2007

When Personal Computers are Transformed into Ballot Boxes: How Internet Elections in Estonia Comply with the United Nations International Covenant on Civil and Political Rights

Sutton Meagher

Follow this and additional works at: http://digitalcommons.wcl.american.edu/auilr

Part of the Law Commons

Recommended Citation

COMMENTS

WHEN PERSONAL COMPUTERS ARE TRANSFORMED INTO BALLOT BOXES: HOW INTERNET ELECTIONS IN ESTONIA COMPLY WITH THE UNITED NATIONS INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS

SUTTON MEAGHER*

INTRODUCTION...........................................................................................................350
I. BACKGROUND........................................................................................................353
   A. ESTONIAN INTERNET ELECTION VOTING PROCESS ...................356
   B. ESTONIAN ELECTION LAWS .........................................................359
   C. ESTONIAN CRIMINAL LAW PERTAINING TO ELECTIONS ....360
   D. ICCPR REQUIREMENTS FOR ELECTIONS .............................361
      1. Secrecy if the Voting Process .............................................362
      2. Equal Suffrage .................................................................364
      3. Auditability ....................................................................365
II. ANALYSIS ...........................................................................................................366
   A. ESTONIAN INTERNET ELECTIONS COMPLY WITH THE
      ICCPR SECRET BALLOT REQUIREMENT .........................367

* J.D. Candidate, 2008, American University, Washington College of Law; M.A. International Affairs Candidate, 2008, American University, School of International Service; B.A. International Relations and Journalism, 2001, Drake University. First, thank you to my husband John who has been so patient and supportive throughout law school. Thank you to my parents, Michael and Cheryl, and my sister, Whitney, for their love, support, and for encouraging me to get out and see the world beyond Independence. I am also grateful to the staff on the International Law Review, especially Tara Castillo, Robin Murphy, and David McKean, for their thoughtful suggestions, guidance, and hard work during drafting and editing. In addition, a thank you to Kevin Kennedy, who inspired me to delve into the world of election law.
INTRODUCTION

For the citizens of most States, election day entails traveling to a polling place, waiting in line, registering, marking a ballot in a voting
booth, and then placing the marked ballot in a large slotted box. In Estonia, however, voters have exchanged their paper ballots and voting booths for mouse clicks, networked computers, and the comfort of their own homes. In this small Baltic country, the Internet has finally invaded one of the holdouts of an increasingly wired world.

Although several States have conducted pilot Internet elections or requested a report on the subject in the past several years, most States have decided that the possible benefits of holding elections over the Internet do not outweigh the perceived risks. This

3. Cf. Stone, supra note 1, at 955 (contemplating the legal and social obstacles to establishing Internet voting in the United States).
6. See Jeno Szep, Adviser, Ass’n of Cent. & E. Eur. Election Officials, Remarks at the OSCE Supplementary Human Dimension Meeting, in OSCE
conclusion has forced States to abandon their plans to implement Internet voting on a large scale, making Estonia’s Internet voting system an anomaly. As of Spring 2007, Estonia had held two binding elections where voters could cast their ballots over the Internet—the first were local elections held in October 2005 and the second were the Parliamentary elections of March 2007.

ELECTION TECHNOLOGIES REPORT, supra note 4, at 31 (commenting that Internet voting “reflects modern lifestyle”). Internet voting is fast, reliable, and makes voting easier for citizens who are abroad, live far from voting stations, or are disabled. See id.

7. See ROBERT S. DONE, INTERNET VOTING: BRINGING ELECTIONS TO THE DESKTOP 18-22 (2002), available at http://www.businessofgovernment.org/pdfs/Done_Report.pdf (analyzing the technological, legal, and social issues that governments must resolve before implementing Internet voting); John Schwartz, E-voting: Its Day Has Not Come Just Yet, N.Y. TIMES, Nov. 27, 2000, at C1 (reporting on the difficulties faced by the Internet voting company that piloted Internet elections in California). Some computer scientists believe that Internet elections are inherently problematic and that the security issues faced by Internet elections could lead to public distrust of the system, which could in turn “threaten democratic society.” See id.


9. See Wolfgang Drechsler, Dispatch From The Future, WASH. POST, Nov. 5, 2006, at B1 (explaining that Estonia’s accomplishment in becoming the world’s first country to have binding online national elections was rooted in the government’s focus on becoming a leader in Internet-based services). Estonians are known to pay their parking tickets via cell phones and submit their taxes online. See id.

This Comment argues that Internet elections in Estonia comply with the standards set out in the United Nations Covenant on Civil and Political Rights ("ICCPR"). Part I describes three requirements of the ICCPR for elections: secret ballot, equal suffrage, and auditability. Part I also describes the legal framework governing elections in Estonia as well as the country's procedures for Internet voting. Part II demonstrates that Estonia's laws and voting procedures create an Internet elections framework that complies with the requirements of the ICCPR. Part III provides three recommendations. First, the United Nations should create an optional protocol for the ICCPR that provides guidelines for Internet elections. Second, Estonia should amend its election laws and prohibit Internet voting at the work place. Third and finally, the Estonian government should create a list of tasks for observers of its Internet elections. This Comment concludes by suggesting that other States look to Estonia as a model when developing the legal framework for Internet elections.

I. BACKGROUND

Estonia's parliament, the Riigikogu, established a legal framework for Internet voting by passing a set of election laws in 2002 and amendments thereto in 2005. Initially there was some political resistance to the scheme from two political parties in the Riigikogu, both of which opposed the Internet voting provisions because of


concerns that voters would not be able to vote secret ballots, that observers could not audit the Internet election, and that voters could face coercion.\textsuperscript{14} President Arnold Rüütel then refused to promulgate the legislation because he believed that Internet voting was unconstitutional.\textsuperscript{15} President Rüütel was of the view that the possibility to change one’s Internet vote during the period of advanced polling\textsuperscript{16} gave voters an advantage over those that attended traditional polling stations and thus violated the constitutional provision of uniformity in elections.\textsuperscript{17} The Supreme Court of Estonia subsequently reviewed the legislation, held that it was constitutional, and ordered the President to promulgate it.\textsuperscript{18}

Estonia introduced Internet voting in stages. Estonia held its first pilot Internet election in January 2005.\textsuperscript{19} Ten months later, in October 2005, Estonia held municipal elections in the city of Tallinn and gave voters the opportunity to cast ballots over the Internet.\textsuperscript{20}

\footnotesize
\textsuperscript{14} See id. (noting that while different political parties balanced the risks and benefits of Internet voting differently, none registered concerns regarding the fundamental security of the system).

\textsuperscript{15} See id. at 5 (explaining that although the President challenged the legislation in the Estonian Supreme Court, no other legal challenges were made to the Internet voting amendment).

\textsuperscript{16} See Riigikohus [Supreme Court], Judgment of the Constitutional Review Chamber of the Supreme Court, Petition of the President of the Republic to Declare the Local Government Council Election Act Amendment Act, Passed by the Riigikogu on 28 June 2005, Unconstitutional, Constitutional Judgment 3-4-1-13-05, ¶ 2, Sept. 1, 2005 (Est.) (finding that Internet voters have the ability to change their vote an unlimited number of times prior to the close of polls on the day of voting).

\textsuperscript{17} See Eesti Vabariigi Põhiseadus [Constitution] § 156 (Est.) ("[E]lections shall be general, uniform and direct.").

\textsuperscript{18} See Riigikohus [Supreme Court], Judgment of the Constitutional Review Chamber of the Supreme Court, Constitutional Judgment 3-4-1-13-05, ¶¶ 30-32 (balancing the “electoral principles arising from the Constitution” and holding that the ability of Internet voters to change their vote is necessary to guarantee free elections).

\textsuperscript{19} See Thumbs up for Online Voting, COMPUTING, June 2, 2005, at 5 (noting that Estonia’s successful pilot Internet elections led to the use of online voting in the city elections of Tallinn in October 2005).

