SECTION: PIL

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL WRIT JURISDICTION)

WRIT PETITION (CIVIL) NO. 434 OF 2023

IN THE MATTER OF:

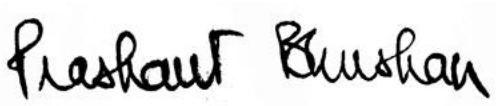
ASSOCIATION FOR DEMOCRATIC REFORMS .... PETITIONER

VERSUS

ELECTION COMMISSION OF INDIA & ANR. .... RESPONDENTS

FILING INDEX

S. NO.	PARTICULARS	COPIES	C. FEE
1.	REJOINDER AFFIDAVIT ON BEHALF OF THE PETITIONER	**1**	**20/-**
2.	ANNEXURE R1 TO R11	**1**	**NIL**



(PRASHANT BHUSHAN)
COUNSEL FOR THE PETITIONER
301 NEW LAWYERS CHAMBER
SUPREME COURT OF INDIA
NEW DELHI-110 001
CODE NO. 515

NEW DELHI
DATED: 18.10.2023

IN THE SUPREME COURT OF INDIA

(CIVIL ORIGINAL WRIT JURISDICTION)

WRIT PETITION (CIVIL) NO. 434 OF 2023

IN THE MATTER OF:

ASSOCIATION FOR DEMOCRATIC REFORMS …. PETITIONER

VERSUS

ELECTION COMMISSION OF INDIA & ANR. …. RESPONDENTS

PAPER BOOK

(FOR INDEX KINDLY SEE INSIDE)

{REJOINDER ON BEHALF OF THE PETITIONER}

COUNSEL FOR THE PETITIONER: **PRASHANT BHUSHAN**

INDEX

8.	**Annexure-R7:** A copy of RTI reply dated 03.04.2019 received from Indian Statistical Institute	**63-67**
9.	**Annexure-R8:** A copy of the opinion of Dr. S.K. Nath annexed as Annexure P14 and P15 in W.P.(C) 1514/2018	**68-79**
10.	**Annexure-R9:** article written by K. Ashok Vardhan Shetty titled, "*Winning Voter Confidence: Fixing India's Faulty VVPAT-based Audit of EVMs*" published on 27.11.2018 in The Hindu Centre for Politics and Public Policy	**80-115**
11.	**Annexure-R10:** A copy of the article titled, "*A Hitchhiker's Guide to Electronic Voting Machines and VVPATs*" published in *The Wire*, on 18th April, 2019,	**116-119**
12.	**Annexure-R11:** A copy of the judgement dated 03.03.2009 of the Second Senate of Germany	**120-156**

IN THE HON'BLE SUPREME COURT OF INDIA
(CIVIL ORIGINAL JURISDICTION)
WRIT PETITION (CIVIL) NO. 434 OF 2023
(UNDER ARTICLE 32 OF THE CONSTITUTION OF INDIA)

IN THE MATTER OF

ASSOCIATION FOR DEMOCRATIC REFORMS .. PETITIONER

VERSUS

ELECTION COMMISSION OF INDIA & ANR. ..RESPONDENTS

REJOINDER AFFIDAVIT ON THE BEHALF OF PETITIONER

I, Jagdeep Chhokar, S/o Raghvir Singh, the Founder-Trustee of the petitioner trust, having its office at T-95, C.L House, II Floor Gautam Nagar, New Delhi, do hereby solemnly affirm and state on oath as under: -

1. That I am the Founder-Trustee of the petitioner trust in the accompanying writ Petition and being well conversant with the fact and records of the case, I am competent and authorised to swear this affidavit on the behalf of Petitioner Trust.

2. That I have gone through the contents of the preliminary counter affidavit dated 04.09.2023 filed by Respondent No. 1 i.e. Election Commission of India and the present rejoinder affidavit is being filed thereto. That a para wise reply is not being filed by the petitioner and the major arguments in opposition raised by the Election Commission are being dealt with. However, if needed or the Hon'ble Court so directs; the petitioners crave liberty of this Hon'ble Court to file a detailed rejoinder.
3. At the outset, it is submitted that the petitioners have not challenged the use of EVM's in the elections. The petitioner's prayer is only for verification of the results of the EVMs by cross verifying them with the

Oath Commissioner, New Delhi

The Seal of the Oath Commissioner
Sl. No. 64/2023
B.P. YADAV
App. By Delhi High Court
Period: 15.07.2023 to
14.07.2025
Supreme Court of India, New Delhi-1

VVPATs. The purpose and need for cross verification of EVMs is no longer *res integra* and has already been decided upon by this Hon'ble Court in ***Subramanian Swamy v. Election Commission of India, (2013) 10 SCC 500.*** Therefore, the reliance of the Election Commission on judgements wherein constitutionality of EVMs was upheld are differentiable. The judgement in *Swamy* is premised on the basis that the results of EVM themselves cannot be verified and therefore a paper trail is required which can verify the results in the EVMs.

4. That the question of integrity of EVMs has specifically been kept open by this Hon'ble Court in ***N. Chandrababu Naidu v. Union of India (2019) 15 SCC 377*** and the number of EVMs to be cross verified was kept at 5 per assembly constituency by this Hon'ble Court in *Chandrababu Naidu* in the facts and circumstances of that matter specifically noting the proximity to the election schedule and administrative difficulties pointed out by the Election Commission in that matter at that time. *Arguendo,* even going by the "science of statistics" relied upon by the Election Commission (which is heavily disputed by other leadings statisticians as elaborated later); even to maintain the same confidence level and probabilities; the number of VVPATs to be cross verified would have to be increased keeping in mind that the number of polling stations and EVMs increases in each general election. For instance in the 2014 general elections there were 9, 27, 553 polling stations whereas in the 2019 general elections there were 10,37,848 polling stations and therefore correspondingly more EVMs. The number of VVPATs to be cross verified even going by the heavily disputed "science of statistics" by the Election Commission can never be fixed and has to be decided keeping in mind the increase in the number of polling stations. It would be irrational, arbitrary, and

violation of Article 14 to fix the number of EVMs to be cross verified fixed at five in view of the judgement in *Chandrababu Naidu's* case even if the number of polling stations changes. Therefore, each election cycle is a new cause of action in so far as the number of EVMs to be cross verified with VVPATs is concerned till the time all EVMs are cross verified with VVPATs.

