

# The Imperatives of Conducting a Source Code Review

*Comelec exerted its best efforts to avoid releasing the source code to interested political parties and groups for their independent review. On the other hand, CenPEG exerted its best efforts to force Comelec to obey the law as stated in Section 12 (Sec 14) of RA-9369. In the end, the Supreme Court has spoken, and has ordered Comelec to do the right thing.*

---

## Definition of Terms

The computer programs that were used for Automated Election System (AES) 2010 could be provided by Smartmatic in two forms: *source code* and *executable code*. Executable code or *machine language code* is the form of the program that the computer can “read” and execute, but human beings cannot, since it is in machine language consisting of sequences of zeroes (0) and ones (1). Source code is the form of the program that human beings, namely computer programmers, write using English-like computer programming languages, such as C or Java, and since programmers can write source code, they can read the source code that they, or other programmers, have written.

Smartmatic actually provided only the executable code of the computer programs that were used for AES 2010, and together with Comelec, exerted all efforts to avoid providing the source code to the public for review. This paper attempts to chronicle these efforts by Smartmatic and Comelec to hide the source code from the public.

To give a better understanding of source code, David Wagner has written a nice description<sup>[1]</sup>: *Source code is the human-readable representation of the instructions that control the operation of a computer. Computers are composed of hardware (the physical devices themselves) and software (which controls the operation of the hardware). The software instructs the computer how to operate; without software, the computer is useless. Source code is the human readable form in which software is written by computer programmers. Source code is usually written in a programming language that is arcane and incomprehensible to non-specialists but, to a computer programmer, the source code is the master blueprint that reveals and determines how the machine will behave. x x x Source code could be compared to a recipe: just as a cook follows the instructions in a recipe step-by-step, so a computer executes the sequence of instructions found in the software source code. This is a reasonable analogy, but it is also imperfect. While a good cook will use her discretion and common sense in following a recipe, a computer follows the instructions in the source code in a mechanical and unfailingly literal way; thus, while errors in a recipe might be noticed and corrected by the cook, errors in source code can be disastrous, because the code is executed by the computer exactly as written, whether that was what the programmer intended or not. x x x*

A source code review<sup>[2]</sup> is where someone other than the original author (programmer) performs a software code audit. A software code audit<sup>[3]</sup> is a comprehensive analysis of source code x x x with the intent of discovering bugs, security breaches or violations of programming conventions. The most important objective of source code review / audit is to establish correctness<sup>[4]</sup> of the program – that the program correctly implements its specifications. The specifications of the computer programs for AES 2010 are contained in our election laws and implementing rules and regulations, namely the AES Law (RA-9369), the Comelec Terms of Reference (TOR) to Bidders, and Comelec General Instructions regarding elections. Thus the ultimate purpose of source code review is to check that the computer programs that were used for AES 2010 are correct implementations of our election laws, and in particular, that these programs will do the counting and canvassing, not only quickly, but more importantly, correctly.

## Source Code Review in Our Election Laws and in the Comelec TOR

The AES Law RA-9369<sup>[5]</sup> recommends that Comelec perform a source code review on its own. Section 9 (Sec 11) contains the following provision,

“Sec. 11. Functions of the Technical Evaluation Committee (TEC). - The Committee shall certify x x x categorically stating that the AES, including its hardware and software components, is operating properly, securely, and accurately x x x based, among others, on the following documented results: x x x 3. The successful completion of a source code review;”

This provision is recommendatory but not mandatory, and Comelec does not have to do its own source code review, as stated in the following continuation of Section 11,

“If the Commission decides to proceed with the use of the AES without the Committee's certification, it must submit its reasons in writing, to the Oversight Committee, no less than thirty (30) days prior to the electoral exercise where the AES will be used.”

This Oversight Committee is the Joint Congressional Oversight Committee (JCOC) created in Section 27 (Sec 33) of RA-9369 to monitor and evaluate the implementation of AES 2010. So this provision allows Comelec, just by advising the JCOC in writing, to not obtain TEC certification, and so to not do a source code review.

While source code review is optional on the part of Comelec, RA-9369 mandates Comelec to make available and open to the public the source code of the election programs, for their own review, in Section 12 (Sec 14), as follows,

“Once an AES technology is selected for implementation, the Commission shall promptly make the source code of that technology available and open to any interested political party or groups which may conduct their own review thereof.”