\textsuperscript{20} See Drechsler, supra note 9, at B1 (examining the success of the October 2005 election in light of the small proportion of voters that used Internet voting); see also Epp Maaten, PowerPoint Presentation, Estonia 2005: The First Practice Of Internet Voting, Meeting to Review Developments in the Field of E-Voting in Strasbourg, F.R.G. (Nov. 23, 2006), available at http://www.coe.int/t/e/integrated_projects/democracy/EVoting/PPT%20MAATEN.ppt (reporting that
Two years after that, Estonia held a national election for Parliament in March 2007, which also included an option for Internet voting.\textsuperscript{21} In a pre-election review of Estonia’s electoral system, the Organization for Security and Co-operation in Europe ("OSCE") concluded that "[t]he legal framework of Estonia overall provides for the conduct of democratic elections."\textsuperscript{22} Although the OSCE is one of the few organizations that has released an official report on the March 2007 election,\textsuperscript{23} media reports were positive about the election and in particular the success of Internet voting.\textsuperscript{24} The OSCE report noted that, while Internet voting appeared to have functioned well during the election, there are still risks to the integrity of the system and the government should improve its auditing efforts.\textsuperscript{25}

Holding Internet elections was a logical step for Estonia. Estonians have integrated the Internet into their lives to such an extent that they even utilize the Internet for routine matters such as personal banking...
transactions. The government has made the implementation of technology a high priority as well. Estonia has thus emerged from its post-Communist economy as a technology powerhouse. Indeed, its preeminence as an Internet pioneer was recently brought to the world spotlight when a large-scale cyber attack forced many of its government and banking websites to shut down.

A. ESTONIAN INTERNET ELECTION VOTING PROCESS

Internet voting is only a supplementary means of voting in Estonia. Other forms of voting are still available for all voters, including voting at polling places, voting early at designated sites, or voting at home. The legislation that provides for online voting contains certain technology requirements, including possession of a computer with access to the Internet, an ID card reader, an ID

26. See The Wired World of E-stonia, NEWSWEEK, Mar. 11, 2002, at 17 (underscoring the fact that almost ninety percent of banking transactions in Estonia take place over the Internet or through special security-enabled cellular phones).

27. See id. at 17 (describing that Estonian lawmakers use specially designed computer programs to amend and comment on proposed legislation, which saves paper and time). Estonia has gone to the extent of posting roadside signs to direct citizens to the nearest Internet locations. Id. One reporter recently considered the Internet in Estonia to be as “vital as running water.” See Mark Landler & John Markoff, Digital Fears Emerge After Data Siege in Estonia, N.Y. TIMES, May 29, 2007, http://www.nytimes.com/2007/05/29/technology/29estonia.html?n=Top/News/World/Countries%20and%20Territories/Estonia.


31. See Riigikogu Election Act, RT I 2002, 57, 355, ch.7 §§ 43(1), 46(1) (providing that a voter may vote at home or at a polling place other than that of their polling division “due to his or her state of health or for another good reason”); see also Local Government Council Election Act, RT I 2002, 36, 220, ch. 7 §§ 49(1), 52(1); Eur. Parl. Election Act, RT I 2003, 4, 22, at ch. 7 §§ 42(1), 45(1).

32. See Borland, supra note 24 (describing that before the March 2007
card, and the appropriate software. Voting takes place on the website of the Estonian National Election Committee ("NEC").

The Estonian government designed the Internet voting procedures to mimic the normal paper ballot voting process used when voters are not voting in their residential district. A voter inserts her marked ballot into a small envelope, which she then places inside a larger envelope bearing her signature. At the end of the election, election officials open the outside envelopes and separate them from the smaller envelopes. This process prevents another party from ever connecting a voter back to their cast ballot, while at the same time providing proof of which voters voted.

The first step in the Internet voting process is for voters to log onto the NEC website, place their ID card in the ID card reader attached to their computer, and log in securely using a Personal Identification Number ("PIN"). Voters then go through the different screens for

---

33. See Madise et al., supra note 12, at 8-10 (maintaining that the ID card is an important part of the design of the Internet election system because it allows for a secure transaction). The security features of the card include a machine-readable code printed on the outside of the card, a microchip containing data regarding the cardholder, and two security certificates. Id. See also Estonian Ministry of Foreign Affairs, E-Estonia, Sept. 20, 2007, http://www.vm.ee/estonia/kat_175/pea_175/1163.html (reporting that as of September 2007, Estonia has distributed over 900,000 ID cards, which includes most eligible voters).

34. See Drechsler, supra note 9, at B1 (reporting that the ID card reader requires software that is complicated to install on personal computers).


36. See Madise et al., supra note 12, at 22.

37. See id. at 22-25.

38. See id.

39. See id. (explaining that this method has been successful in keeping the voter's identity confidential and allowing election officials to properly calculate the votes).

each office and select their candidates. The voting software encrypts the cast ballot to prevent a third party from ascertaining for whom the voter voted. The voters then cast their ballot electronically, after confirming their choices and entering a second PIN. The voter completes the ballot with his digital signature, which is part of the ID card. The use of the digital signature during Internet voting is thus analogous to the voter's signature on the outer envelope in paper ballot voting.

At the end of the election, election officials must count the electronic ballots and add them to the paper ballot tally. In order to accomplish this, the voting software first separates the encrypted ballot from the digital signature of the voter. The separation process ensures that a third party cannot later connect a voter with her cast ballot and it preserves a record indicating which voters cast ballots electronically. At the end of the process, election officials will have

http://www.4qconference.org/liitetiedostot/bp_esitykset/Estonia_B.pdf (providing details about the Internet voting process and showing images of how the process appears on a voter’s computer screen).

41. See generally NATIONAL ELECTION COMMITTEE, supra note 35, at 8-11 (giving an overview of the Internet voting process and a description of the computer components involved in making the system work).

42. See Borland, supra note 24 (describing the way in which the electronic vote is relayed through a series of servers, creating a record of the vote after a voter casts his ballot electronically).

43. See Ina Rottscheidt, Estonia’s E-Lection Voting Begins With Doubts Over Security, DEUTSCHE WELLE, Mar. 4, 2007, http://www.dw-world.de/dw/article/0,2144,2372334,00.html (explaining that the Estonian government also uses the PIN numbers for other secure online activities, including shopping and tax returns).

44. See Epp Maaten, Towards Remote E-Voting: Estonian Case in ELECTRONIC VOTING IN EUROPE: TECHNOLOGY, LAW, POLITICS AND SOCIETY, supra note 8, at 87 (explaining the encryption of voters' ballots and the required digital signature).


46. See NATIONAL ELECTION COMMITTEE, supra note 35, at 14-16 (explaining the process election officials use to tally Internet votes and cancel multiple conflicting votes).

47. See id. at 15 (stating the technical procedure for separating the encrypted ballots from the digital signatures); Schwartz, supra note 8, at C1 (describing the difficulty of auditing ballots while also maintaining their secrecy).

48. See Maaten, supra note 44, at 87 (explaining that voter privacy is protected by two encryption points in the voting process whereby one key encrypts voters' ballots and a second key possessed by the National Electoral Committee decrypts
two separate sets of information—a vote tally and a list of voters who voted electronically.

Election officials next compare the lists of voters who voted electronically and those who voted a normal paper ballot to ensure that no one has voted multiple times. If there are any names that appear on both lists, officials go through a process to delete the vote cast electronically. This process ensures that no voter has the opportunity to cast more than one ballot.

B. ESTONIAN ELECTION LAWS

Estonia has three primary pieces of legislation that govern the conduct of Internet elections: the Riigikogu Election Act, the Local Government Council Election Act, and the European Parliament Election Act (collectively, “Acts”). The Riigikogu amended the Acts to allow Internet voting as a voting option by specifying that Internet voting can take place between the sixth and fourth day prior to election day and that voting can take place at all hours during this time. The Acts require voters to vote on their own behalf and

the ballots). To protect voter privacy, at no time should a single party possess both keys. Id.; see Triinu Mägi, Practical Analysis of E-voting Systems 30 (2007) (unpublished Masters thesis, Tallinn University of Technology), http://triinu.net/e-voting/master%20thesis%20e-voting%20security.pdf (last visited Sept. 22, 2007) (comparing the Estonian Internet voting system with the U.S. pilot Internet voting process—the Secure Electronic Registration and Voting Experiment ("SERVE") and concluding that the Estonian system is more secure, mainly because the Estonian system employs the decryption and encryption method).

49. See Maaten, supra note 44, at 88 (describing how electronic voter lists are sent to the local polling stations making it easy for election officials to determine if any voters voted both at the polling place and over the Internet).