DIFFERENCE IN VOTE COUNTS IN VVPAT AND EVM IN POLLING STATIONS

5. That as of date 5 polling stations per assembly constituency are randomly chosen where results in VVPATs are cross verified with that of EVMs as per the judgement of this Hon'ble Court in *N. Chandrababu Naidu v. Union of India, (2019) 15 SCC 377*. Hitherto, the case of the Election Commission has been that if no problem is detected in the results in these 5 randomly chosen polling stations where result is cross verified with that of VVPATs, then it can be safely concluded that the probability of there being a problem in any of the other polling booths where EVMs are not cross verified with the VVPATs is close to nil.

6. That notably at paragraph 4.33, the Election Commission has admitted in it's counter affidavit that during the random cross verification of five VVPATs with EVMs in each assembly constituency; there have been instances wherein the total count of votes in the EVM has differed with the total count of votes in the VVPATs in response to the petitioner's contention that the EVM and VVPAT count differed in Polling Station No. 63 of Mydukur Assembly Constituency in Andhra Pradesh in the 2019 general elections wherein the EVM count was 233 votes whereas the VVPAT count was 219 votes i.e. a total difference of 6 percent in votes counted.

7. That the Election Commission has failed to provide data as to in how many polling stations discrepancy between vote count in EVMs and VVPATs have been detected.

8. The Election Commission has stated that it has protocols in place as per Para 14.5 of Chapter 14 of the *Updated Manual on Electronic Voting Machine and VVPAT* for counting of votes in the polling station where a difference in the total vote counts in the EVMs and VVPATs is detected during cross verification. It is submitted that as the protocol can only come into effect when the discrepancy is detected; it begs the question as to how the discrepancy can be detected in those polling stations where the results in the EVMs are not cross verified with that in the VVPATs.

9. That the Election Commission has failed to state as to what inference can be drawn about the correctness of the total vote count in EVMs in those polling stations where the VVPATs are not cross verified with the EVMs.

10. That since five EVMs per constituency represent roughly two percent of the polling booths; it can be shown that even if ten percent of the EVMs have a mismatch with the VVPAT counts; the chances of even one of the ten percent faulty EVMs being picked up in the random VVPAT checks will be (1-(9/10)^5) * 100 which is roughly equal to 40.95%. Therefore, a student of mathematics/probability/ statistics would be able to show that the claim of the Election Commission that not finding any EVM tampered with would show more than ~99.9999% probability of their being no fault in any EVM is false.

11. That if some EVM is found faulty/mismatched with VVPAT; the protocol of Election Commission is only to count the VVPATs in only that polling station and no procedure is laid out to match the other EVMs with VVPATs which also makes a mockery of the two percent sample testing.

12. That apart from all this, there is massive apprehension of the possibility of the EVM tampering among not merely large sections of people but also large sections of political parties who have jointly asked for return to paper ballots. Even the Citizens Committee headed by Hon'ble Justice (Retd.) Madan B. Lokur after consulting a large number of international experts came to the conclusion that there was certainly a possibility of EVM manipulation or malfunction or wrong recording of votes. This is apart from the possibility of EVMs being replaced before counting.

13. That the Election Commission of India says that the counting of VVPATs will take additional six days. The basis for this calculation has not been explained. Even in the era of paper ballots (just 15 years ago) the maximum time for counting and declaration of results was two days. Counting VVPAT slips would be easier than counting the ballot papers as the VVPAT slips only contain one name and symbol whereas the ballot paper was much longer containing multiple names and symbols. In any case, at a time when elections are conducted in multiple phases spread over a month or more; the declaration of results takes place more than a month after the first polling.

14. The contention of the Election Commission that an insurmountable administrative burden would be cast upon it if all the VVPATs were to

be cross verified is denied. The Election Commission has stated that for counting of VVPATs one counting booth is converted into a VVPAT counting booth (VCB) like bank cashier cabin where three officers count one VVPAT box under monitoring of CCTV in about one hour (para 4.49). In the general elections for 2019, there were about 10.35 lakh polling stations where 17.4 lakh VVPATs were used as per the statistics released by the Election Commission. All that the Election Commission needs to do is to create more VCBs and have the existing manpower deployed, count the VVPATs in teams of three under CCTV monitoring as per the existing procedure for which only the manpower needs to be trained and requisite VCBs need to be set up.

15. That former Chief Election Commissioner Sh. S.Y.Quraishi (in whose tenure the VVPATs were deployed) has also stated that instead of returning to the paper ballot system as demanded by some political parties; it is better to count all VVPATs and the time taken for the same would not be significantly more than the time taken to count EVMs and it is important to ensure that the results of the elections are seen as credible. A copy of the interview[1] dated 28.12.2020 of former Chief Election Commissioner Sh. S.Y. Quraishi given to *The Quint* is annexed herewith as **Annexure R1 (Pages** 17 **to** 20**).**

16. Further, period for counting can be reduced to a few hours if barcodes were put on the VVPAT slips which will allow them to be counted mechanically as seemingly suggested by the Election Commission itself in its present counter affidavit (para 4.49 at Page 67 of counter affidavit) as also the counter affidavit filed in Chandrababu Naidu's case.

17. Therefore, even if one assumes that EVMs are incapable of being tampered with or malfunctioning or showing wrong counts; even then the counting of VVPAT slips would give much greater assurance about the integrity of the Election process and results and instil greater public confidence in the electoral process and results.