The “source code” referred to here is the source code of the AES computer programs, in whatever state they are, “once an AES technology is selected for implementation”, that is, once Comelec awarded the AES contract<sup>[6]</sup> to Smartmatic on July 10, 2009. On this date, the Comelec is mandated by law to make the source code of the AES technology available and open to any political parties or groups who have indicated interest in doing their independent reviews of the source code, most especially when interest is indicated in writing, implying seriousness of purpose. There are canonical reasons why a review has to be done as soon as possible. First is that once the AES technology is selected, then Comelec has determined that the selected technology is in a state that is good enough to use, except probably for minor corrections in the program code (“raw source code”) and minor adjustments in program configuration. Thus the selected technology is good enough to be reviewed. Second is that once the AES technology is selected, there is usually too little time for the independent reviewers to do a thorough study of the source code for the purpose stated above, namely for the purpose of determining compliance with our election laws and implementing regulations. A thorough study should take anywhere between six to 12 programmer-months, when done in a review environment of total freedom, where programmers can discuss the code among themselves and with the public, which is the intention of Section 12 (Sec 14) of RA-9369.

The Comelec is cognizant of this obligation to make the source code available and open, although in a different sense, and has included in its TOR<sup>[7]</sup> to Bidders the following requirement,

“V. Other Specifications No. 7.4: The winning bidder shall authorize Comelec to make the final source code of the PCOS & CCS and all of its components available and open to any interested party or groups w/c may conduct their own code review thereof”

There is a major error in this requirement to bidders, and that is, that bidders make the “final source code” available and open to any interested party or groups. The “final source code” usually means the version of the source code that is “good enough” to run the PCOS computers at the precincts and CCS computers at the canvassing centers on election day, May 10, 2010. Everyone involved in software development knows that source code is “never final”, and that source code will never reach that stage of finality that is reasonably bug-free, especially software that is developed in a closed-source environment in which only the programmers of the software vendor Smartmatic-Dominion<sup>[8]</sup> can read, review and debug the source code. The bugs and non-conformity in the source code that the programmers of the vendor cannot see in the privacy of their corporate offices with their intellectual property rights (IPR) restrictions, the public can see when they work together, when they can review the source code in an environment of freedom, and when they can debate the source code in free public discussions. That is why Section 12 (Sec 14) specifies that “once the AES technology is selected for implementation”, the source code be made available and open to the public, whatever “raw” version the source code might be at the time of selection.

### **What is Needed to Make AES Source Code “Available and Open”?**

If Comelec is to obey the law, Section 12 (Sec 14) of RA-9369, it has to consciously and wilfully make the proper arrangements so that it can “make the source code of that (AES) technology available and open to any interested political party or groups which may conduct their own review thereof”. There are two ways to do these “proper” arrangements.

[A] If the AES technology selected by Comelec is released under one of the available open source licenses (GPL, BSD, Apache, MIT, Mozilla, Eclipse, etc)<sup>[8a]</sup>, then Comelec does not have to arrange anything special, since these licenses provide a mechanism for the public to download the source code that they will need in order to do the review.

[B] If the AES technology selected by Comelec is released under a closed-source commercial license, like the Smartmatic AES technology which Comelec has selected for the Philippine AES 2010, which is released under a closed-source commercial license from Dominion Voting Systems of Canada<sup>[9]</sup>, then Comelec, through vendor Smartmatic, or directly itself, has to arrange with licensor Dominion a special source-level license that will allow Comelec to “make the source code of that (Dominion) technology available and open (to itself and) to any interested political party or groups (in the Philippines) which may conduct their own review thereof”. In fact, Comelec should have made this arrangement of a special source-level license (that allows public source code review) a prerequisite qualification for any vendor to join the bidding for AES 2010. That Comelec did not do this in the case of winning bidder Smartmatic is, in my opinion, either due to gross ignorance of the law that it is expected to uphold, or gross negligence, or gross favoritism, or blatant disregard of RA-9369.

Source code that is made “available and open” connotes a greater pro-activeness than source code that is just simply made “open”. Source code is “open”<sup>[10]</sup> if it “is published and made available to the public, enabling anyone to copy, modify and redistribute the source code without paying royalties or fees. Open source code evolves through community cooperation. These communities are composed of individual programmers as well as very large companies”. Source code is made “available and open” by Comelec, if not only is it made “open” in the sense above, but its availability to the public is guaranteed by Comelec, by, say, making the source code available at a government-sponsored website specifically for the purpose of public distribution.

