"[65] Verification is an attempt to ensure that the *product is built correctly*, in the sense that the output products of an activity meet the specifications imposed on them in previous activities. Validation is an attempt to ensure that *the right product is built*, that is, the product fulfills its specific intended purpose."[66]

In other words, verification is attuned to how the process is carried out – whether the process can be said to lead to correct results, while validation looks at the end results and tries to see if they match up with the overall goals of the user or customer. If the end user/customer in this scenario is the people of a nation, then answers to both questions are of import to the observation process. Verification might be considered with whether defined e-voting processes have been followed while Validation relates rather to the goals or ends of an e-voting system to fulfill legal obligations for a democratic election. It should also be noted that software V&V processes requires participation at a very early

[64] Kåre Vollan, *Observing Electronic Voting* (Norwegian Resource Bank for Democracy and Human Right (NORDEM), 2005), emphasis added.
[65] Attributed to Boehm, Software Engineering Principles.
[66] Institute for Electronics and Electrical Engineers (IEEE), "Chapter 11: Software Quality," in *Guide to the Software Engineering Body of Knowledge*, accessed October 3, 2013, http://www.computer.org/portal/web/swebok/html/ch11.

development stage – something that will need to be taken into account for Internet voting observation development.

For the most part, Vollan outlines what he believes are the responsibilities of Electoral Management Bodies (EMBs) and not observers. He is right to point out that an observation mission cannot *fully* verify nor validate the system, and certainly not certify it. For observers, he stresses a role of review and audit around processes and some amount of verification. In his opinion, "The observer mission may, however, do very useful checks on both the process of acquisition, the overall functionality of the system, and the electoral process based on audit trails.[67]

But does this mean that observers cannot validate any I- (or E-) voting? Consider paper voting contexts, where in fact, observation includes components of validation in addition to review, audit, and verification. At the individual observer level, the election-day procedures themselves are certainly being evaluated when observers use checklists or questionnaires. For this purpose, references to *ISO 9001* or even *CMMI* – examples of two process improvement models with certifications used in software development – makes a lot of sense: so long as a process is well documented, then individual observers can certainly engage in checks against that process.

But this is only at the level of an observer filling out the checklist; both the construction of the observation checklists themselves and the interpretation of the data following from them involve elements of validation, and this is because of the nature of election observation itself. Election observation, as defined by the Declaration of Principles for International Election Observation, is the "systematic, comprehensive, and accurate gathering of information concerning the laws, processes, and institutions related to the conduct of elections and other factors concerning the overall electoral environment" with one of its goals being the enhancement of the integrity of election processes.[68] This interest in electoral integrity – different from vote integrity – requires attention both to processes and the norms undergirding them.[69] For the election observation organization, procedures may to a certain extent vary, but the hallmark of evaluation is ultimately whether or not the vote was "genuine" or "expressed the will of the people."

If the observation of an election – the ability to allow citizens access to points of validation and verification – is a requirement, then Internet voting (indeed for a number

[67] Vollan, *Observing Electronic Voting*, 16.

[68] "Declaration of Principles for International Election Observation," October 27, 2005.

[69] Pippa Norris, "The Concept of Electoral Integrity," Working Paper for upcoming symposium of Electoral Studies, May 10, 2013, https://dl.dropboxusercontent.com/s/gseod991492m2oq/Pippa%20Norris%20The%20Concept%20of%20Electoral%20Integrity%20Forthcoming%20in%20Electoral%20Studies.pdf?dl=1&token_hash=AAFG7wNSf9zJ3NozTYOyNkvm4nT4UyR6ReuUSAhjvvQMrA.

of electronic voting systems) poses a significant challenge. The degree to which a system involves cryptography or sophisticated, distributed software and hardware architecture decreases the prospects that voters can take part in the verification and validation process. Some technical concepts are too complicated for an average voter to be expected to understand.

However, this may underscore the value and role that professional observation can play. Already, if international and domestic observation organizations can be said to serve as a proxy for the citizen at large, their expertise in legal affairs is one among many things they bring to the table when assessing a country's electoral integrity. Professional observation organizations have the time, knowledge, and resources to devote to the process that average citizens are without. And technical expertise is something that is a growing requirement as well, as evidenced in elections with electronic voting systems. For Internet-voting observation, professional assessment needs may require further amplification and include additional specialized experts like cryptographers.