SANCTITY OF EVMs: ECI's EXPERTS V OTHER DOMAIN EXPERTS

18. The Election Commission of India has submitted that it has it's own Technical Expert Committee which consists of professors from eminent institutes of excellence such as IITs which reviews and monitors the design of EVMs and that the EVMs undergo quality and functional testing by an independent third party which works under Ministry of Electronics & Information Technology (para 4.43). The Commission has further averred that the software is developed by separate teams from ECIL and BEL independently. That, thereafter it is reviewed by an independent third party and thereafter by the Technical Expert Committee of Election Commission which 'seals' the source code and the "*golden copy remains under sealed condition only*"(para 4.56)

19. That as the Counter Affidavit does not give a para wise reply to the writ petition, the contents of the writ petition specifically paras 15 to 18 containing the findings, conclusions and recommendations of the report titled, '*An inquiry into India's Election System: Is the Indian EVM and VVPAT system fit for democratic elections?*' published in January, 2021, by Citizens' Commission on Elections' (CCE) chaired by Hon'ble Justice (Retd.) Madan B. Lokur which have not been specifically addressed by the Respondent No. 1 are reiterated and may be treated as

part and parcel of the present rejoinder and are not being repeated herein for brevity.

The sum and substance of the aforementioned report based on deposition of various domain experts is that it is not possible for the voters to verify based solely on the results of the EVMs that their vote has been 'recorded as cast' and 'counted as recorded' because of the opaque manner in which the software and hardware of the EVM has been developed and deployed by the Election Commission of India.

20. The report by domain experts specifically points out that the claims of the Election Commission that the chip used in an EVM is not reprogrammable is false; that the EVM by itself does not ensure 'end to end' verifiability; the contention that an EVM cannot be hacked is false.

21. Further, Election Commission's claim that the EVMs are secure as the software and hardware for it is developed exclusively by inhouse employees of Bharat Heavy Electronics Limited (BHEL) and Electronics Corporation of India Limited (ECIL) is denied. News publication, *The Quint,* in an article titled, *'RTI Reveals Pvt Consultants Have EVM Access, Why is EC Denying It?'* published on 04.08.2019, reported that as per RTI documents available with it; the ECIL, a PSU that manufactures EVMs and VVPAT machines, engaged private engineers as "consultants" and that these private engineers have worked with the Election Commission in Assembly Elections since 2017 and even in the 2019 Lok Sabha election. Their job was extremely sensitive – to check and maintain EVMs and VVPATs, starting from First level Checking (FLC) right up till and including the Counting Day, which means they had easy access to EVMs through the course of the

elections. ECIL engaged these private engineers for the Election Commission from a Mumbai-based private company called M/s T&M Services Consulting Private Limited. ECIL confirmed that close to 50 private consulting engineers were used to check EVMs during the 2017 Uttarakhand Assembly elections, and that only eight regular employees of ECIL were involved. The private consulting engineers' job was to upload key details like party symbols and candidates' names on the EVMs and VVPAT, for which they had access to these machines for 15 days before polling. A copy of article titled, 'RTI Reveals Pvt Consultants Have EVM Access, Why is EC Denying It?' published on 04.08.2019 by *The Quint* is annexed herewith as **Annexure R2 (Pages 21 to 25).**

22. It would appear that there is a difference in opinion between the experts engaged by the ECI and other domain experts. As the court and the citizens have no methodology to decide which of the experts is correct, especially because the source code of the EVM is kept in a sealed cover by the ECI which it refuses to subject for audit for whatever reason; the issue is in what other manner can the veracity of the election be verified. While the entire report of the Committee chaired by Hon'ble Justice (Retd.) Madan B. Lokur is based on depositions of experts a few opinions of Domain experts are annexed herewith to substantiate that other domain experts disagree with the Election Commission's view on the integrity of EVMs. A copy of expert opinion of Professor Subhashish Banerjee who was a professor at IIT and is presently with Ashoka University is annexed herewith **Annexure R3 (Pages 26 to 27).** A copy of the deposition of Professor Poorvi Vora, George

Washington University, Washington, DC, USA, et all is annexed herewith as **Annexure R4 (Pages** 28 **to** 51**).** A copy of paper titled, "*Electronic Voting and Democracy*" published by Subodh Sharma of School of Computer Science & Engineering at IIT, Delhi is annexed herewith as **Annexure R5 (Pages** 52 **to** 59**).** A copy of deposition titled, "To use or not to use? Electronic Voting Machines in Indian Elections." by Sandeep K Shukla, Professor at IIT Kanpur is annexed herewith as **Annexure R6 (Pages** 60 **to** 62**).**

23. That even in *Chandrababu Naidu's* case this court had refused to go into the issue of technical sanctity of the EVMs and left the issue open.

24. It is in this context that the writ petition effectively seeks appropriate directions from this Hon'ble Court to ensure that the voters are able to verify that their vote has been 'recorded as cast' and 'counted as recorded' and to this end seeks cross verification of the results stored in VVPATs with that of the EVMs in line with the purport and object of introduction of VVPATs by this Hon'ble Court in ***Subramanian Swamy v. Election Commission of India*, (2013) 10 SCC 500** as because of the secrecy of software and hardware maintained by ECI as regards EVMs; it is impossible for anyone including the members of the Election Commission who are not technical experts themselves to verify the sanctity of the same.

STATISTICS: ECI'S DOMAIN EXPERTS V. OTHER DOMAIN EXPERTS

25. That the reliance by the Election Commission on what it calls the report of Indian Statistical Institute dated 22.03.2019 (at Paras 4.8 to 4.12) and which report the petitioner's term as Dr. Ajay Bhat report which

submitted that 479 randomly selected sample VVPATs are sufficient to declare the entire election as a whole to be defect-free and bias-free with 99.99% confidence level is misconceived.

26. Firstly, there was no formal engagement of the Indian Statistical Institute by the Election Commission to prepare a report. At best, one Deputy Election Commissioner wrote directly to one particular professor i.e. Dr. Ajay Bhat who proceeded to co-opt persons of his own choice on an ad hoc basis to prepare the report. There is no record available with ISI of it having formed a committee to study the issue. There is no record available with ISI showing the members of the committee. There are no records available with ISI as regards the proceedings of the committee. A copy of RTI reply dated 03.04.2019 received from Indian Statistical Institute is annexed herewith as **Annexure R7 (Pages 63 to 67).**

27. On merits, it may be noted that Dr. Ajay Bhat report itself notes that it had also consulted Dr. S.K. Nath, *inter alia* a former Director-General of the Central Statistics Organisation and who had in fact opined that the Election Commission's decision to cross-verify only one (1) randomly chosen polling station from all polling stations in an assembly constituency was woefully inadequate and statistically insignificant and that for a 98% confidence level of less than 2% margin of error, the percentage of randomly chosen polling stations for cross verification must at least by 30% in an assembly segment with 200 polling stations. Dr. S.K. Nath had in fact critiqued the methodology adopted by Dr. Ajay Bhat's team. This opinion of Dr. S.K. Nath who is also a domain expert formed the basis for the petitioners in tagged petitions in Chandrababu Naidu's case (W.P(C) 1514 of 2018 titled M.G.