### **Comelec Compliance to Section 12, CenPEG's Position and the Supreme Court Ruling**

CenPEG<sup>[11]</sup> is the Center for People Empowerment in Governance, a non-government organization and public policy center established to help promote people empowerment in governance, especially advocating the democratic representation of the poor.

Our perception of Comelec's attempts to avoid implementation of Section 12 of RA-9369, of CenPEG's dogged determination to pursue source code review of the AES 2010 computer programs as a right of the people, and the Supreme Court's decision to uphold CenPEG's petition for mandamus to compel Comelec to release the source code to the public, are now all part of Philippine election history, and serves as a reminder that when the cause is good, the truth will out. Veritas liberandum – the truth shall set us free! We recount the events<sup>[12]</sup> that lead to this Supreme Court decision.

These events happened in 2009:

On May 26, CenPEG wrote an official letter to Comelec requesting for a copy of the source code of the PCOS program, the BOC CCS program, and the Comelec DCS utilities. The letter indicated that the request was made by CenPEG as an interested party to do source code review, as provided for by RA-9369.

On July 10, CenPEG received Comelec's reply dated June 24, with an attached Comelec en banc resolution dated June 16. The said Comelec resolution approved CenPEG's request for all of the requested source code, except for that of the DCS utilities.

After July 10, CenPEG immediately called on volunteers from U.P., Ateneo, La Salle, and other universities, and from the software houses in Metro Manila, and from the Philippine Linux Users' Group, to form a team of C/C++ and Java programmers who will do the actual source code review under the auspices and support of CenPEG. These programmers were the start of the CenPEG AES source code review team. Invitations were sent in the various mailing lists, and in face-to-face meetings at the CenPEG U.P. Office and at the U.P. College of Law.

On July 13, CenPEG wrote to Comelec, requesting for a meeting with Comm. Melo to discuss the plans for the conduct of the review.

On July 17, CenPEG wrote to Exec. Dir. Tolentino, acknowledging Comelec's positive response to CenPEG's request for the source code, and asking for the immediate release of the source code, as approved by Comelec en banc.

On July 20, CenPEG wrote to Comm. Melo, expressing readiness of CenPEG's AES team to pick up the source code for review.

On August 24, Dean Marvic Leonen of the U.P. College of Law, then ex-officio head of the U.P. Law-CenPEG project to study the AES2010, wrote to Comm. Melo for the immediate release of the source code for review of the CenPEG AES team.

On August 26, Comelec, through Law Department Head, Ferdinand Rafanan, wrote to CenPEG, saying that the source code "for implementation" does not exist at that time, for the following reasons [a] The baseline source code of the provider (Smartmatic) has not been received (since the payment has not yet been made to the provider as of that date). [b] The customization of the baseline source code is currently targeted for completion in November 2009. [c] The customized source code shall be reviewed by an "established international certification entity", on which basis, among others, the TEC shall issue its certification. The target for these is end of February 2010. [d] Only thereafter will the AES technology be available and can be made open to any interested political party or groups for review under a controlled environment. In the same letter, Comelec requested CenPEG to submit its profile with full disclosure on its registration and permits from national and local government authorities, on its by-laws, officers, members of the board, stakeholders, general membership, organization and experience, among others.

Note that Section 12 never mentioned anything about “source code for implementation”. On the contrary it mentions that “Once an AES technology is selected for implementation, the Commission shall promptly make the source code of that technology available and open to any interested political party or groups which may conduct their own review thereof.” At the moment that Comelec selected the Smartmatic AES technology for implementation of AES 2010, it is the duty of Comelec to obtain from Smartmatic the source code, in its “raw” state, without any additional “customizations” or “localizing program code” for the Philippines, and to make this source code available and open to any interested political party or groups, because that is what Section 12 mandates Comelec to do. Furthermore, Item [d] which states that only after [a], [b], and [c] have been resolved will the AES technology be available x x x for review under a *controlled environment*. Every programmer knows that the term “once an AES technology is selected for implementation” does not mean the same as “once conditions [a], [b], and [c] have been resolved”. Furthermore, every programmer knows “the Comelec shall promptly make the source code of that technology available and open to any interested political parties and groups which may conduct their own review thereof” and “Only thereafter will the AES technology be available and can be made open to any interested political party or groups for review under a controlled environment” are completely antithetical, since the two terminologies “conducting their own (independent) review” and “review under a controlled environment (controlled by Comelec and Smartmatic)” are in diametrical opposition. We cannot understand how Ferdinand Rafanan can use unbelievable lawyer language to twist and contort a “computer source code” provision of the law, to solve the “software licensing problem” that Comelec finds itself under, for selecting a vendor that, in the first place, should have failed to qualify under Section 12 of RA-9369.