50. See generally NATIONAL ELECTION COMMITTEE, supra note 35, at 14-15 (describing the several steps that take place before votes are cancelled and explaining that the NEC makes the final decisions about canceling votes).

54. See MADISE ET AL., supra note 12, at 13-15 (providing a chronological list of the debates held in the Riigikogu regarding the Internet voting amendments).
specify that only those voters who hold a digital signature certificate may vote electronically.\textsuperscript{56}

The Acts also set out the framework for Internet voting.\textsuperscript{57} The Acts state that a voter must first verify his or her identity using the digital signature on the ID card, then confirm their electoral district, and finally cast their ballot.\textsuperscript{58} The Acts also provide for receipt by the voter of official notification that indicates that they have cast their ballot successfully.\textsuperscript{59}

Estonia's Constitution contains provisions regarding voting as well.\textsuperscript{60} Although the Estonian Constitution does not specifically mention Internet voting, it does state that elections must be "general, uniform and direct."\textsuperscript{61} The Constitution also provides for the secret ballot.\textsuperscript{62}

\textbf{C. ESTONIAN CRIMINAL LAW PERTAINING TO ELECTIONS}

The Estonian Penal Code has a broad set of criminal provisions relating to elections. The Penal Code prohibits interfering with voting and utilizing violence or taking advantage of a relationship to influence how another person votes.\textsuperscript{63} Criminal laws also prohibit anyone from violating the confidentiality of the secret ballot\textsuperscript{64} or

\textsuperscript{56} See Maaten, supra note 44, at 85 (stating that ID cards provide the digital signature for Internet voting and that this is a unique approach to voter identification in Internet elections).
\textsuperscript{60} See EESTI VABARIIGI PÕHISEADUS §§ 57, 60, 156.
\textsuperscript{61} See id. §§ 60, 156.
\textsuperscript{62} See id.
\textsuperscript{64} See id. § 166 (providing punishment by fine or detention for violations of secret ballot procedures).
employing bribery to induce someone to vote, not vote, or vote in a certain way.65

D. ICCPR REQUIREMENTS FOR ELECTIONS

There are no binding international laws governing Internet elections,66 but there are international standards for paper ballot elections.67 The ICCPR is an important standard of this nature, containing specific guidelines and requirements for elections68 that are made binding on States that sign or ratify the ICCPR.69 The United Nations Human Rights Committee ("UN HRC"), which oversees the implementation of the ICCPR, has not made any recommendations on the specific type of voting system that a State should implement, but supports any electoral framework that conforms to the principles contained in the ICCPR.70

65. See id. § 164 (prohibiting bribery with the intention of influencing someone’s vote).
67. E.g., ICCPR, supra note 11.
68. See id. art. 25 (declaring that every citizen shall have the right to vote by secret ballot in genuine elections with universal, equal suffrage and a guarantee of free expression).
1. Secrecy if the Voting Process

ICCPR Article 25 requires that each voter have the opportunity to vote a secret ballot,71 echoing similar principles incorporated into other international standards.72 Two primary reasons support keeping the voting process secret—ensuring that voters are free from undue influence when casting their vote and ensuring the right of voters to cast their ballots in private.73 Almost all democratic States adhere to this principle.74 There are a variety of ways in which States protect the secret ballot. Many States have requirements that voters enter polling booths alone and many States penalize individuals that reveal how a voter voted.75 UN HRC has interpreted Article 25 as imposing

71. ICCPR, supra note 11, art. 25.
72. See Universal Declaration of Human Rights, G.A. Res. 217A, art. 21, ¶ 3, U.N. GAOR, 3d Sess., 1st plen. mtg., U.N. Doc. A/810 (Dec. 12, 1948) (stating that elections “shall be held by secret vote or by equivalent voting procedures.”); Council of Eur., Eur. Comm’n for Democracy Through Law (Venice Commission), Draft Convention on Election Standards, Electoral Rights, and Freedoms art. 11, Doc. No. CDL(2003)57 (Sept. 11, 2003) (declaring that “(1) The rights of citizens to secret voting shall not be restricted or infringed in any way; (2) Elections shall be held by secret voting that ensures free and secret expression of the voter’s will; and (3) Observance of the principle of secret and free voting in the forms established by law means the exclusion of any kind of control whatsoever over the expression of voters’ will, as well as the provision of equal legal conditions for making a free choice between candidates, lists of candidates, or political parties (coalitions”).


74. See, e.g., CARLSON & GISVOLD, supra note 70, at 151 (observing that when the States Parties drafted the ICCPR, the inclusion of the secret ballot requirement did not meet as much opposition as other electoral requirements).

75. See INTERNATIONAL INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE (IDEA), INTERNATIONAL ELECTORAL STANDARDS: GUIDELINES FOR REVIEWING THE LEGAL FRAMEWORK OF ELECTIONS 71 (2002), available at
an affirmative obligation on States to protect voters from such coercion.\footnote{76} Voter coercion or undue influence generally can arise at two different times during the voting process: as the voter is voting and after the voter has cast his ballot.\footnote{77} Voter coercion that transpires as a voter is casting a ballot is unique to voting that takes place outside of the polling place, such as absentee voting or voting over the Internet.\footnote{78} In such a situation, there is a danger that another person might vote someone else’s ballot or make the voter cast their vote in a specific way.\footnote{79} Illicit influencing of voters can also take place when a voter believes that he or she may face consequences for voting a particular way and the voter does not trust that the election officials or voting technology will keep his vote confidential.\footnote{80} In this situation, a voter is likely to succumb to another party’s influence over his voting decision.\footnote{81}

http://www.idea.int/publications/ies/upload/12.%20Balloting.pdf [hereinafter IDEA GUIDELINES] (emphasizing the importance of voter privacy and providing suggestions of how states can comply, such as requiring voters to go into a voting booth by themselves and that no one except a voter should handle their marked ballot until election officials open ballot boxes).

76. See General Comment No. 25, supra note 70, ¶ 20 (explaining that a state’s duty to prevent coercion extends to voters casting absentee ballots); see also ALEX CONTE ET AL., DEFINING CIVIL AND POLITICAL RIGHTS 71 (Ashgate Publishing 2004) (asserting that the ICCPR imposes affirmative obligations on states to allow citizens to exercise the right to vote).

77. NORWEGIAN MINISTRY, supra note 5, at 46 (noting that secrecy serves two important functions: protecting the voter’s privacy as the vote is cast, and preventing any trace between the voter and his or her vote once the ballot has been cast).


79. See WATT, supra note 73, at 13-15 (discussing provisions to deter voter coercion under UK law and analyzing the effectiveness of techniques preventing such coercion under circumstances of in-person, postal, and electronic voting).

80. See Norwegian Ministry, supra note 5, at 46-47 (providing an explanation of the importance of secret suffrage and stating that ensuring ballot secrecy deters buying and selling of votes).

2. Equal Suffrage

Equal suffrage is another requirement of the ICCPR. A basic interpretation of this standard is that each person only has one vote to cast. Another interpretation holds that equal suffrage under Article 25(b) requires that all voters' votes count equally. UN HRC requires that the election procedures and laws of States Parties comply with both interpretations of the equal suffrage principle.

