!"#$%&'!"#$%& ' ())(*+&, -. */"
!"#$%&'(#'$%#)(#'
!"#$%"$#&' (#)"*&+),(# !"#$%&!"#$%&'#()*+,) - ./0)*1#2+.30,4/"

!"#$%&'(#)*!+,#

-./'0123/#405 5%&6#

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.

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:

<9:1/.1=#1(/#->/'19&%1/#%:?#1(/#46;1/5#

Before addressing the

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 […]

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.

<9:1/.1=#)*!G#H%&>2%5/:1%&6#->/'129:;#4:%I;(91#

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] =2)+''(,(%2),%)D%&9.)+4&/+'U)8(,/')(2),6(.)A+A/&1).//)+4.%)H%;28(4)%F)-;&%A/)N/2(8/)H%55(..(%2) <-;&%A/+2)H%55(..(%2)F%&)W/5%8&+8U):6&%;G6)X+D1)8$-(%#*("*#0$*M(H-&#'N')'#C*(A*8$H(#$*2(#'"3* &">*+)$.#%("'.*2(#'"3*/'#0*#0$*B#&">&%>:*(A*#0$*M(9".')*(A*+9%(-$K*=>(-#$>*NC*#0$*2$"'.$*M(HH'::'("*&#* !#:*OP#0*6)$"&%C*B$::'("*Q2$"'.$K*FD1FG*I&%.0*DEERS1)?,;'U)2%E)#Y@C#@@R)<?,&+.J%;&GB)H%;28(4)%F) -;&%A/1)S+&86)#@@T"1)6,,ABCCDDDE0/2(8/E8%/E(2,CD/JF%&5.C'%8;5/2,.CHWXKZW<#@@T"@!#E+.AP[) */2)3%4'.5(,61)=>-?)K)=2,/&2/,)N%,(2GB)I+.,1)I&/./2,)+2')>;,;&/1)+88/../')?/A,/5J/&)\1)#@!R1) 6,,ABCCDDDE(F/.E%&GCH%2,/2,CI;J4(8+,(%2.C=2,/&0(/D.C#@!RC=2,/&2/,]#@N%,(2G]#@I+.,]#@I&/./ 2,]#@+2']#@>;,;&/[)!"#%(>9.'"3*+)$.#%("'.*2(#'"34*+::$"#'&)*M(":'>$%&#'(":1)I%4(8U)I+A/&1) =2,/&2+,(%2+4)=W-Z)M/.%;&8/.)%2)-4/8,%&+4)I&%8/../.)<=2,/&2+,(%2+4)=W-Z1)W/8/5J/&)#@!!"1) 6,,ABCCDDDE('/+E(2,CA;J4(8+,(%2.C(2,&%';8(2GK/4/8,&%2(8KO%,(2GC;A4%+'CII0/KO%,(2GEA'F[)^?) -4/8,(%2)Z..(.,+28/)H%55(..(%21)=*B9%?$C*(A*!"#$%"$#*2(#'"31):/.,(2G)+2')H/&,(F(8+,(%2):/862(8+4) I+A/&)<^?)-4/8,(%2)Z..(.,+28/)H%55(..(%2"1)+88/../')$;4U)Y1)#@!R1) 6,,ABCCDDDE/+8EG%0C+../,.C!CW%8;5/2,.C?=NK>=7ZXEA'F[)H+&,/&)H/2,/&1);0$*M&%#$%*M$"#$%* T&">N((U*("*LN:$%?'"3*+)$.#%("'.*2(#'"3E

[11] Siri Dolven, Follow-up discKup C[)H&,/& 1 Tf[K

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]

- . I >% : %129 : #9B#1 (/ #JK3912 : A#46;1/ 5 !L#

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

1) Voters would be able to gain *e gh f a fficie ecei* – 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).

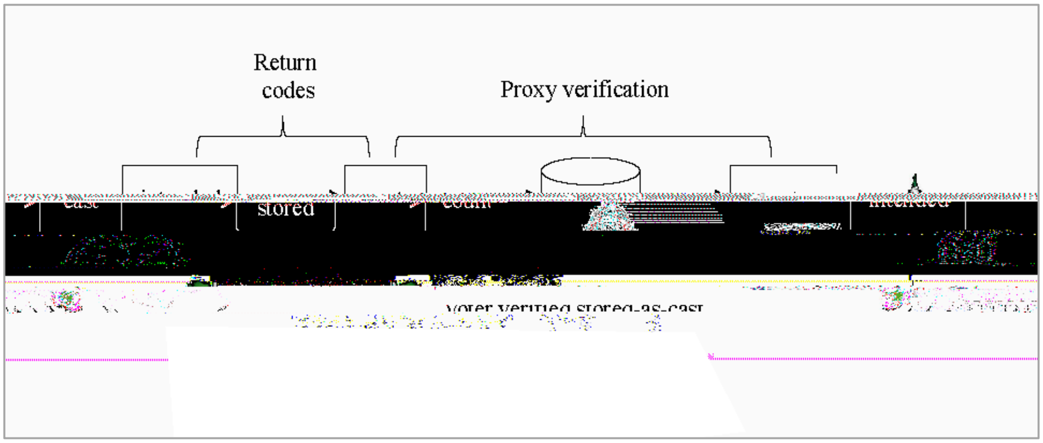

Figure 2 - Verification chain for Internet voting, provided by KRD.[20]

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 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]

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*
24 0 003 (ndi) 0.2(da) 0.2 (t) 0.2 (0.2 (a) 0.24 ET Qq 0.24 4504.2(da) 0.2 (t) 0.2 (0.2 (63.68cm 0 0

To make this work, upon submitting her vote, the voter also received an invitation to participate in additional verification. Although the vote was repository’s files and

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

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.

Zero knowledge proofs are blackwere 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 snctho24 0 0(84) 0.2 2 (n) 80 0 Tm /TT231 Tf [(c) 0.2 4ng

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 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 requirem

observation, the relationship between testing, software development, and verification

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

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 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 increase

U&0;1#2:#%#'95I>/.#D9&>?##

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

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 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.

U(/#S9>/#9B#@8;/&3%129:##

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 *verify.2 (niat) 0.2 (i)]TJ ET Q q 0.24 0 0 0.*
audit, observation, and

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

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

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.

<9:;2?/&%129:;#%:?#&/'955/:?%129:;#

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.

. First and foremost, in order to be observable

software verification, creating confidence in them through education, and encouraging vendors to submit to them are activities in which a variety of election stakeholders

#

7'F:9D›/?A5/:1;#

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,

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*

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.

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