On September 21, Ferdinand Rafanan delivered a final blow to the call public source code review, by announcing at the ANC-TV Automation Forum that “CenPEG and other interested groups will not do a source code review, but that an independent certification agency will do it as a prerequisite to TEC certification”. As we mentioned earlier, by a provision under Section 9 (Sec 11), Comelec is not even required to seek TEC certification of AES 2010, but is mandated under Section 12 (Sec 14) to make the source code available and open x x x etc.

On October 3, a joint appeal initially signed by 201 stakeholders representing CenPEG, NASSA-CBCP, AMRSP, UPAA, Transparency International-Philippines, the Computer Science Departments of several universities, Deans and faculty of several law schools, various religious congregations, various NGOs, etc., was addressed to Comelec, for the poll body to comply with the AES law by releasing the source code.

On October 5, a *mandamus* case was filed by CenPEG with the Supreme Court to compel the Comelec to release the AES source code to interested parties for review.

On October 16, CenPEG received a letter dated September 23 from Comelec, asking for CenPEG's application as a precondition for doing a review of the May 10, 2010 election source code.

On October 30, CenPEG replied to Comelec, asking what specific provisions of the law requires interested parties to submit such requirements, and saying that such requirements might only create administrative roadblocks in the conduct of review by different parties.

These succeeding events happened in 2010:

On January 26, Comelec announced the release of the source code to parties who will submit documents required by the Comelec, and that the review will start February 5. The Comelec also released the nine-point guideline for the review.

During the period February 1-4, Comelec conducted orientations at Palacio del Gobernador, with parties interested on the review of the source code, and during this time a SysTest representative created the Final Trusted Build (FTB) of the AES programs, in the presence of representatives of

political parties. The FTB procedures followed are as follows: The source code of the PCOS and CCS programs are certified by SysTest and the TEC. Then the source codes are compiled to produce the executable code that will actually be installed in the PCOS and CCS computers on election day. Then the hash values of all source code and executable code are computed and reported to the public. Finally, all source code, executable code, and hash values are saved on CD/DVD, and deposited in escrow with the Bangko Sentral ng Pilipinas, in conformity with Section 9 (Sec 11 Item 4) of RA-9369. All of these were done in the presence of representatives of political parties, hence the name Final Trusted Build.

On February 19, some political parties and groups issued a joint statement that they are willing to conduct the source code review, but found the guidelines to be too restrictive.

On February 24, Comelec invited representatives of political parties and interested groups, and Comm. Gregorio Larrazabal advised them that a facility has been prepared by Comelec where parties may access the source code, and that the guidelines for review originally issued will not be changed. The representative from Liberal Party withdrew its intent to participate in the review, because of the restrictive conditions and the lack of material time (less than three months). The AESWatch representative also confirmed non-participation for the same reasons.

On March 9, the TEC released its certification of the AES, which includes a certification of the source code review done by SysTest Labs, the international certification body commissioned by Comelec as provided for in a non-mandatory provision of Section 9 (Sec 11) of RA-9369. The official report of the TEC and SysTest certifications were never released to the public until after the Supreme Court granted the mandamus petition of Teofisto Guingona, Jr., et. al.<sup>[13]</sup>, “compelling respondent Comelec to explain fully the complete details of its preparations for the May 10, 2010 elections, in view of the unraveling of alarming events of late”. The petition was granted on May 6, Thursday of the week before the May 10 elections. CenPEG was able to get hold of a copy of the SysTest and TEC certifications only in the first week of October. Also the Supreme Court decision mandates Comelec to supply the source code of the AES to the petitioners, but to date, Comelec has not complied with this mandate.

Finally, the following historic event serves as climax to CenPEG's quest for the source code of AES 2010.