In the context of voting procedures, the presence of multiple methods of casting one's ballot cannot cause one group in society to have an unfair advantage over another group. Voting methods can be particularly difficult to analyze because there are a variety of factors that can make methods unequal—from the amount of time a person has to cast their ballot, to the technology needed to vote, to the ability for a person with a disability to vote. The crucial inquiry, then, is to determine whether the aggregate impact of a particular method of voting disadvantages any particular group. Article 2 of

---

82. See General Comment No. 25, supra note 70, ¶ 21 (noting that a State Party must ensure that its electoral system makes each voter's vote equal to that of other voters).
83. See Pierre Garrone, Fundamental and Political Rights in Electronic Elections, in THE EUROPEAN UNION AND E-VOTING 113 (Alexander H. Trechsel & Fernando Mendez eds., 2005) (explaining that in an Internet election the one-person, one-vote standard is more complex than in normal elections). Because of the need for election officials to audit who voted in an election, a voter cannot be completely anonymous in the process. Id.
84. See CONTE ET AL., supra note 76, at 73 (2004) (reporting that the HRC applied this standard in a complaint where the drawing of electoral boundaries had caused an inequality for voters).
85. See id.
86. See Stacker, supra note 78, at 476, 482-85 (analyzing Internet elections under the United States Voting Rights Act provisions which prohibit dilution of minority votes and electoral processes that might reduce participation in elections and concluding that Internet elections could violate these regulations because of the digital divide, which is used to describe the inequality in technology that exists between different groups in society).
87. IDEA GUIDELINES, supra note 75, at 72-3 (noting that voting procedures should be able to adapt to changes in technology, voting methods, and other population-specific factors, such as physically disabled voters).
88. See CONTE ET AL., supra note 76, at 73 (pointing out that states must also ensure that the method of allocating votes does not limit the right of any particular group to select their representatives in an election).
89. See ICCPR, supra note 11, art. 2.
the ICCPR supports this rationale because it requires that States Parties to the ICCPR ensure that they apply the rights guaranteed in the ICCPR "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status." 90

3. Auditability

ICCPR Article 2591 requires that States Parties' electoral processes have a built-in auditing mechanism.92 With elections based upon the normal paper ballot, observers or independent government agencies usually conduct auditing.93 Observers' tasks can include monitoring the counting of ballots, testing voting equipment, and observing voting at polling stations.94 The role of observers and their reports play an important part in determining if an election has met international standards95 and developing public trust in the election

90. See id.
91. See id. art. 25.
92. See General Comment No. 25, supra note 70, ¶ 20 ("[T]here should be independent scrutiny of the voting and counting process . . . .").
93. See Declaration of Principles for International Election Observation and Code of Conduct for International Election Observers 1 (Oct. 27, 2005), available at http://www.cartercenter.org/documents/2231.pdf [hereinafter Declaration of Principles] (stating that international election observers must be impartial and should judge elections based on both the domestic law of the country in which the election is being held as well as "international principles for genuine democratic elections"). The Declaration of Principles define election observation as "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; the impartial and professional analysis of such information; and the drawing of conclusions about the character of electoral processes based on the highest standards for accuracy of information and impartiality of analysis." See id. at 2, ¶ 4. See also ACE Electoral Knowledge Network, Monitors of Electoral Integrity (Sept. 8, 2006), http://aceproject.org/ace-en/topics/ei/eid/default (listing specific tasks for effective election monitoring, which include assessing the legal framework, the freedom of assembly and movement, the counting of ballots, and whether there are processes in place by which a citizen can submit a complaint about the election).
94. See Declaration of Principles, supra note 93, at 5, ¶ 14 (explaining that election observers should be involved in an election from the pre-election period through the post-election period).
95. See KÅRE VOLLAN, OBSERVING ELECTRONIC VOTING 3 (Norwegian Centre for Human Rights 2005), available at http://www.humanrights.uio.no/forskning/publ/nt/2005/1505.pdf (explaining that a host state can use election
process. Auditability can also include the incorporation of procedures that make the voting process more transparent and allow third parties to verify the voting equipment and vote count.

II. ANALYSIS

Internet elections must adhere to the same requirements of secret ballot, equal suffrage, and auditability that are provided in the ICCPR for normal paper ballot elections. Estonia's Internet elections do not run afoul of ICCPR Article 25 because Estonia's election procedures, electoral laws, and penal code provide a framework that adheres to the principles in the ICCPR as that instrument is interpreted by UN HRC.

As other states move...
forward and create the legal framework for Internet elections they should look to Estonia as a model.\textsuperscript{100}

\textbf{A. ESTONIAN INTERNET ELECTIONS COMPLY WITH THE ICCPR SECRET BALLOT REQUIREMENT}

Estonia is able to comply with the ICCPR secret ballot requirement through a combination of its election laws, penal code, and the design of its Internet voting procedures. Most importantly, the Estonian Constitution and Estonian election Laws create a strong legal framework because they both state that elections must be secret.\textsuperscript{101} Because Internet voting takes place in an environment that election officials do not oversee, there is an increased chance of voter coercion or violation of the secret ballot.\textsuperscript{102} In light of these dangers, the Estonian government has established additional laws and special voting procedures to guarantee that voters will be able to exercise their right to a secret ballot when voting over the Internet.

\textsuperscript{100}\textit{See Needs Assessment Report, supra note 13, at 1 (summarizing the current electoral framework in Estonia and concluding that, “Estonian legislation overall provides a sufficient framework for the conduct of democratic elections...”).}

\textsuperscript{101}\textit{See Eesti Varbariigi Põhiseadus § 60; Riigikogu Election Act, RT I 2002, 57, 355, ch. 1 § 1(2) (“Riigikogu elections shall be free, general, uniform and direct. Voting shall be secret.”); Local Government Council Election Act, RT I 2002, 36, 220, ch. 1 § 1(1) (“The elections of members of local government councils [] shall be free, general, uniform and direct. Voting shall be secret.”); Eur. Parl. Election Act, RT I 2003, 4, 22, ch. 1 § 2(2) (“Elections to the European Parliament shall be free, general, uniform and direct. Voting is secret.”).}

\textsuperscript{102}\textit{See Mieke Loncke & Jos Dusmortier, Online Voting: A Legal Perspective, 18 INT’L REV. L. COMPUTERS & TECH. 59, 63 (2004) (arguing that the only way to fully guarantee that another party is not coercing a voter is to have the voter physically present in the polling station).}
1. Estonian Laws Protect Voters Against Undue Influence or Coercion

Estonian laws provide effective protection against voter coercion with a two-way approach that criminalizes coercion and places a duty on voters to keep their vote secret. The Estonian election laws require that “a voter shall vote himself or herself.” This affirmative duty protects the secrecy of the ballot because it prevents a voter from allowing another person to vote in his or her place. Estonia’s laws also make it a crime to influence or coerce a voter. Although Estonia’s criminal laws do not specifically contemplate coercion in the context of Internet voting, the broad language of the statutes permit the government to enforce the criminal provisions against coercive conduct directed at Internet voters.

2. The Design of the Election Provides Safeguards Against Voter Coercion During Internet Voting

The design of Estonia’s Internet election process fulfills the ICCPR Article 25 secret ballot requirement by ensuring that a third party is not able to trace a voter to his vote. The envelope method used by the Estonian government allows election officials to verify which voters have cast their ballots and makes it impossible for the government or anyone else to connect a voter with her specific vote.
ballot. The Estonian Internet voting system employs two separate encryption keys—one for the voter to encrypt his ballot and another for the election officials to decrypt the ballot. This double-encryption method creates a secure system that protects voter privacy.

3. Voters Can Cancel Their Electronically Cast Ballots by Voting at a Polling Place

The Estonian election laws allow a voter to go to the polling place and recast an electronically cast ballot, which provides a safeguard in the event that another person coerced the voter or hacked into the Internet voting system and manipulated the vote tally. In the event that a voter does recast her ballot at the polling place, the ballot at the

110. See id. (discussing the positive attributes of the envelope method); Remmert, supra note 98, at 15 (describing secrecy requirements for Internet elections). But see Stone, supra note 1, at 979 (proposing another method of ensuring the secret ballot while maintaining the auditability of the Internet voting system). After voters have cast their ballots over the Internet, they would receive numbers corresponding to the order in which they voted. Id. A local newspaper would then print the voter number and the voter’s selection, allowing voters to know that their vote had been properly cast. Id.

111. See Maaten, supra note 44, at 88 (contending that the “envelope method” is simple in its system architecture because it utilizes a limited number of components); Arthur M. Keller et al., Privacy Issues for a Voting System with a Modular Voting Architecture 8-9 (Workshop on Rating Voting Methods, June 8-9, 2006), available at http://vote.cs.gwu.edu/vsrw2006/papers/4.pdf (discussing a prototype of an electronic voting system that could protect a voter’s secret ballot by eliminating any information in the ballot about the timing or sequence of votes cast).


113. Cf. NORWEGIAN MINISTRY, supra note 6, at 9 (recommending that, if Norway were to implement Internet voting, the government should allow voters to vote at a traditional polling place to cancel out an electronically cast ballot, as a procedural safeguard to ensure that the voter casts his ballot without undue influence); Rebekah K. Browder, Comment, Internet Voting with Initiatives and Referendums: Stumbling Towards Direct Democracy, 29 SEATTLE UNIV. L. REV. 485, 486-87 (2005) (listing the benefits of Internet voting, including that Internet voting allows voters to change their votes before the close of the polls on election day).
polling place will cancel out the electronically cast ballot. The Estonian Supreme Court has held that this provision is necessary to bring the Internet election laws into compliance with the Estonian Constitution because it ensures that a voter who has been coerced still has the opportunity to vote a secret ballot.