The specialized role of professional observation may help address issues with regards to Internet voting, and even have a special relevance for the specific question of individual and universal verifiability in Internet voting schemas. Consider to what degree paper verification processes are *truly* individual and universal. If there is a complete paper trail, for example, an election may in fact be verifiable or auditable both individually and universally. However, verification and audit of issues such as ballot validity are activities that take training as well as a certain skill set. It is worth mentioning, in other words, that the average person off the street is not without training able to verify or validate paper voting.

However, such observation can only take place when two conditions have been met – well-documented procedures and a long-term context. Opportunities for comprehensive observation over the long term are fundamental to the election observation process, specifically so as not to place undue emphasis on election day events themselves.[70] This again stresses processes within a system or context in the overall evaluation of electoral integrity. And, with regards to Internet voting E2E verifications: E2E is not sufficient to demonstrate vote secrecy or integrity, and in fact increases the need to have robust documentation. The point of both technical and operational procedures is not just for transparency, or protecting against bad intentions. Regardless of trust, procedures help establish the very ability of the implementation team to carry out good ones. It is only with full documentation, especially the non-software procedures, that one can have a clear view to the system and all its dependencies. The system and its dependencies are of primary import, because it is likely that some aspect will go awry. But without

[70] "Declaration of Principles for International Election Observation," 3.

understanding the assumptions that have gone into each step of the process, we cannot understand the implications of any decision in isolation.

In Norway 2013, the example of the IEC and the cryptography problem illustrated this point best. In the end, it may be that the best solution and decision was made. But it is important to note that cryptography is a critical foundation upon which the Internet voting process rests. If the cryptography is broken, the system's integrity is compromised.

Should an Internet-voting project be able to build and document their procedures clearly, along with all other system documentation, then observation may be able to serve an important function.[71] For professional organizations, it would require a shift in the observation model, as most of both the important work and observation would need to be done well in advance during the periods of development and setup and with much interaction of the planning and development technical team. Understanding the creation of procedures and then creating checklists against them is one way that observation may contribute to uncovering the dependencies that exist in the system and how they impact address concerns of integrity and secrecy. The Carter Center has noted similar challenges with regards to observing E-voting, including the need to start observation work much earlier and for persons on the mission with specialized skills.[72] Nevertheless, the specifics of an observation practice demanded by Internet voting would require more investigation.[73]

Conclusions

Despite concerns, Internet voting will possibly be employed more broadly in the future.[74] An overall transition to "e-governance" for some nations – nations with advanced Internet and mobile services – may transform or raise expectations about the ways that citizenry and government institutions should interact. Internet voting in the future may

[71] Observing certain information during an election period – for example, web stats and IP addresses – may be of limited value though possible. Sophisticated external attacks may be able to mask their source of origin, and in any case: should anomalies occur, the question then is: what then should occur if discovered – are points that need to be seriously mapped out in contingency planning, Georgia Tech Cyber Security Team, interview by Connie Moon Sehat, August 16, 2013.

[72] Carter Center, *The Carter Center Handbook on Observing Electronic Voting*, 5–6, 105.

[73] Preliminary discussion on this possibility of an Internet voting checklist/precondition with J. Alex Halderman, interview by Connie Moon Sehat, August 21, 2013.

[74] Although Canada has halted Internet voting aspirations for the time being, the government cites budgetary reasons, not conceptual ones. In fact, while (temporarily) halting the initiative, they noted the problems that currently confront paper voting, "Elections Canada Drops Plan for Online Voting due to Cuts," *CBC News Canada*, May 30, 2013, http://www.cbc.ca/news/politics/elections-canada-drops-plan-for-online-voting-due-to-cuts-1.1346268.

also offer ways of addressing deficiencies in particular country contexts that outweigh concerns. For example, considering the ways that electronic voting technologies have provided trust for Indian or Brazilian citizens, perhaps there is an Internet corollary.

Is Internet voting observable in a meaningful way? Based on the experience in Norway, the answer to this question is: yes, so long as adequate conditions and access have been provided. However, the requirements and conclusions from an Internet voting observation will be different from a paper-based election. What this report first stresses are important commonalities. Based on international obligations such as participation in political affairs or access to information, observation is derived from the citizen's right to confirm the integrity of the entire election framework and process. Over the last 15 to 20 years, election observation has developed into a professionalized practice that incorporates a wide range of legal and other technical areas of expertise. Any observation mission will encompass aspects of validation and verification, but it cannot serve as a complete validation or verification of the entire electoral process itself – whether paper- or computer-based.