On September 21, the Supreme Court granted CenPEG's petition for mandamus<sup>[14]</sup>, compelling Comelec to make the source code of AES 2010 available to CenPEG and to all other interested political parties and groups.

Today, Comelec has not released the source code of AES 2010 to anyone. It seems not to have any intention to do so today, or any time soon, despite the Supreme Court ruling.

### Transparency and Source Code Review

The basic principle of elections in a democratic society is *secret voting and public counting*. But how do we implement computerized counting that the public can see, when the computer counts too fast for the public to follow the count? Also when there are 51 million ballots to count, it does not make sense to slow down the counting computers so that the voters in the precinct can visually verify the correctness of the computer count of each of the 1,000 ballots cast in that precinct. We propose here that source code review is a reasonable substitute to public counting in a computerized election, if used together with an anonymous but positive voter verification that his vote is included in the final count, as in the Scantegrity II System[14a].

In Multiply blog<sup>[15]</sup>, this author writes about why the public has to do a source code review of the AES computer programs, and I quote, “You cannot compare the computer programs used by banks for their on-line transaction processing with the computer programs used for national and local elections. In the case of banking transactions, the secrecy of the computer source code is sacred, because if a hacker-thief learns of the

vulnerabilities of the banking system from reviewing the source code, he could steal money from the depositors using his knowledge of the vulnerabilities. But the computer programs for elections are different. Just as you want to know how the teachers belonging to the Board of Election Inspectors are counting your votes in a manual election, and in fact you want to watch them count your votes in a manual election, you also want to know, and want to watch the computer count your votes in a computerized election. But the computer is too fast, so you cannot see what it is doing. So you rely instead on the programmer-reviewers, who will watch what the program is doing, by reading the source code. So the reviewers will do the watching for you, and make sure that your votes are counted”.

### **Implications of the Lack of Source Code Review on Election Day**

The following disastrous events happened at, or around, election day 2010. They could have been prevented if the interested political parties and groups had been allowed to do their own independent, early, and thorough, source code review.

On May 3, during the Final Testing and Sealing (FTS) activities at the precincts, the mismatch between ballot faces and CF-card configuration data for the PCOS computer was discovered to occur nationwide. Had a source code review been done early enough, this mismatch could have been predicted, and prevented from happening, by putting into the source code the necessary algorithm to match ballot face with proper CF-card configuration data, without resorting to trial-and-error testing procedures.

On May 10, during actual election day, about 200 PCOS computers transmitted FTS results, consisting of ten or less ballots, to the municipal CCS computers, and these FTS results were accepted as official election returns (ER). When the actual election returns were being transmitted, PCOS computers would not transmit and CCS computers would not receive, since an earlier transmission from the same precincts have already been accepted. Had a source code review been done early enough, these transmissions of FTS results and actual election day results could have been differentiated by proper PCOS and CCS program design, and properly handled.

After May 10, during national Comelec canvassing, the CCS server being used to canvass votes for partylist and senators generated a total of 153.9 million registered voters<sup>[16]</sup>, while Comelec has only 50.7 million registered voters. Also during the national Congressional canvassing, the CCS server being used to canvass votes for president and vice-president generated a total of 256 million registered voters<sup>[17]</sup>. These two conflicting totals, both of which are in error, is proof of serious bugs in the CCS source code, or of a serious error in the design of the canvassing logic, both of which could have been prevented by a proper and early source code review.

During election day on May 10, and for several days thereafter, Comelec's public website<sup>[18]</sup> was reporting election results from all the clustered precincts, cities, municipalities, districts, and provinces all over the country. A significant number<sup>[19]</sup> of these election results contain html syntax errors, such as [a] improperly paired tags (<html> tag without the matching </html> tag, <td> tag without the matching </td> tag, etc), [b] an entire candidate position, such as vice-governor, with no candidates names and no votes reported, [c] an empty html page of filesize zero, and several other kinds of html syntax errors. These html syntax errors can only result from errors in the CCS program, errors that could have been discovered by an early and thorough source code review.