Allowing voters to cancel out their electronically cast ballots at the polling place is also a safeguard against an outside party influencing the election by hacking into the voting system. Some computer scientists assert that it is impossible to conduct an Internet election that is one hundred percent secure because of the likelihood that hackers will disrupt an election or manipulate votes. While the government of Estonia cannot provide a one hundred percent guarantee against hacking, this vote cancellation safeguard can prevent such hacking from affecting final election results. In the event that authorities find that someone has corrupted the election or that the election officials have lost the electronic results, the

114. See Maaten, supra note 44, at 85 (asserting that the possibility of a revote does not amount to voting twice because the system will only count one vote per voter).

115. See Riigikohus [Supreme Court], Judgment of the Constitutional Review Chamber of the Supreme Court, Constitutional Judgment 3-4-1-13-05, ¶ 30 (finding that the possibility to change one's electronic vote is an “essential supplementary guarantee to the observance of the principle of free elections”); see also MADISE ET AL., supra note 12, app. 2 at 44-45 (reporting on the Estonian President's challenge to the Internet voting Amendment). The Court held that although this provision conflicted with uniformity, it was justified by the need to allow voters to vote without being coerced. Id. at 45. “To those persons who did not vote secretly the possibility to change one's vote gives an essential remedy for restoring the secrecy of voting.” Id.

116. See CAL. TASK FORCE, supra note 5, app. A at 37-38 (recommending that Internet voting end before election day to prevent possible technical problems from disenfranchising voters).

117. See, e.g., DAVID JEFFERSON ET AL., A SECURITY ANALYSIS OF THE SECURE ELECTRONIC REGISTRATION AND VOTING EXPERIMENT (SERVE) 3 (2004), app. D, at 32-33, available at http://www.servesecurityreport.org/paper.pdf (concluding that a secure election over the Internet could not be conducted due to the structure of the Internet itself and the current design of personal computers). This evaluation was conducted by a panel of computer scientists with an expertise in election security for the U.S. Department of Defense’s Federal Voting Assistance Program (FVAP) Voting Over the Internet Pilot. Id.

118. Cf. supra note 29 and accompanying text (discussing alleged “cyber attacks” on Estonian websites by agencies of the Russian government).
government can instruct voters to recast their votes at a normal polling site.\textsuperscript{119}

B. ESTONIAN INTERNET ELECTIONS COMPLY WITH THE ICCPR STANDARD OF EQUAL SUFFRAGE

The notion of equal suffrage contained in ICCPR Article 25(b) has a dual meaning. It means that each voter should vote only once and that each such vote should be weighed equally as against all other votes.\textsuperscript{120} To comply with ICCPR Article 25(b), a government must ensure that its electoral procedures comply with both aspects of equal suffrage.\textsuperscript{121} Where a state provides voting via the Internet as an option, compliance with the latter aspect of the equal suffrage principle becomes more difficult. Because the basic purpose of providing the option to vote via the Internet is to encourage voter participation by making voting more convenient, the opportunity to vote via the Internet comes into conflict with the principle that all voters must have an equivalent opportunity to cast their ballot.\textsuperscript{122}

Some observers argue that Internet voting frustrates equal suffrage because it provides voters who have Internet access with twenty-four hour access to voting, while voters who must vote at the polling station have a limited window in which they can cast their ballot. Critics also argue that the technology required to vote over the Internet, such as a computer, telecommunications services, and

\begin{footnotesize}
\textsuperscript{119} See Needs Assessment Report, supra note 13, at 7 (stating that the NEC has the power to nullify electronic election results, but also noting that there are no specific criteria for this process). But see Jefferson et al., supra note 117, at 11-12 (hypothesizing that many cyber-attacks can take place without the knowledge of election officials).

\textsuperscript{120} See Garrone, supra note 83, at 112-13 (discussing the content of the principle of equal suffrage under ICCPR Article 25(b)).

\textsuperscript{121} See Lilian Mitrou et al., Revisiting Legal and Regulatory Requirements for Secure E-Voting, in Security in the Information Society: Visions and Perspectives 469, 475 (Ghonaimy et al. eds., 2002) (discussing the standards for Internet elections and stating that equal suffrage includes both the one person, one vote standard, as well as an equal opportunity for all voters to cast their ballot).

\textsuperscript{122} See Kimberly C. Delk, Comment, What Will it Take to Produce Greater American Voter Participation? Does Anyone Really Know?, 2 Loy. J. Pub. Int. Law 133, 168-70 (2001) (describing the backlash in the United States when states introduced Internet voting, because critics believed that allowing Internet voting would put minority voters at a disadvantage because they did not have the same level of accessibility to computers as predominately white voters).
\end{footnotesize}
special government issued ID cards, is costly and can be difficult to obtain. Some computer scientists also argue that a poorly designed voting system would allow someone to hack into the system and change the vote tallies or allow hackers to vote multiple times. Estonia has developed an Internet voting regime that simultaneously addresses the experts' security concerns and observes the equal suffrage standard of ICCPR Article 25(b).

1. The Design of the Internet Election System Prevents Someone from Voting More than One Time

The technical design of Estonia's Internet election system and counting procedures ensure that Estonia's Internet elections do not violate the ICCPR equal suffrage standard. In an election where voters only vote on a paper ballot at the polling place on election day, it is not difficult for election officials to ensure the one person one vote standard by monitoring the voting process. In this type of election there is usually a registration process that keeps track of which voters have already cast ballots. After the voting has taken place, election officials then compare the number of voters to the number of ballots to ensure that there are an equal number of cast ballots and voters. In an Internet election, where voters are

123. See Norwegian Ministry, supra note 5, at 19-20 (discussing some of the inequalities that Internet voting might create, such as a reluctance to vote on the part of voters who are less competent in their use of the Internet).
124. See DoD E-Voting Assessment, supra note 81, at 4-31 to 4-33 (concluding that the U.S. Dept. of Defense should not implement Internet voting because of the many security risks involved in Internet voting, including computer attacks and vote manipulation).
125. See General Comment No. 25, supra note 70, ¶ 20 (explaining that ICCPR Art. 25(b) requires an independent electoral authority to supervise the electoral process); Loncke & Dusmortier, supra note 102, at 63 (stating that existing technology does not permit an electronic voting system to verify voter identity with 100 percent accuracy); Larson, supra note 125, at 1806 (explaining that attendance at a polling station, rather than voting online, allows an election official to verify the voter’s identity in person).
126. See, e.g., ACE Electoral Knowledge Network, Overview of Voter Registration (Sept. 8, 2006), http://aceproject.org/ace-en/topics/vr/vr10 (providing a summary of the voter registration process and some of the goals of the process, including ensuring that each citizen only votes one time).
completing the voting process through a website, complying with this standard can be more complicated because there is no election official physically present when a person casts a ballot and because there is no physical ballot to use during a recount.\textsuperscript{128}

In Estonia, only voters holding ID cards may vote over the Internet.\textsuperscript{129} This requirement creates documentation regarding the names of eligible voters and adds a layer of security because it restricts the number of people having access to the voting system to eligible, ID card-carrying voters.\textsuperscript{130} This requirement is not discriminatory because the government requires all Estonian citizens to obtain the card and, to date, most eligible voters have obtained the card.\textsuperscript{131}

Estonian election procedures require that election officials compare the list of voters who voted online with a list of voters who voted at the polling place prior to initiating the vote tally at the end

---

\textsuperscript{128} See CALTECH/MIT REPORT, supra note 95, at 10 (maintaining that any voting that takes place outside the polling place, such as absentee voting, carries a strong chance of voter fraud). But see Bryan Mercurio, Democracy in Decline: Can Internet Voting Save the Electoral Process?, 22 J. MARSHALL J. COMPUTER & INFO. L. 409, 439-40 (2004) (arguing that voting over the Internet reduces the occurrence of illegally voting more than once by requiring voter identification when voters log into a website).