Devasahayam & Ors. v. Election Commission of India) to argue that the number of VVPATs that need to be cross verified needs to be much more than one. Dr. S.K. Nath's report was on record before this Hon'ble Court in *Chandrababu Naidu's* case. A copy of the opinion of Dr. S.K. Nath annexed as Annexure P14 and P15 in W.P.(C) 1514/2018 is annexed herewith as **Annexure R8 (Pages 68 to 79).**

28. Dr. Ajay Bhat's/ISI's recommendation is based on the standard hypergeometric distribution in probability theory and it assumes that the entire nation -with a deployment of about 10,00,000 EVMs- is a single population. However, this is inappropriate as election results are declared at the level of a constituency and the 543 parliamentary constituencies are not homogeneous. If instead a parliamentary constituency is considered as a population -with the number of EVMs deployed ranging from 300 to 1800 in a parliamentary constituency- then the same formula will suggest that a much higher number of EVMs need to be cross verified. In fact, with 1000 EVMs in a typical constituency, the number of EVMs that will be required to be cross checked according to the same formula will be about 370. This is adequately explained in the CCE report, based on depositions from Poorvi Vora and others. It is further explained in an article written by K. Ashok Vardhan Shetty titled, "*Winning Voter Confidence: Fixing India's Faulty VVPAT-based Audit of EVMs*" published on 27.11.2018 in The Hindu Centre for Politics and Public Policy annexed herewith as **Annexure R9 (Pages 80 to 115).**

29. That Dr. Ajay Bhat's report though referred to in the *Chandrababu Naidu's* case was clearly not relied upon by this Hon'ble Court as the court went on to increase the number of VVPATs to be cross verified to

five per assembly segment instead of one over the objection of the Election Commission of India which had taken the stand that counting one VVPAT per assembly constituency was already more than the 479 referred to by Dr. Ajay Bhat's report.

30. That though no reasoning has been provided by this Hon'ble Court in *Chandrababu Naidu's* case for increasing the VVPATs to be counted from one to five; it can only be presumed that it was on account of the fact that there were time constraints when that petition was decided as explicitly noted by this Hon'ble Court in that judgement.

31. That pursuant to the judgement in *Chandrababu Naidu's* case; other experts at Indian Statistical Institute have critiqued the decision of the court to increase the number of VVPATs to be cross verified to 5 per assembly constituency only terming it statistically insignificant in an article titled, "A Hitchhiker's Guide to Electronic Voting Machines and VVPATs" in The Wire, an online news journal, on 18th April, 2019 by Antar Bandyopadhyay, Krishanu Maulik and Rahul Roy all of whom work at the work at the Theoretical Statistics and Mathematics Division of the Indian Statistical Institute. A copy of the article titled, "*A Hitchhiker's Guide to Electronic Voting Machines and VVPATs*" published in *The Wire*,on 18th April, 2019, is annexed herewith as **Annexure R10 (Pages 116 to 119).**

DEMOCRACY PRINCIPLES

32. That the aforementioned difference between domain experts in the same fields on the issue of sanctity of EVMs and the usage of statistics to determine the correct number of VVPATs to be cross verified only shows that the experts don't agree with each other. The common citizen

has no recourse to independently verifying that his vote has been 'recorded as cast' and 'counted as recorded'. The citizenry is being asked to blindly put it's faith in verification given by domain experts when the domain experts even from the same institutes can't agree with each other.

33. It is in this context that the underlying principle of judgement dated 03.03.2009 of the Second Senate of Germany which ordered the discontinuation of the use of EVMs there is important. In view of the public nature of elections; the court held that, "*it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of results reliably and without special expert knowledge.*" A copy of the judgement dated 03.03.2009 of the Second Senate of Germany is annexed herewith as **Annexure R11 (Pages** 120 **to** 156 **)**.

34. That it is in the aforementioned circumstances that the Committee headed by Hon'ble Justice (Retd.) Madan B. Lokur has reiterated certain basic principles which must govern democratic elections which are as under:

- The voting process should be transparent in a manner that the general public can be satisfied that their vote is correctly recorded and counted.
- The voting and counting process should be publicly auditable.
- Ordinary citizens should be able to check the essential steps in the voting process. If special expert knowledge is required then all should be able to select their own experts.

- There should be verifiability in the counting of votes and ascertainment of the results reliably without too much special knowledge.
- An election process should not only be free and fair, but also be seen to be free and fair.
- Election Commission should be in full control of the entire voting process, and the public at large should be able to verify.
- Electronic processes, if they are to be used for voting, should be in sync with changing technologies and technological practices, and be subject to public scrutiny/examinability

35. That the stand of the Election Commission that it is not bound by these basic principles and is only bound to conduct the elections in terms of the statutes is misconceived as free, fair, and credible elections and elections that are *seen* to be free, fair, and credible goes to the root of the elections and their legitimacy.

36. That the Election Commission of India has submitted that the only statutory provision for cross verification of EVMs is Rule 56(D) (4) of Conduct of Election Rules, 1961, (introduced vide gazette notification dated 14.08.2013) which provides for cross verification if any candidate or his agent makes an application to the concerned returning officer and who may direct so for reasons to be recorded in writing by him and in case of a difference, the VVPAT count is to prevail over the EVM count. Importantly, *vide* instructions dated 11.10.2017, the ECI on it's own directed that EVM will be cross verified with VVPAT in one (1) randomly selected polling station per assembly constituency.