Considerations and recommendations

For Internet voting, challenges emerged in particular regarding two key obligations:

- *Secret Ballot* – was a voter's right to anonymity preserved during the entire process and afterwards?
- *Equal Suffrage* – was one and only one vote counted per eligible voter, or did each vote have equal weight?

This has translated into two aspects of keen focus for votes cast over the Internet: *secrecy* and *integrity* of the vote.

As Internet voting moves forward, there are several points and recommendations to consider for electoral management bodies such as the KRD and for observation organizations such as the Carter Center.

Documentation regarding the system and procedures needs to be made available as soon as possible and maintained throughout the process. First and foremost, in order to be observable in a meaningful way, the process and software need to be described and explained as much as possible *in advance*, which includes but is not limited to

- Meaningful and timely access to hardware, software and, other key information, processes, equipment, personnel;
- Thorough and up-to-date documentation about all components of the system design and architecture;
- Well-documented procedures about the implementation of the system (and any changes introduced to it) at every level, and

- Well-documented procedures about the decision-making processes around the system.

The degree to which the system is documented affects the degree to which an observing group has access to the system's integrity, and therefore to which it can offer assessments about the degree to which Internet voting reflected the will of the people. System documentation affects an observer's ability to understand how a particular instance of Internet voting relates to international obligations both under optimal implications as well as in practice despite best efforts. Electoral management bodies should consider documentation needs during the earliest phase of an I-voting trial, and incorporate these products in the design requirements.

Internet voting systems are not static, and are at least as complicated, if not much more complicated, as new versions of software that should be tested accordingly. Second, an observation of a particular election cannot certify or confer the kind of formal approval that certification does regarding the software and hardware system used. Though seemingly straightforward, it is particularly important to recognize that software and hardware infrastructures will necessarily be different in later instances or versions, given the kind of changes that happen in computer development. This means that as an Internet voting system develops, one cannot assume the challenges or problems mastered earlier are still resolved. The important takeaways for observation organizations are:

- Every time a system is reviewed, no matter of previous legacies, requires a review of the entire system (in the Norwegian context, including what 'stayed the same' from the 2011 trials)
- It is important to note that an observation of an internet election is not of a particular "system" per se (e.g., Scytl-Norway) but of a version – the way it worked at a point in time (e.g., Scytl-Norway in September 2013).

As a related consideration, especially for electoral management bodies: compared to electronic voting systems with a lot of specialized hardware, internet voting systems do allow for an important possibility, the ability with relatively little additional outlay for the system to be practiced in public. It would be very helpful for electoral management bodies and for observation organizations to see these systems implemented in smaller ways – e.g., use in the elections of local councils, universities, or particular referenda with low political/financial impact. The on-going development of a platform or system in advance of nationally binding elections might play a key role in building confidence in Internet voting in the future.

Internet voting will require related experts in electoral management and observation. Third, the complexity of Internet (and also electronic) voting demands the involvement of the appropriate technological experts whose objectivity and competence is trusted, whether they act as proxy verifiers for electoral bodies or technical analysts on observation teams. In addition, introducing the standards of computer development or software verification, creating confidence in them through education, and encouraging vendors to submit to them are activities in which a variety of election stakeholders can take part.

Internet voting challenges the secrecy of the ballot in ways that must be resolved by each state. Finally, Internet voting will continue to present serious challenges to obligations of *secrecy* that encryption alone cannot solve. As Barrat i Esteve, Goldsmith, and Turner have expressed quite succinctly, "unsupervised environments cannot guarantee that voters cast their ballots alone."[75] Beyond this, they recognize that a key challenge in Internet voting is obscuring the connection between vote and vote cast, and recommend that "authentication data and the vote's value should remain separated."[76] Recommending this and ensuring this, with the possibilities for quick and massive data capture, are however two different things. The questions of privacy and secrecy in an age of big data against other obligations such as equal suffrage are difficult ones. As constituencies make decisions regarding paper versus electronic or even Internet voting systems, electoral management bodies can help people by providing clear explanations of the advantages, disadvantages, and risks of each system.

In the end, so long as international election observation helps to increase the transparency of the process of internet voting, it can contribute to an understanding of how well such a process can reflect the will of the people overall, preserving their right to secrecy, and ensuring each citizen's right to participate. And election observation organizations will be better placed to answer these challenges should future Internet voting projects make themselves as transparent as the Norwegian Ministry of Local Government and Regional Development did.

[75] Barrat i Esteve, Goldsmith, and Turner, *International Experience with E-Voting: Norwegian E-Vote Project*.

[76] Ibid.