\textsuperscript{129} See Riigikogu Election Act, RT I 2002, 57, 355, ch. 7 § 44; Local Government Council Election Act, RT I 2002, 36, 220, ch. 7 § 50; Eur. Parl. Election Act, RT I 2003, 4, 22, ch. 7 § 43. But see République et Canton de Genève, supra note 4 (explaining that the Geneva voting system does not require the connection of any peripheral components to the voter’s personal computer). The state mails voters a voting card that has a personal identification number that the voter uses to identify herself when she casts a ballot online. Id.

\textsuperscript{130} See République et Canton de Genève, supra note 4 (describing the process of encoding a unique picture into the ballot through a voter’s ID to provide additional protection).

\textsuperscript{130} See Maaten, supra note 44, at 85 (describing how the ID cards limit who may access the system to only those eligible to vote).

\textsuperscript{131} See id. (reporting on the many different transactions in which Estonians can use their ID cards and that Estonian law identifies the ID card as a legal means of identification in transactions over the Internet).
of an election.\textsuperscript{132} If one individual appears on both lists, the officials cancel the electronic vote to prevent anyone from voting twice.\textsuperscript{133} Although voters may change their vote as many times as they wish, the system prevents multiple votes.\textsuperscript{134}

2. Citizens Voting over the Internet Do Not Have an Advantage over Voters Voting a Paper Ballot

Estonia complies with the second equal suffrage component of the ICCPR Article 25(b) standard because voters in Estonia who utilize the Internet to cast their ballot do not have a substantial advantage over voters who vote using a paper ballot.\textsuperscript{135} Some experts argue that the ability to vote with a home computer makes the voting process inherently more accessible and gives those voters who vote electronically a longer time period in which to cast their ballot.\textsuperscript{136} Critics also assert that the Internet voting option is an unfair advantage because Internet voters have the opportunity to re-vote later at a polling site, while voters attending a normal polling place only have one chance to make their voting decision.\textsuperscript{137} Additionally, experts argue that Internet voting is unequal when there is a “digital

\begin{itemize}
    \item \textsuperscript{132} See National Election Committee, \textit{supra} note 35, at 7 (describing the procedures in place for electronically sorting cast ballots and then canceling out the duplicate ballot if the voter also voted at the polling place).
    \item \textsuperscript{133} See \textit{id}.
    \item \textsuperscript{134} See Maaten, \textit{supra} note 44, at 86 (explaining that one of the important principles of Internet voting is the opportunity for voters to recast their ballot, and, because the system will only register one vote per voter, this does not constitute voting multiple times).
    \item \textsuperscript{135} See Garrone, \textit{supra} note 83, at 114 (noting that because Internet voting adds an additional manner in which voters can cast their ballots, governments must ensure electronic voting is accessible to voters in practical terms as well as in terms of the voters' capacity to understand and utilize the method provided).
    \item \textsuperscript{136} See \textit{id}. (reasoning that to ensure equality, governments should offer voters the opportunity to cast their ballots electronically in public spaces so as not to discriminate against voters who do not have access to a computer at their home or work).
    \item \textsuperscript{137} See Loncke \& Dusmortier, \textit{supra} note 102, at 59, 62 (recommending that governments adopting the Internet voting option should equalize access by extending the time period for voting for all voting methods and placing remote voting terminals in public places such as libraries, grocery stores, and post offices).
\end{itemize}
divide”¹³⁸ in society, which occurs when certain demographics do not have equal access to the technology needed to vote electronically.¹³⁹ To compound the problem, a “digital divide” could also violate ICCPR Article 2, which requires States Parties to the ICCPR to administer the requirements of the ICCPR non-discriminatorily.¹⁴⁰

Estonia’s Internet elections withstand these criticisms. In Estonia, the opportunity to vote over the Internet is restricted to the fourth through the sixth day before the election.¹⁴¹ Because voters may still go to early voting sites and vote during this time, voting over the Internet does not offer Internet voters a special time advantage.¹⁴²

¹³⁹. See id. (providing statistics illustrating the difference between socio-economic and racial groups’ access to Internet technology in the United States); Larson, supra note 116, at 1814-15 (summarizing a case brought in United States District Court against the Arizona Democratic Party when it held its primary over the Internet). The Voting Integrity Project, along with an African-American man and a Hispanic woman, brought the lawsuit asserting that the election was discriminatory under the Voting Rights Act of 1965, claiming that all citizens did not have equal access to the Internet. Id.; see KEVIN COLEMAN, CONGRESSIONAL RESEARCH SERVICES, INTERNET VOTING 5-6 (2003) (reporting that the District Court decided not to grant the injunction that the Voting Integrity Project had sought).
¹⁴⁰. See ICCPR, supra note 11, art. 2 (prohibiting states from discriminating due to “race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status”). But see John T. Nockleby, Why Internet Voting, 34 LOY. L. REV. 1023, 1025-26 (reasoning that Internet voting might enhance political equality because it would eliminate obstacles for certain groups that have difficulty in getting to a polling place on election day, such as the elderly and disabled).
¹⁴¹. See Local Government Council Election Act, RT I 2002, 36, 220, ch. 7 § 44 (detailing the two time periods for advance electronic and non-electronic voting).
¹⁴². See Riigikohus [Supreme Court], Judgment of the Constitutional Review Chamber of the Supreme Court, Constitutional Judgment 3-4-1-13-05, ¶¶ 22-24 (holding that the actual inequality of individuals in terms of personal access to the Internet does not constitute inequality in the sense of the Estonian constitutional principle of equal treatment because the Estonian government has enacted legislation that enables all individuals to use Internet voting). But see Nadja Braun, E-Voting: Switzerland’s Projects and Their Legal Framework – In a European Context, in ELECTRONIC VOTING IN EUROPE: TECHNOLOGY, LAW, POLITICS AND SOCIETY, supra note 8, at 43, 47 (stating that Geneva’s experimental Internet voting system permits voting as early as three weeks prior to the election and ends the day before the election closes).
The availability of computers with the ID card-reader in multiple public places allows individuals who do not have a computer at home to take advantage of this voting option. Moreover, the "digital divide" in Estonia is not as great as in other states. The government of Estonia has made it a priority to promote access to the Internet and it has one of the highest rates of Internet access of any former Soviet Republic.

C. ESTONIAN INTERNET ELECTIONS COMPLY WITH THE ICCPR STANDARD OF AUDITABILITY

The government of Estonia developed the Internet voting system to be as straightforward and transparent as possible. The system’s auditing capacity permits verification of voting data by a third party and thus facilitates this transparency and contributes to voter confidence. Taken together, these factors demonstrate that Estonia’s Internet voting system complies with the election auditability requirement of ICCPR Article 25.

Auditing Internet elections can be particularly difficult because the technology used is not readily accessible to election observers. This is a consequence of the logistics of the Internet voting system,
WHEREBY THE VOTERS' HOME COMPUTERS AND THE CENTRAL SERVERS THAT COLLECT THE VOTING DATA ARE DISPERSED THROUGHOUT THE COUNTRY. \(148\) Compounding the problem of election observation is the fact that the Internet voting process itself takes place in a variety of environments, where observers are unable to monitor the voter's polling experience. \(149\) It is thus exceedingly difficult for a single election observer to oversee simultaneously the process of voting, where coercion may occur, and the process of vote collection, where fraud may occur. \(150\)

1. Estonia Has Made the Software that Drives Its Election Systems Available to the Public, Facilitating Auditing of the Internet Voting Process

One of the most important technological components in an Internet election is the software that counts and stores the votes. \(151\) The software used in the Estonian Internet election is Linux-based,

---

148. See generally id. at 9-10 (discussing Internet voting system architecture).
149. See NORWEGIAN MINISTRY, supra note 5, at 22 (explaining two different types of voting, one where voters are in a controlled environment and the other where the voters are in an uncontrolled environment, and noting that Internet voting is part of the latter category).
150. Cf. LAWRENCE NORDEN ET AL., POST-ELECTION AUDITS: RESTORING TRUST IN ELECTIONS 31 (2007) (comparing the election audit provisions of various states in the United States). Norden points out that New York law permits a single party to appoint an observer to oversee polling stations as well as an observer to oversee the selection of polling machines for audit. See id. See generally ACE Electoral Knowledge Network, Guiding Principles of Vote Counting, http://aceproject.org/ace-en/topics/vr/vr10 (last visited Mar. 1, 2007) (outlining some of the standards for vote counting and noting that if votes are counted electronically it is important to have an independent audit of the counting process).
151. See Jay Lyman, Canada Marks First Internet Election in North America, TECHNEWSWORLD, Oct. 11, 2003, http://www.technewsworld.com/story/32098.html (discussing the debate about the security of the various types of software that could be used to support Internet voting); Jay Lyman, OPEN SOURCE ELECTION SYSTEMS DESIRABLE, UNAVAILABLE, NEWSFORGE, THE ONLINE NEWSPAPER FOR LINUX AND OPEN SOURCE, Mar. 6, 2006, http://trends.newsforge.com/article.pl?sid=06/02/28/1648218&tid=136 (suggesting that the use in an election of software containing privately owned code leads to a lack of trust and transparency). However, some experts maintain that the ownership of the underlying rights to the voting software is less important than the ability to inspect the source code, as the software may be provided for inspection regardless of who holds the intellectual property rights. See id.
which has a source code that is open to the public. Open source software makes it easier for the public and observers to access the software and check for vulnerabilities. Supporters of election reform have also lauded open-source software because it increases transparency in the voting process and makes independent testing of the election software straightforward.