This shows that Election Commission has inherent power to direct cross verification of more VVPATs with EVMs and nothing in law restrains them from doing so. Thereafter, this Hon'ble Court increased the number of VVPATs to be cross verified with EVMs to five per assembly constituency in *Chandrababu Naidu* showing there is nothing in law to restrain this Hon'ble Court from increasing the number of VVPATs to be cross verified with EVMs. In short, there is no restraint on either the Election Commission or this Hon'ble Court to grant the petitioners prayers.

37. Lastly, the contention of Election Commission of India that there is no fundamental right in voters to verify that their vote has been 'recorded as cast' and 'counted as recorded' is incorrect. Free and fair elections have been held by this Hon'ble Court to be part of the Basic Structure. Inheres within 'free and fair' elections the ability to verify that the elections are in fact 'free and fair'.

38. Prayed, Accordingly.

IDENTITY THE EXECUTANT/DEPONENT WHO WAS SIGNED IN THE PRESENCE OF

Association for Democratic Reforms ADR New Delhi

DEPONENT

VERIFICATION

I, the above named deponent, do hereby verify that the contents of the above affidavit are true and correct to the best of my knowledge and belief, no part of it is false and nothing material has been concealed therefrom.

The Seal of the Oath Commissioner Sl. No. 64/2023 B.P. YADAV App. By Delhi High Court Period: 15.07.2023 to 14.07.2025 Supreme Court of India, New Delhi-1

Verified at N. Delhi on this 18th day of October, 2023.

CERTIFIED THAT THE DEPONENT Shri/Smt./Km. Jagdeep Chhokar S/o W/o D/o ..... R/o ..... aged about ..... Identified by Shri/Smt. Prashant ..... has solemnly affirmed before me at New Delhi on 18.10.23 as Sl. No. ..... that the contents of the affidavit which have been read & explained & are true & Correct to his/her Knowledge.

Association for Democratic Reforms ADR New Delhi

DEPONENT

Count All VVPAT Slips, Make Info on EVM-VVPAT Public: Ex-CEC

28 Dec 2020, 6:32 PM IST, Poonam Agarwal, *The Quint*

"I would say VVPAT slips should be counted 100 percent. Then, questions are raised on the amount of time taken. Number one, time should not matter, credibility should.": SY Quraishi, former Chief Election Commissioner of India

The former Chief Election Commissioner SY Quraishi who had always defended the Electronic Voting Machine (EVM) and the Voter Verifiable Paper Audit Trail (VVPAT) systems – told **The Quint** that the Election Commission of India (EC) should count 100 percent paper slips rather than EVM votes.

The Quint has reported a series of articles highlighting EVM-VVPAT vulnerabilities and the EC's lack of transparency in addressing the issue.

Here is the full interview with SY Quraishi.

Due to lack of transparency and vulnerabilities of the EVM voting system, there is a demand for ballot paper voting. What do you have to say?

Returning to the ballot paper would be a step backward. I would say, VVPAT slips should be counted 100 percent. Then, questions are raised on the amount of time taken. Number one, time should not matter, credibility should. But, it should not even take time, as I have checked with people who have been conducting the VVPAT election. Counting one VVPAT slip from one machine takes about 20-25 minutes and the EVM takes the same time. We should not dispense the EVM as it is essential, it should stay. (The VVPAT) is just a 3-inch slip on which one vote is mentioned – either candidate A, B or C. It is much easier to count. So, (the EC) should try it out.

Why is a cloak of secrecy maintained over the EVM-VVPAT? Because, as per cyber experts, the source code and the component used in the EVM-VVPAT should be made public.

I would like to say, and it was my attitude even then (when I was the Chief Election Commissioner) that anybody who is questioning the EVM shouldn't be treated as an anti-national or an enemy. You have to treat him as a friend. If you point out some flaw, which I had not noticed, and on the basis of which I get the EVM-VVPAT examined, you are actually doing me and the nation a favour by improving the system. So, all those who are questioning the EVM-VVPAT should be brought onboard and should provide proof rather than (the EC) looking down on them and treating them as hostile people, which is wrong.

The Election Commission should not maintain secrecy. It should be transparent. The EC is like a glasshouse, and everything should be visible to the people. I would suggest that everything (related to EVM-VVPAT) should be out in open and nothing should be held back.

Do you think the EC is not addressing concerns related to the EVM-VVPAT?

I have been cautioning the EC about one thing – when a political party is doubting our system and the machine, it is easy for us to call them and persuade them to accept our point of view. But, once it percolates into the public's mind, it is impossible to change their minds. Unfortunately, what we see now...I am on social media and every time I open it, 10 people pounce on me, asking about my opinion on the EVM. Any suspicion in the public's mind about the EVM is very unfortunate. The EC should be concerned about it, and it should do everything to dispel such notions.

Is it correct to declare election results on provisional data?

To say that the exact figures (of votes polled or counted) will be known after a few days is wrong and unacceptable. When the polling is over, say 650 votes have been cast in a machine. That number is sacrosanct and known to everybody. Everybody knows that this

particular machine has 650 votes. So, the polling data is known by the evening. And the counting day data is known as soon as you open the machine. The figures are there, and they are exact. To say that they are tentative is absolutely not understandable to me.

What do you have to say about some of the crucial matters related to the EVM-VVPAT that are pending in the Supreme Court?

Why should the Supreme Court decide about these discrepancies? A detailed statement from the EC should have been good enough. What surprises me frankly is that why is the SC taking so long? These issues are of national importance, and our democracy is dependent on them. And the SC taking so long on such cases is another cause of concern. I had always said that the SC is the guardian angel of democracy and the EC, but this is something I used to say earlier. However, some cases of this nature, like statistics and electoral bonds, have been pending for years – that is not desirable or a happy situation at all.

Do you think the functioning of the EC is being questioned?

Not that there were no mistakes in our time. Eleven million people were conducting elections. Somebody somewhere will make a mistake. Any question mark on the EC is a matter of national concern. The person to be concerned about it should be the Commission itself, and they should introspect on why people are raising questions and take corrective measures as well. The trust of the people and the (almost) blind faith we had in our time has eroded a bit because the EC is not prompt in its communications.