Acknowledgments

The Carter Center offers its sincere appreciation to Norway's Ministry of Local Government and Regional Development, and in particular Hans Petter Gravdahl, Henrik Nore and Christian Bull, for their hospitality and readiness to answer all questions regarding the 2013 Internet voting system. We thank again the willing cooperation of the OSCE/ODIHR for allowing the Carter Center expert to collaborate with their mission and to participate in multiple join meetings and share information.

In addition, several exchanges with technical experts from within and without Norway helped to provide clarity with regards to the difficult issues surrounding Internet voting. Conversations and e-mail exchanges with J. Alex Halderman, Andrew Howard, Rob Myers, Chris Smoak, Kåre Vollan, and David Wagner were greatly appreciated. Any misunderstandings or misrepresentations in this report of the Internet voting system in Norway, Internet voting more broadly, or the complex world of cryptography belong however to the author and The Carter Center.

Thanks too are offered to Isabella Sanchez and Christelle Lorin who provided support as Democracy Program Interns. This study was led by Connie Moon Sehat, assistant director of the Democracy Program, with key input from fellow assistant director Avery Davis-Roberts. David Carroll, director of the Democracy Program, provided oversight for the study.

Connie Moon Sehat wrote this report, which was greatly improved by the feedback and editing from Avery Davis-Roberts, Buster Zalkind, and David Carroll.

Bibliography

Adida, Ben. “Helios: Web-Based Open-Audit Voting.” In *USENIX Security Symposium*, 17:335–348, 2008. https://www.usenix.org/legacy/event/sec08/tech/full_papers/adida/adida.pdf.

Adida, Ben, and C. Andrew Neff. “Ballot Casting Assurance.” In *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*, 7–7, 2006. http://www.usenix.org/event/evt06/tech/full_papers/adida/adida.pdf.

Anderson, Scott A. “The Enforcement Approach to Coercion.” *J. Ethics & Soc. Phil.* 5 (2010): i.

Barrat i Esteve, Jordi, Ben Goldsmith, and Nick Turner. *International Experience with E-Voting: Norwegian E-Vote Project*. IFES, June 2012. http://www.ifes.org/Content/Publications/News-in-Brief/2012/June/~/media/Files/Publications/Reports/2012/EVote_International_Experience_2012.pdf.

Barrat, Jordi, Michel Chevalier, Ben Goldsmith, David Jandura, John Turner, and Rakesh Sharma. “Internet Voting and Individual Verifiability: The Norwegian Return Codes.” In *Electronic Voting*, 35–45, 2012. http://www.e-voting.cc/wp-content/plugins/download-monitor/download.php?id=210.

Benaloh, Josh. “Rethinking Voter Coercion: The Realities Imposed by Technology.” *The USENIX Journal of Election Technology and Systems*, 2013, 82.

Bull, Christian. “Safety First! Verifiability in the Norwegian E-Voting System.” presented at the Seminar on Internet Voting, Oslo, Norway, September 8, 2013.

———. Letter to Connie Moon Sehat. “SV: Timetable/calendar for I-Voting Trials, Esp. July Timeframe,” June 24, 2013.

Carroll, David J., and Avery Davis-Roberts. “The Carter Center and Election Observation: An Obligations-Based Approach for Assessing Elections.” *Election Law Journal* 12, no. 1 (2013): 87–93.

Carter Center. *The Carter Center Handbook on Observing Electronic Voting*. 2nd ed., 2012. https://cartercenter.org/resources/pdfs/peace/democracy/des/Carter-Center-E_voting-Handbook.pdf.

Clark, Jeremy. “Democracy Enhancing Technologies: Toward Deployable and Incoercible E2E Elections.” University of Waterloo, 2011. http://www.uwspace.uwaterloo.ca/handle/10012/5992.

Committee of Ministers - Council of Europe. *Legal, Operational and Technical Standards for E-Voting*. Recommendation Rec(2004)11 adopted by the Committee of Ministers of the Council of Europe on 30 September 2004 and explanatory memorandum. Strasbourg: Council of Europe Publishing, 2005.

“Computer Technologists’ Statement on Internet Voting | Verified Voting.” Accessed October 14, 2013. https://www.verifiedvoting.org/projects/internet-voting-statement/.

Council of Europe Venice Commission (European Commission for Democracy Through Law. *Report on the Compatibility of Remote Voting and Electronic Voting with the Standards of the Council of Europe, Adopted by the Venice Commission at Its 58th Plenary Session (Venice, 12-13 March 2004)*. Study no. 260/2003. Strasbourg: Council of Europe, March 2004. http://www.venice.coe.int/webforms/documents/CDL-AD(2004)012.aspx.