Before Estonia held its 2005 election, the NEC tested the electoral system and an independent outside expert reviewed the source code. Although this was not an entirely open process, it still provided a level of security to ensure that the software was going

---

152. See Election Mission Report, supra note 23, at 11-12 (detailing the technical specifications of the various components of Estonia's Internet voting system and the type of software that each component utilizes); Sean Dunne, Case Study: Information Technology: Elections and Technology, in Electoral Management Design: The International IDEA Handbook 240, 243, 246 (International Institute for Democracy and Electoral Assistance 2006), available at http://www.idea.int/publications/emd/upload/EMD_inlay_final.pdf (recommending that to ensure security in an Internet election, governments should have ownership of the code on which the election software is based); Watt, supra note 73, at 18, 32-33 (noting that an additional benefit to using open-source code is that in the event a technology supplier is no longer able to provide the government with equipment, the government would be able to have the equipment manufactured by another company).

153. See Caltech/MIT Report, supra note 95, at 46-47 (listing recommendations for electronic voting, including that all vote counting and recording software should be open source and non-proprietary); Editorial, Making Democracy Credible, N.Y. Times, Feb. 9, 2007, at A18 (reporting that trust in the voting system in the United States is undermined when private companies maintain the secrecy of software code used in the counting of electronic ballots).


155. See Needs Assessment Report, supra note 13, at 3-4 (describing the role of the NEC as a non-partisan professional group that administers elections in Estonia).

156. See id. at 6 (describing the steps that the NEC has taken to develop and test the Internet voting system). The OSCE Mission noted that the NEC has not conducted additional testing, however, and the system itself is not subject to any certification requirements. See id.

157. See id. (noting that the NEC hired an outside expert to review the system source code).
to work properly. Before the March 2007 election, the Estonian government hired an outside consulting company to audit Estonia's voting technology and the auditors found no problems. Additionally, one computer expert has noted that Estonia's small population may detract hackers from attempting to foil an election in the country because hackers usually focus on events that will affect many people, giving them more notoriety.

2. Estonia’s Voting Procedures Require Auditing of the Internet Election Process

Election observers in Estonia have the opportunity to review the source code and the architecture of the electoral system, which is essential for a thorough audit of an election with Internet voting. In Internet elections, observers still have the same goals as they do in a paper ballot election, but their specific duties are different. Observers likely will need technical expertise to identify flaws in an Internet election.

158. See Loncke & Dusmortier, supra note 102, at 66-67 (acknowledging that making source code available to citizens would increase voter confidence, but also makes the election system more vulnerable to hackers). Loncke and Dusmortier suggest that a compromise solution would be to have the open source code only available to a certain group of experts or the electoral administration body. Id.

159. See Borland, supra note 24 (reporting that the multinational auditing firm KPMG completed a review of the Internet voting technology and that observers from political parties observed the auditing).


161. See NEEDS ASSESSMENT REPORT, supra note 13, at 6 (reporting that the NEC made all aspects of the election system open to political parties and observers and that a training for these groups was slated for February 12, 2007, prior to the 2007 Parliamentary elections). The goal of the training is to familiarize observers with procedures such as installing the software, testing the electronic tallying software, transporting the servers, and generating the encryption keys. Id.

162. See Szep, supra note 6, at 33 (noting that the primary difference for observers of Internet elections is that while they are unable to conduct on-the-spot inspections of the system software, they are still able to inspect items such as system certificates and system architecture to ensure that the domestic electoral authorities have met national and international standards).

Estonia’s process enables observers to view the entire election process. Before the 2005 elections, the Estonian government invited political parties and other interested organizations to a training on observing Internet elections. The OSCE did not note any problems with access to viewing election procedures in its assessment of Estonia’s March 4, 2007 Parliamentary elections.

III. RECOMMENDATIONS

Despite their success, Estonia’s elections remain an experiment in a relatively new field. The Estonian government should thus continually improve its Internet voting system. It appears that electronic voting is going to become a voting option in many states in the coming years in spite of the absence of widely recognized international guidelines for Internet elections. The international community should respond to this need and develop a set of standards for Internet elections. Additionally, at the national level, Estonia’s government should strengthen its laws and procedures available at http://www.e-voting.cc/files/Working-Paper-1-2006/ (providing an overview of observers’ tasks during elections that employ internet voting). The observer should ensure that the system prevents unauthorized access to the server that records votes and encrypts voters’ data. Id. But see VOLLAN, supra note 95, at 16 (cautioning against any technical assessment by observers that the public might construe as certification of the voting equipment, which should not be the responsibility of the observers, but rather the government and electoral management body).

164. See MADISE ET AL., supra note 12, at 21 (explaining that the participants were introduced to the required documentation for Internet voting during the training). The Estonian government also offered foreign officials the opportunity to observe the Internet voting in two different cities. Id. at 21-22.

165. See NEEDS ASSESSMENT REPORT, supra note 13, at 6 (noting that few Estonian political parties focused their efforts on election observation missions despite the fact that the NEC permitted interested parties to observe implementation of the new Internet voting systems).

166. See Shari Claire Lewis, Internet Voting: Validity, Safety Issues Must Be Addressed to Reach Full Potential, 236 N.Y. L.J. 5, 5-6 (Aug. 1, 2006) (describing the New York Firefighters Union’s use of online voting for election of union officials and a thwarted plan to offer online voting to members of the military stationed abroad). But see Operational and Technical Standards for E-Voting, supra note 66, at 23-29 (suggesting standards for Internet voting for European Union ("EU") Member States and calling on EU Member States to conduct evaluations of their procedures for Internet voting and report their findings to the Council of Europe).
pertaining to the ICCPR requirements of auditability and equal suffrage. By addressing these concerns, Estonia will become an even better model for states that are implementing Internet elections.

A. THE UNITED NATIONS SHOULD CREATE AN OPTIONAL PROTOCOL TO THE ICCPR THAT SETS OUT GUIDELINES FOR CONDUCTING INTERNET ELECTIONS

As states venture into the new territory of Internet elections, it will become increasingly more important for the international community to establish procedural and technical standards for Internet elections.167 The creation of an ICCPR Optional Protocol containing standards for Internet voting could resolve this problem.168 An Optional Protocol would be an effective solution because the ICCPR is already one of the most widely recognized guidelines for elections.169 An Optional Protocol would assist election observers and governments by outlining criteria with which a state must abide.170 Additionally, this would assist states interested in implementing Internet elections by allowing them to know what the standards are as they develop a new system.171


170. See ELECTION MISSION REPORT, supra note 23, at 10 (recommending that the Riigikogu codify further regulations on the security requirements for Internet elections).

171. See Colin B. Picker, A View from 40,000 Feet: International Law and the Invisible Hand of Technology, 23 CARDOZO L. REV. 149, 184-86 (2001) (arguing that any international standards that are created to govern the use of technology must be inherently flexible because the fast changing nature of technology could well conflict with the slow pace at which international law ordinarily evolves).
The Optional Protocol should create an advisory body of computer scientists that will evaluate the technological systems proposed by states. The scientists could use the factors set out in the protocol to make their decisions. Having an independent body evaluate election technology will increase trust in Internet voting systems and could allay the public's fears that a government might misuse the voting technology, which is under the government's control, to manipulate elections in favor of particular constituencies.