SOURCE:
https://www.thequint.com/news/india/election-commission-of-india-count-all-vvpat-slips-make-info-on-evm-vvpat-public-ex-cec#read-more, accessed 14.10.2023

Prashant Bhushan

(TRUE COPY)

ANNEXURE: R2

Electronic Voting Machine and VVPAT: EC is misleading that Private consultants in ECIL are not involved in EVM checking during LS & Assembly Elections

03 Aug 2019, 3:11 PM IST, Poonam Agarwal, *The Quint*

Video Editor: Vishal Kumar

The Election Commission of India has always maintained that no private company or outsourcing in any form is involved in the election process. But **The Quint**'s investigation has found this to not be true.

An RTI in **The Quint's** possession shows that the Electronics Corporation of India Limited (ECIL), a PSU that manufactures EVMs and VVPAT machines, engaged private engineers as "consultants" and that these private engineers have worked with the Election Commission in Assembly Elections since 2017 and even in the 2019 Lok Sabha election.

Their job was extremely sensitive – to check and maintain EVMs and VVPATs, starting from First level Checking (FLC) right up till and including the Counting Day, which means they had easy access to EVMs through the course of the elections.

ECIL engaged these private engineers for the Election Commission from a Mumbai-based private company called **M/s T&M Services Consulting Private Limited.**

the quint

ARE EVMS & VVPATS IN SAFE HANDS?

Private Engineers Employed 'On Contract' During Elections

Election Commission of India

Employed

Electronic Corporation of India Limited (ECIL)
(EVM & VVPAT manufacturer)

Employed

T&M Services Consulting Pvt Ltd

Employed

Engineers as 'Private Consultants'
Their job – Check, program & maintain EVMs & VVPATs in Assembly & Lok Sabha elections

BUT WE WERE NOT TOLD!

ECIL engages private consulting engineers from a Mumbai based private company T&M Services Consulting Private Limited(Photo: Shruti Mathur/The Quint)

When we checked with the Election Commission, the body's reply was,"No private company was engaged to provide engineers by BEL & ECIL."

Clearly, the Election Commission is hiding information and misleading the public. Why?

An RTI about engaging private engineers was filed with ECIL in the context of the 2017 Uttarakhand Assembly Elections by a lawyer named Amit Ahluwalia.

The Mystery 'Consultant' Firm

ECIL's RTI reply said, "ECIL is engaging skilled and semi skilled 'Consultants' through a single authorised manpower supply agency, **M/s T&M Services Consulting Private Limited**."

ECIL confirmed that close to 50 private consulting engineers were used to check EVMs during the 2017 Uttarakhand Assembly elections, and that only eight regular employees of ECIL were involved.

We spoke to some of the 'consultant' engineers, and some even confirmed to The Quint that they had been deputed for the 2019 Lok Sabha Elections… once again to handle EVMs and VVPAT up until and including the Counting Day.

It's remarkable that part of the private consulting engineers' job was to upload key details like party symbols and candidates' names on the EVMs and VVPAT, for which they had access to these machines for 15 days before polling.

- Were these engineers vetted by the Election Commission? We don't know!

- The company, T&M Services Consulting, which provided these engineers – was it vetted by the Election Commission, at least? We don't know that either!
- What we do know and can say is that the entire election process might have been compromised!

Free & Fair Elections Compromised?

The Quint has found out that about this matter, the Election Commission hasn't just misled the public, but even one of its own former bosses!

Former Chief Election Commissioner Dr SY Quraishi has told **The Quint** that in 2017, he heard allegations that the sensitive task of handling EVMs was being outsourced during Assembly elections in 2017. On reaching out to the EC, Quraishi says he was assured by EC officials that only in-house engineers had checked EVMs and VVPAT during those elections.

Quraishi had even tweeted about it in November 2017, going as far as to even attach the guidelines EC had shared with him, which said:

“Only engineers of BEL/ECIL, who are on their payroll, are deployed for FLC (First Level Checking) of elections.”

And yet, ECIL’s RTI reply concedes that they *did* use private engineers during the Uttarakhand state elections – something the Election Commission continues to deny!

We ask: Why this contradiction?

How can the EC *not know* whether ECIL is engaging a private company for engineers or not? In national interest, in their role as guarantors of free and fair elections, they *have* to know. And they are obliged to tell you, the voter, as well!

ECIL and T&M Services Consulting have not yet responded to our queries. We will update this story when they do.

(At The Quint, we are answerable only to our audience. Play an active role in shaping our journalism by becoming a member. Because the truth is worth it.)

Read Latest News and Breaking News at The Quint, browse for more from news and india

Topics: EVM EVM Expose Lok Sabha elections 2019

Published:

Viewed using Just Read
Report an error

SOURCE:
https://www.thequint.com/news/india/pvt-consultants-had-evm-vvpat-access-why-is-the-ec-denying-it#read-more

Prashant Bhushan
(TRUE COPY)

Concerns with the current EVM and VVPAT system and recommendations for improvement

1 Concerns with EVM+VVPAT

1. In a stand-alone Electronic Voting Machine (EVM) without Voter-Verified Paper Audit Trail (VVPAT), where votes are recorded electronically by press of a button and the voter cannot examine what has been recorded, **there is no way to provide a guarantee to a voter** that her vote is *cast as intended* (recorded correctly in the EVM), *recorded as cast* (what is recorded in the EVM is what is collected in the final tally) and *counted as recorded*. This casts doubts on a purely EVM based system.

2. It is well known that establishing the correctness of a system as complicated as an EVM is a computationally intractable problem. It is also well known that testing is never adequate to establish the correctness of an EVM, and tests can detect only a small fraction of possible software or hardware errors (follows a common maxim that **tests do not constitute a proof of correctness**). Further, **pre-determined and preset test patterns are inadequate for verification of the integrity of an EVM**.

3. If the correctness of an EVM cannot be established then it is impossible to predict whether an EVM can be hacked or not, or whether all EVMs used in an election are identical in functionality. In particular, **that an EVM has not yet been hacked provides no guarantee whatsoever that it cannot be hacked**. Thus, **elections must be conducted assuming that the electronic voting machines may possibly be tampered with**.