### **Best Industry Practice**

A number of organizations have offered election programs which are either open source or whose source code (though not open) is available for public scrutiny. First is the Open Source Digital Voting Foundation (OSDV) with their “Trust the Vote” Project<sup>[20]</sup>. Second, Sequoia Voting Systems has announced in December 2009 that it is open-sourcing its Frontier Voting System, a product that it will sell in the future<sup>[21]</sup>. Third is Australia's Electronic Voting and Counting System (eVACS), for which its source code is available for public scrutiny<sup>[22]</sup>. Fourth is the OpenSTV.Org<sup>[23]</sup>, which implements a single transferable system of voting used in

Ireland. Fifth is the Free eDemocracy Project<sup>[24]</sup> which aims to provide a non-commercial private, secure, reliable and open electronic voting alternative to the commercial offerings of questionable quality. Sixth is the Open Voting Consortium EVM project<sup>[25]</sup>, an open source voting machine project that is written in Python. This is different from the Indian EVM project<sup>[26]</sup>, which may also be open source. This is not an exhaustive listing, and there are other open source or open-to-public-scrutiny election programs that can still be added to this list.

In the Philippines, we are fortunate that public source code review of our election computer programs is provided for in our laws (Section 12(14) of RA-9369). But we are also unlucky because we have a Comelec that does not respect the rights of the voters to know how the election computer programs work. Furthermore, Comelec does not value the potential contribution of the Filipino programming community, which includes the world's best programmers in its ranks, towards making the Philippine AES the world's best.

### Conclusion

It is clear to us that Comelec exerted its best efforts to avoid releasing the source code to interested political parties and groups for their independent review. On the other hand, CenPEG exerted its best efforts to force Comelec to obey the law as stated in Section 12 (Sec 14) of RA-9369. In the end, the Supreme Court has spoken, and has ordered Comelec to do the right thing.

---

### End Notes:

- [1] David Wagner, "Testimony on Source Code Disclosure for the House Administration Elections Subcommittee" of the United States Congress, [http://www.votetrustusa.org/index.php?option=com\\_content&task=view&id=2327&Itemid=26](http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2327&Itemid=26)
- [2] Source code review is defined in [http://en.wikipedia.org/wiki/Defensive\\_programming](http://en.wikipedia.org/wiki/Defensive_programming)
- [3] Source code audit is defined here: [http://en.wikipedia.org/wiki/Code\\_audit](http://en.wikipedia.org/wiki/Code_audit)
- [4] Program correctness is defined here: [http://en.wikipedia.org/wiki/Program\\_correctness](http://en.wikipedia.org/wiki/Program_correctness)
- [5] Republic Act 9369 is available for downloading from <http://www.chanrobles.com/republicactno9369.html>
- [6] This contract between Comelec and Smartmatic is entitled, "Contract for the Provision of an Automated Election System for the May 10, 2010 Synchronized National and Local Elections", and is dated July 10, 2009.
- [7] The Comelec Terms of Reference (TOR) to Bidders of the 2010 National and Local Elections was made available to interested bidders for PHP1.0 million per bidder. A version of this document is now posted at the Comelec website, [http://www.comelec.gov.ph/modernization/2010\\_natl\\_local/2010\\_Election\\_automation\\_project.html](http://www.comelec.gov.ph/modernization/2010_natl_local/2010_Election_automation_project.html)
- [8] The vendor of the AES technology is Smartmatic International, but the technology is owned and licensed by Dominion Voting Systems of Canada, so the term "Smartmatic-Dominion" for vendor is appropriate in this context.
- [8a] The specifics of these open source licenses, and their differences, can be found in the website, <http://www.opensource.org/licenses/category>.
- [9] The software license agreement between Smartmatic and Dominion is entitled, "License Agreement between Smartmatic International Corporation (Smartmatic) and Dominion Voting Systems (dominion)", and dated April 4, 2009. The license agreement is signed by Antonio Mujica for Smartmatic and Chris Iskander for Dominion. The license is a closed-source commercial license that does not give Comelec the right to offer the source code for review to interested political parties and groups, but in fact, prohibits such activity in Item 7 of the agreement, which states, "Dominion will retain sole liability to amend, change or develop all software, or firmware or EMS".