Davis-Roberts, Avery, and David J. Carroll. "Using International Law to Assess Elections." *Democratization* 17, no. 3 (June 2010): 416–441. doi:10.1080/13510341003700253.

"Declaration of Principles for International Election Observation," October 27, 2005.

Dolven, Siri. Follow-up discussion. Interview by Connie Moon Sehat, September 8, 2013.

"E-Voting - The Geneva Internet Voting System." Accessed October 16, 2013. http://www.geneve.ch/evoting/english/presentation_projet.asp.

"Election Observers Find Some Faults." *NewsinEnglish.no*, September 9, 2013. http://www.newsinenglish.no/2013/09/09/election-observers-find-some-faults/.

"Election Standards at The Carter Center | Election Observation Best Practices." Accessed February 1, 2014. http://electionstandards.cartercenter.org/.

"Elections Canada Drops Plan for Online Voting due to Cuts." *CBC News Canada*, May 30, 2013. http://www.cbc.ca/news/politics/elections-canada-drops-plan-for-online-voting-due-to-cuts-1.1346268.

Georgia Tech Cyber Security Team. Interview by Connie Moon Sehat, August 16, 2013.

Goldsmith, Ben. IFES - Internet Voting: Past, Present and Future. Accessed September 7, 2013. http://www.ifes.org/Content/Publications/Interviews/2013/Internet%20Voting%20Past%20Present%20and%20Future.

Halderman, J. Alex. Interview by Connie Moon Sehat, August 21, 2013.

"IFES Election Guide | Elections: Norway Parl Sept 2013." Accessed October 8, 2013. http://www.electionguide.org/election.php?ID=2076.

Institute for Electronics and Electrical Engineers (IEEE). "Chapter 11: Software Quality." In *Guide to the Software Engineering Body of Knowledge*. Accessed October 3, 2013. http://www.computer.org/portal/web/swebok/html/ch11.

Introducing Electronic Voting: Essential Considerations. Policy Paper. International IDEA Resources on Electoral Processes. International IDEA, December 2011. http://www.idea.int/publications/introducing-electronic-voting/upload/PP_e-voting.pdf.

"Judge Upholds Vote-Rigging Claims." *BBC*, April 4, 2005, sec. West Midlands. http://news.bbc.co.uk/2/hi/uk_news/england/west_midlands/4406575.stm.

Karlof, Chris, Naveen Sastry, and David Wagner. "Cryptographic Voting Protocols: A Systems Perspective." In *USENIX Security Symposium*, 12:39, 2005. http://www.usenix.org/event/sec05/tech/full_papers/karlof/karlof.pdf.

Koenig, Reto E. "A Security Flaw in the Verification Code Mechanism of the Norwegian Internet Voting System." presented at the Ministry of Regional of Local Government and Regional Development, Oslo, Norway, September 8, 2013. http://www.regjeringen.no/pages/38377245/4_a_security_flaw_koenig.pdf.

Kommunal- og Regionaldepartementet. "Election Manual: Overview of Election Rules." Ministry of Local Government and Regional Development, Norway, August 26, 2013. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/valgmedarbeidere/Valghandbok/Valghandbok_2013_engelsk.pdf.

———. "How to Vote via the Internet in the Parliamentary Election 2013," September 2013. http://www.regjeringen.no/pages/597658/how_to_vote_internet.pdf.

———. *Regulations Relating to Trial Internet Voting During Advance Voting and Use of Electronic Electoral Rolls at Polling Stations on Election Day During the 2013 Parliamentary Election in Selected Municipalities*, 2013.

———. "Valg 2013 - Stortingsprognose - Grafisk." *Stortingsvalget*, September 9, 2013. http://www.valgresultat.no/bs7g.html.

Ministry of Local Government and Regional Development. "Protection of the Internet Votes." Redaksjonell artikkel, September 6, 2013. http://www.regjeringen.no/en/dep/krd/information-campaigns/election_portal/nytt-om-valg/2013/protection-of-internet-votes.html?id=735145.

Nore, Henrik, and Christian Bull. "An Observable Internet Election." presented at the Seminar on Internet Voting, September 8, 2013. http://www.regjeringen.no/pages/38377245/2_an_observable_internet_election.pdf.