The Optional Protocol could also facilitate the prosecution of election-related cyber crimes. Because it is not geographically delimited, the Internet has created jurisdictional complications in many areas of criminal law. Even where a state has enacted criminal statutes with respect to certain conduct, such as voter coercion or election fraud, such statutes can be impossible to enforce when the perpetrator or the conduct are located in another jurisdiction. An international instrument that facilitates cross-border prosecution of such activity will greatly lessen incentives for the commission of cyber-crime and disruption of elections.

172. See CALTECH/MIT REPORT, supra note 95, at 47 (recommending that the United States create a national commission of information security experts to develop voting equipment software); Picker, supra note 189, at 185-86 (recommending that one way for international law to keep up with fast changing technology is for an international organization to oversee the rules).


174. See Stephan Wilske & Teresa Schiller, International Jurisdiction in Cyberspace: Which States May Regulate the Internet, 50 FED. COMM. L.J. 117, 119-25 (1997) (describing the evolution of the regulation of the Internet and an analysis of the different means under international law that states have tried to use when persecuting international crimes).

175. See id.

176. See Ryan P. Wallace et al., Computer Crimes, 42 AM. CRIM. L. REV. 223, 272-74 (Spring 2005) (asserting that cyber-crime is difficult for states to prosecute because the Internet does not have a geographic boundary and recommending that the international community create a functional international legal framework to deter cross-border criminal conduct).
B. ESTONIA SHOULD ENACT SUPPLEMENTARY LEGISLATION THAT PROHIBITS VOTING AT WORK TO BOLSTER ITS ELECTION SYSTEM’S COMPLIANCE WITH THE ICCPR

Estonia should place restrictions on the locations from which voters may cast online ballots. Such restrictions would enhance the secret ballot element of the Internet voting system and reinforce the secret ballot standards of the ICCPR. Because many of the fears of undue influence often involve voting that might occur in a voter’s workplace, Estonia should make it a crime to vote at work and also require employers to block the NEC website from workplace computers.

The workplace is one of the places where a voter could easily face intimidation. By forcing voters to use a personal or public computer instead of a company computer, there is less likelihood that an employer could find out how a voter voted and therefore less chance of retaliation. Other states have acknowledged the special potential for coercion that exists in the employer-employee relationship in the context of voting and have enacted legislation to protect voters. Estonia should do the same.

177. See ICCPR, supra note 11, art. 25.
179. See Loncke & Dusmortier, supra note 102, at 64-65 (arguing that the only way to guarantee against coercion of voters is to have voting take place in a controlled environment such as a polling place, and that Internet voting outside of such controlled environments should be regulated by laws that deal with the potentiality of coercion). Cf. NORWEGIAN MINISTRY, supra note 5, at 91 (acknowledging that when voting takes place in uncontrolled environments outside the polling place, it is difficult to ensure that the transaction will be secure).
180. See CAL. TASK FORCE, supra note 5, at 40 (recommending that California consider amendments to election laws to penalize employers who monitor or intimidate their employees' online voting in the workplace). Cf. Mercurio, supra note 128, at 434-35 (analogizing the potential for voter coercion in Internet voting with similar opportunities for coercion in absentee balloting).
181. See, e.g., 42 U.S.C. § 1973aa-6 (1982) (providing that a voter's employer, agents of a voter's employer, and agents of the voter's labor union are prohibited from providing assistance to a voter in the voting booth—other parties may provide assistance to the voter upon the voter's request).
C. THE NEC SHOULD CREATE A PROCEDURE FOR ELECTION OBSERVERS AT INTERNET ELECTIONS TO FACILITATE AUDITING

Observers are an integral part of the election process. They help to ensure the integrity of the voting process and instill public trust in the election results. Creating a uniform list of procedures for observers will make the electoral system more transparent and will permit Estonia to maintain uniform records of its elections. These procedures could take several different forms, such as a checklist of inquiries observers should make during their observation mission. Such a list of procedures will also facilitate independent auditing of the election because it will enable the observers to generate a coherent data set that later can be examined to assess the quality of the election system in various regions. Clearly, observation procedures that are tailored to a state’s unique political and electoral environment are much more effective than generic procedures.

The Estonian National Elections Commission could structure the checklist in several ways. One way would be to list the different steps in the Internet voting process, with corresponding questions for

182. See supra notes 93-97 and accompanying text (discussing the importance of election observation and the manner in which it reinforces the auditability of an election).
183. See id.
184. See VOLLAN, supra note 95, at 3-4 (noting the important role observers must play in ensuring accurate and trustworthy electronic elections, especially in transitioning countries where the electorate already generally distrusts the government).
185. See, e.g., Verified Voting Foundation, Local Election Administration Voting Technology Full Questionnaire (Aug. 3, 2004), http://www.verifiedvotingfoundation.org/article.php?id=6151 (directing observers of elections utilizing technology to analyze issues such as the testing of the equipment, information about the vendors of the equipment, and the accessibility of the equipment).
186. See ELECTION MISSION REPORT, supra note 23, at 1, 10, 16 (recommending that the election software be subject to a more comprehensive security audit, that an independent body conduct the audit in accordance with published benchmarks, and that the final audit reports be publicly available).
187. See INSTITUTE FOR DEMOCRACY AND ELECTORAL ASSISTANCE, THE FUTURE OF INTERNATIONAL ELECTORAL OBSERVATION: LESSONS LEARNED AND RECOMMENDATIONS: CONFERENCE REPORT 12 (1999) (cautioning that observation questionnaires that are not tailored to the particular country where the observer is monitoring can cause confusion and lead to an inaccurate assessment of the election).
each period, while another way might involve listing primary areas of concern with respect to Estonia’s Internet voting regime, with corresponding inquiries that the observer would be instructed to make during the mission. The list below employs the latter method, focusing on two main areas: assessing the laws and procedures in place to govern Internet elections and assessing voters’ perceptions of the election itself.

Proper inquiries for the observer regarding the laws and procedures governing Internet elections might include:

- Have the National Election Commission (NEC) and local election officials complied with the required procedure for counting ballots?

- Has the NEC made the election software code available for review, if not to the public at least to political parties and experts?

- Do procedures exist for the testing of election technology by a third party? If there are such procedures, has auditing taken place?

Proper inquiries to make of voters might include:

- How much trust do you have in the NEC?

- Do you know of any segments of the population that election officials have discriminated against, or who have difficulty voting?

---


189. Cf. id. ann. B at 86-88 (giving an example of an election observer’s checklist organized by steps in the electoral process).

190. Cf. id. at 61-64 (describing the necessary aspects of a legitimate counting procedure in traditional elections).

191. Cf. id. at 37-45 (emphasizing the importance of impartiality and openness in election administration meetings).

192. Cf. id. at 43 (recommending that the OSCE review the ballot printing and security procedures prior to the administration of a traditional election).

193. Cf. id. at 56 (suggesting that election observers assess voters' confidence in the election).
Did you find it easy to vote via the Internet? If not, was sufficient assistance available to you when you encountered difficulties?195

CONCLUSION

While many states are interested in implementing voting over the Internet,196 Estonia is one of the first states to make Internet voting possible on a large scale in a binding election.197 As technology changes in elections, states should still adhere to the ICCPR because the principles contained therein continue to provide a solid foundation for the dual values of equal suffrage in the context of voting via the internet. Estonian legislation and the design of its Internet voting system succeeds in maintaining compliance with the basic principles of the ICCPR. As more states begin to augment their electoral systems with the Internet voting option, Estonia's model should serve as a guiding light.198

194. Cf. id. at 41-42 ( recommending that observers note where discrimination is apparent in the voter registration process).
195. Cf. id. at 56 (directing an election observer to discuss a voter's impression of the secrecy of his or her ballot when doubt regarding the confidentiality of voters' choices exists).
197. See supra notes 4-10 and accompanying text.
198. See Drechsler, supra note 9, at B1 (reviewing the results and lessons of Estonia's first online election and praising the idea as a model for future nations to follow); Robin O'Brien Lynch, Estonia Takes the Lead in Online Voting, THE IRISH TIMES, Oct. 21, 2005, at 7 (comparing favorably the smooth Estonian online voting process against the problems Ireland has experienced with its traditional voting methods).