- [10] This is the definition of “open source software”, given in [http://en.wikipedia.org/wiki/Open\\_sourceresults/2010\\_natl\\_local/](http://en.wikipedia.org/wiki/Open_sourceresults/2010_natl_local/)
- [11] This description of CenPEG is from the website, [http://www.cenpeg.org/about\\_us.htm](http://www.cenpeg.org/about_us.htm)
- [12] All correspondence mentioned here are on file at the CenPEG office in the U.P. Diliman campus.
- [13] This is Supreme Court decision GR-191846, dated May 6, 2010, available at the website, [http://www.lawphil.net/judjuris/juri2010/may2010/gr\\_191846\\_2010.html](http://www.lawphil.net/judjuris/juri2010/may2010/gr_191846_2010.html)
- [14] The Supreme Court's decision to grant CenPEG's petition for mandamus is contained in GR-189546, dated September 23, 2010, and is available for download from the website <http://www.cenpeg.org/>
- [14a] A method that provides “voter verification” and a positive check that the vote is included in the count is the Scantegrity II System (<http://www.scantegrity.org/washington/>). In this system you mark your choices by applying a special ink on the oval of the candidate of your choice. The special ink reveals a random number assigned to the candidate (the random number for each candidate changes from ballot to ballot and the candidate does not know what numbers are assigned to him). Your ballot also has a random number assigned to it. You copy these random numbers, and check if they appear in the election website. If they do, then your vote for that candidate has been included in the count.
- [15] The difference between source code review of a banking program and source code review of an election program is discussed in the blog post, [http://pmana.multiply.com/journal/item/113/COMELEC\\_ALLOWS\\_SOURCE\\_CODE\\_REVIEW\\_A\\_COMMENTARY\\_Feb\\_04\\_10](http://pmana.multiply.com/journal/item/113/COMELEC_ALLOWS_SOURCE_CODE_REVIEW_A_COMMENTARY_Feb_04_10)
- [16] The error of 153.9 million registered voters is reported in <http://votereportph.org/blog/total-registered-voters-printed-national-canvass-report-153902003>
- [17] The error of 256 million voters is reported in <http://www.abs-cbnnews.com/nation/05/24/10/house-server-shows-256-million-filipino-voters>
- [18] The Comelec public website used to be at <http://electionresults.comelec.gov.ph/>. Lately the site was moved to [http://www.comelec.gov.ph/results/2010\\_natl\\_local/](http://www.comelec.gov.ph/results/2010_natl_local/).
- [19] In our Multiply blog, [http://pmana.multiply.com/journal/item/204/Errors\\_in\\_Election\\_2010\\_Oct\\_13\\_10](http://pmana.multiply.com/journal/item/204/Errors_in_Election_2010_Oct_13_10), we scanned the Comelec public website as of May 22-24, 2010, and discovered more than 21,000 precinct results that contained html syntax errors, out of the total of about 76,000 precincts. This is about 27.6% error rate, and is a dismally embarrassing figure for a computerized election.
- [20] The Open Source Digital Voting (OSDV) Foundation (<http://www.osdv.org/>) has the “Trust the Vote” Project (<http://www.trustthevote.org/>). The source code for the project is available for download from, <http://github.com/trustthevote>
- [21] Although it has been announced that Sequoia is open-sourcing ([http://www.theregister.co.uk/2009/12/02/sequoia\\_source\\_code\\_disclosure/](http://www.theregister.co.uk/2009/12/02/sequoia_source_code_disclosure/)) its “Frontier” voting system, and in fact, has released the first batch of “Frontier” source code, it appears that Dominion Voting has acquired Sequoia. On visiting the Sequoia page <http://www.sequoiavote.com/>, you get directed to <http://www.dominionvoting.com/>. It is not clear how this affects the continued release of the “Frontier” source code, which was made available in <http://sequoiadev.svn.beanstalkapp.com/projects/>
- [22] The source code of Australia's eVACS is available for download from, <http://www.elections.act.gov.au/downloads/evacs2008.zip>
- [23] The OpenSTV website is <http://www.openstv.org/>. The source code is downloadable from, <http://stv.googlecode.com/files/OpenSTV-1.6.1.tar.gz>
- [24] Free eDemocracy Project is available from Sourceforge, <http://sourceforge.net/projects/free/files/FREE/GNU.FREE-1.9/gnufree-1.9.tar.gz>
- [25] The Open Voting Consortium EVM project is described here, [http://www.openvotingconsortium.org/our\\_solution](http://www.openvotingconsortium.org/our_solution). The source code for EVM is available here, <http://sourceforge.net/projects/evm2003/files/>
- [26] The Indian EVM project is described here, <http://www.indian-elections.com/electoralsystem/electricvotingmachine.html>