Norris, Pippa. "The Concept of Electoral Integrity." Working Paper for upcoming symposium of Electoral Studies, May 10, 2013. https://dl.dropboxusercontent.com/s/gseod991492m2oq/Pippa%20Norris%20The%20Concept%20of%20Electoral%20Integrity%20Forthcoming%20in%20Electoral%20Studies.pdf?dl=1&token_hash=AAFG7wNSf9zJ3NozTYOyNkvm4nT4UyR6ReuUSAhjvvQMrA.

Norwegian Helsinki Committee, and European Platform for Democratic Elections. *Parliamentary Elections 9 September 2013 Kingdom of Norway Press Release: Fair Elections with Potential for Improvement*, September 10, 2013. http://www.epde.org/tl_files/Newsletter%20Norway/Press%20Release_fair%20el%20with%20potential%20for%20improvement.pdf.

OSCE/ODIHR. *Internet Voting Pilot Project Local Government Elections 12 September 2011: OSCE/ODIHR Election Expert Team Report*. Accessed July 11, 2013. http://www.osce.org/odihr/88577.

———. "Norway - Parliamentary Elections 9 September 2013 - OSCE/ODIHR Election Assessment Mission Final Report," December 16, 2013.

———. *Norway Parliamentary Elections - 9 September 2013 - Needs Assessment Mission Report*. Warsaw, Poland, July 12, 2013.

"Probe Launched into Ballot 'scandal.'" *NewsinEnglish.no*, September 13, 2013. http://www.newsinenglish.no/2013/09/13/probe-launched-into-ballot-scandal/.

Raddum, Håvard. Interview by Connie Moon Sehat, September 9, 2013.

Representation of the People Act (the Election Act). Accessed October 15, 2013. http://www.regjeringen.no/upload/KRD/Kampanjer/valgportal/Regelverk/Representation_of_the_People_Act170609.pdf.

Riise, Marianne, Dolven, and Mjøsund. "Information Session on the Norwegian Electoral System." presented at the Seminar on Internet Voting, September 8, 2013. http://www.regjeringen.no/pages/38377245/1_information_session_election_observers.pdf.

Spycher, Oliver, Melanie Volkamer, and Reto Koenig. "Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting." In *E-Voting and Identity*, edited by Aggelos Kiayias and Helger Lipmaa, 19–35. Lecture Notes in Computer Science 7187. Springer Berlin Heidelberg, 2012. http://link.springer.com/chapter/10.1007/978-3-642-32747-6_2.

State Chancellery, Republic and Canton of Geneva. *Comparison of OSCE Observations and Recommendations with the Genevia Internet Voting Procedures*, March 7, 2012. http://www.ge.ch/evoting/doc/rapports/OSCE_final_report_w_comments_E.pdf.

———. *State Council's Report to the Grand Council on the Geneva Electronic Voting Project*, June 2006. http://www.ge.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf.

Statistik sentralbryå. "Storting Election, Persons Entitled to Vote, 9 September 2013." *Statistik Sentralbryå - Statistics Norway*, September 3, 2013. http://www.ssb.no/en/valg/statistikker/stemmerettst.

Trechsel, Alexander, and Urs Gasser. "Casting Votes on the Internet." *Harvard International Review*, April 17, 2013. http://hir.harvard.edu/the-future-of-democracy/casting-votes-on-the-internet.

Trømborg, Ingrid, Anne Skau, and Marit Hexeberg. Municipality of Frederikstad preparations for I-voting trials and EVA, July 2013.

US Election Assistance Commission. *A Survey of Internet Voting*. Testing and Certification Technical Paper. US Election Assistance Commission. Accessed July 6, 2013. http://www.eac.gov/assets/1/Documents/SIV-FINAL.pdf.

Volkamer, Melanie, Oliver Spycher, and Eric Dubuis. "Measures to Establish Trust in Internet Voting." In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance*, 1–10. ICEGOV '11. New York, NY, USA: ACM, 2011. doi:10.1145/2072069.2072071.

Vollan, Kåre. *Final Verification Report from the Voting Card Printing and the Secure Handling of Cryptographic Keys, Version 0.1 DRAFT*. The Internet Voting Board Representative: Internet Voting Trial 2013, August 26, 2013.

———. *Observing Electronic Voting*. Norwegian Resource Bank for Democracy and Human Right (NORDEM), 2005.

———. "Voting in Uncontrolled Environment and the Secrecy of the Vote." In *Electronic Voting 2006*, edited by Robert Krimmer. Lecture Notes in Informatics. Gesellschaft für Informatik, 2006.

Wagner, David. Letter to Connie Moon Sehat. "Norway Internet Voting System and Election Observation," August 7, 2013.