4. Using VVPAT is one possible way to make the voting system auditable. Using VVPAT a voter can in principle verify that her vote is *cast as intended*, and a suitably designed end-of-poll statistical audit can possibly determine that the collection and counting are correct. **The electronic and paper records can be used to cross check the integrity of each other.** This, however, is crucially dependent on the following requirements:

   (a) **The VVPAT slips should be counted before declaring the results**, and used to audit the electronically determined results. **Currently, this is not the case**.

   (b) The **VVPAT system should be made truly voter-verified**. The correct VVPAT protocol would be to allow a voter to approve the VVPAT slip before the vote is finally cast, and to provide an option to cancel her vote if a discrepancy is noticed. This also requires a clear protocol for dispute resolution if a voter complains that a VVPAT printout is incorrect. **The ECI's current VVPAT system is not truly voter-verified** because it does not provide the necessary agency to a voter to cancel her vote if she thinks it has been recorded incorrectly. Also, in case the voter raises a dispute, there is no way for her to prove that she is not lying. As such, penalizing a voter in such a situation is incorrect.

2 Recommendations

1. **EVMs cannot be assumed to be tamper-proof**. The electronic voting system **should be redesigned to be software and hardware independent in order to be verifiable or auditable**. This does not imply that software or hardware cannot be used, but that the correctness of the election outcome cannot be entirely dependent on the assumption of their working correctly.

2. The VVPAT system should be **re-designed to be fully voter-verified**. The voter should be able to approve the VVPAT printout before the vote is finally cast, and be able to cancel if there is an error. It is well understood in literature that **this cannot be achieved by an additional electronic Cancel button**. If the first button cannot be trusted then neither can be the second. The only way the VVPAT slips can be truly voter-verified is if a voter is able to obtain the VVPAT slip in her hand and cast it into a box or discard it with her own agency. There may be the concern that a malicious voter may try to discredit the system by not casting a VVPAT or by casting a bogus one. This risk can be mitigated by requiring that the voter folds the VVPAT slip in the privacy of the booth, comes out and casts the VVPAT in a ballot box kept in full

public view in front of polling agents and poll officials. They may possibly verify that a genuine VVPAT slip is being cast by checking a predesignated mark on the outside of the fold.

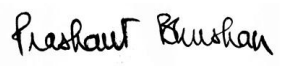
3. The integrity of the VVPAT slips and the EVM machines during the entire time after polling and before counting and auditing must be ensured in a manner that is verifiable by all (and especially the candidates). There should be no trust requirement on the custody chain.

4. **There must be stringent audit of the electronic vote count before the results are declared**. The **audit should not be based on ad hoc methods but by counting a statistically significant sample of the VVPAT slips according to rigorous and well-established statistical audit techniques like the Risk Limiting Audits (RLA, used in many elections world-wide)**, which guarantee that the declared outcome matches the one that would have been determined with a full manual count of the VVPATs. Such RLA may in some cases -- depending on the margin of victory -- require a full manual counting of VVPAT slips. **Moreover, the entire nation should not be treated as one population for the statistical audit. Since election results are declared at the granularity level of constituencies, it is important that there should be independent statistical audits for each constituency.**

5. **There should be legislation to decide what is to be done if the audits reveal a problem**. The amendments to the Representation of the People Act (RPA) suggest that in such cases the VVPAT count should be considered as the correct one, which appears to be reasonable.

6. There is a definite need to move away from certification of voting equipment and processes and demonstrate – using RLA, or a full manual count of the VVPATs -- that the outcome of an election is correct irrespective of machines and trust requirements on custody chains of EVMs.

7. Finally, the voting system design should be subjected to independent (of the government and ECI) review and the integrity of the election process should be subjected to independent audit. **The findings should be made public**. In particular, all design details should be transparent and publicly available.



(TRUE COPY)

ANNEXURE: R4

DEPOSITION ON: ELECTRONIC VOTING AND THE INDIAN EVM

20 April 2020

To,

Citizens' Commission on Elections, India

Dear Chair Justice (Retd.) Lokur, Vice-Chair Habibullah and Other Members of the Commission,

We are election integrity, computer security and computer science researchers with hundreds of years of collective experience. We provide this deposition on:

(a) Compliance of electronic voting with the principles of democracy and

(b) EVM/VVPATs before and during polling, storage, counting and declaration of results.

The content of the deposition is summarized as follows.

ELECTRONIC VOTING AND THE PRINCIPLES OF DEMOCRACY

An accurate and incorruptible voting process provides legitimacy to elected representatives and is hence essential for a healthy democracy. Transparency is a key factor in achieving these goals; aspects of an election that may be observed and independently-verified by the public will naturally be viewed as accurate and incorruptible.

Electronic counting mechanisms—whether implemented in computer hardware and firmware as in Indian EVMs, or software as in western electronic voting systems—are not transparent to the voter, who does not know whether the vote was correctly recorded or counted. Internet access is not the only way to manipulate electronic voting machines; they provide a long time window—over the cycle of design, implementation, manufacture, testing, maintenance, storage and deployment—for insiders or criminals to attempt other means of access. The EVM is a computerized system and its internal logic can be changed by someone with physical access to the machine.

While one may publicly test an electronic voting system for some known problems before use, there are at least three challenges with testing. First, it is not possible to know every vulnerability. Second, and relatedly, it is not possible to determine how a computer software or hardware module will perform in all circumstances. Hence, even for each known vulnerability, it is not possible to fully test that an electronic voting system will function as desired in each possible scenario. Third, computerized systems, such as the EVM, can be programmed to determine when they are being tested and to behave as expected during the test. Thus, while one should test as extensively as possible, testing can only reveal some

problems. The absence of problems during testing does not mean that problems do not exist.

For the above reasons, no electronic voting machine, including the Indian EVM, can be assumed tamper-proof. Many countries—and even individual hackers—have the technical expertise to manipulate voting systems. The EVM is no exception. The vulnerabilities of electronic counting motivated France and The Netherlands to use paper ballots and hand count their recent elections. There are reports that Russia tried to change the 2014 election totals in Ukraine and to access voter databases in the 2016 US election.

Knowing that testing is not sufficient, what additional precautions can we take? While voters cannot observe the internal counting mechanism of an electronic system, the principles of public observation can and should be applied to elections that rely on electronic technology. Best practices require that the use of an electronic voting system be accompanied by the generation and secure curation of a voter-verified paper audit trail (VVPAT). After the election, in addition to public audits of all election processes, the paper record must be publicly audited to verify the election outcome. These public audits provide the counterweight to the vulnerabilities of electronic counting mechanisms.

In summary, elections relying on electronic voting machines should be conducted assuming the machines can be tampered with. Assurances from any official entity that the process or technology is tamper-proof are not sufficient. Voters and losing candidates should not have to trust an opaque machine and its counting mechanism, or an insider design, manufacture, testing and maintenance process. Every part of the election process and the technology should be open to examination and analysis by the candidates and the public. Transparency in design, implementation and use; an openness to the incorporation of ideas from the latest results in computer security; independent security testing of the design and implementation by experts and its feedback into the design cycle; education of the public on these aspects; full observation of the election process and manual audits of the VVPAT slips are all essential for high integrity elections that rely on electronic voting machines.

THE INDIAN EVM, VVPATS AND ELECTION PROCEDURES

The Indian EVM is interesting because its design is far simpler than that of other electronic voting machines. In India, it has greatly increased the efficiency of vote counting and facilitated enfranchising voters in remote areas. It has also made ballot box stuffing much harder. Pre-election procedures are, by and large, designed to be transparent and fair. **However, this is not sufficient to ensure high integrity elections.**

We are not aware of any evidence that any elections using Indian EVMs were rigged. However, the vulnerability of a fully-electronic vote counting mechanism is significant. Attackers can be sophisticated enough to avoid detection, and the absence of evidence does not imply that election integrity can be assumed. It is not sufficient to rule out some

specific attacks, because other attacks could be discovered by those who wish to meddle with elections. The Election Commission's excessive reliance on secrecy of design and the obviously false claim that the machines are tamper-proof greatly diminish the trustworthiness of the electoral process. The following changes can improve trustworthiness by increasing transparency:

1. EVM design and implementation, as well as the results of both software and hardware verification, should be **public and open to full independent review**. Reports from independent experts should be made available to the public, and the important vulnerabilities discovered should be addressed as part of a regular public process with comments from the public as well as experts not involved in the review.
2. A Voter Verifiable Paper Audit Trail (VVPAT) should be generated for **every EVM in every election**. The printed VVPAT slips should be stored securely and separately from the EVMs. The storage boxes should be sealed in the same manner that EVMs are sealed, with signatures from observers representing all candidates.
3. **Voters should be allowed to verify the printed VVPAT slip before the vote is cast**. The use of a paper trail can greatly enhance the integrity of an electronic voting system. VVPAT slips are, however, weaker than paper ballots because paper ballots exactly represent the intended vote, but the VVPAT slip does so only if it is verified by the voter. **The Indian VVPAT system does not allow the voter to verify the slip before the vote is cast.**

   The correct VVPAT protocol is to allow a voter to approve the VVPAT slip before the vote is cast, to cancel her vote if there is a discrepancy, and have the opportunity to vote from another machine. Such a protocol should be implemented with Indian EVMs and VVPATs.

   Additionally, it is virtually impossible to determine whether a voter reporting a discrepancy is lying, because the EVM can behave differently when being observed. Stringent punishment for voters unable to prove a reported discrepancy between the VVPAT slip and the vote is counterproductive in this scenario.
4. It is heartening that the recent Indian general election was carried out with full VVPAT capability and that VVPAT audits were carried out. However, the results of the audit were confusing and not easily available to the public. Additionally, auditing a fixed number of EVMs per constituency is not sufficient to verify elections with narrow margins. A robust, well-designed audit can provide considerable confidence in the outcome, and statistical principles would dictate when a full hand count would be required. Subtle differences among audits can result in a significant difference in the ability to detect problems. For this reason, **best practices in the design of robust election audits should be followed, and expert advice on their design sought**.
5. **Legislation** will be needed on what to do when the audit reveals an outcome different from that declared by the EVMs. Legislation on how/when/whether a candidate may

request a full manual count independent/instead of the audit would need to be developed, or existing legislation modified.

6. The use of risk-limiting audits using current EVMs, and end-to-end-independently-verifiable (E2E-V) techniques for future EVMs, may be explored.

If recommendations 1-5 above are followed, it may not be necessary to go back to paper ballots. If the VVPAT is not strengthened through improved voter-verification, secure storage, robust audit and supporting legislation, however, the vulnerabilities of the EVM will continue to pose a serious problem to election integrity and paper ballots could be preferred.

Please find, on subsequent pages, details on the above comments and short biographies of the signatories. Should you have additional questions, we would be happy to answer them. Please send them to Prof. Poorvi L. Vora, poorvi@gwu.edu.

Signatories

Note that affiliations below are included for identification purposes only and do not reflect the view of the signatories' employers or collaborators.

Poorvi L. Vora, (poorvi@gwu.edu), George Washington University, Washington, DC, USA

Alok Choudhary, Northwestern University, Evanston, Illinois, USA

J. Alex Halderman, University of Michigan, Ann Arbor, Michigan, USA

Douglas W. Jones, University of Iowa, Iowa City, Iowa, USA

Nasir Memon, New York University (Brooklyn), New York, New York, USA

Bhagirath Narahari, George Washington University, Washington, DC, USA

R. Ramanujam, Institute of Mathematical Sciences, Chennai, India

Ronald L. Rivest, Massachusetts Institute of Technology, Cambridge, Massachusetts

Philip B. Stark, University of California, Berkeley

K. V. Subrahmanyam, Chennai Mathematical Institute, Chennai, India

Vanessa Teague, Thinking Cybersecurity, Australia

DETAILED DEPOSITION

1. **Uniqueness of the Indian EVM:** The Indian EVM has an interesting design because it relies largely on hardware and firmware, unlike other electronic voting machines which are software-intensive. Additionally, it is a single-purpose machine; this implies that its design could be very simple, allowing for more thorough security analysis. Its prescribed use does not involve connections beyond its sole wired connection to the control unit, and it is not fitted for internet or other network access, including wireless access. The procedures used immediately pre-election are remarkably public. These features could serve to strengthen the integrity of elections run using Indian EVMs.
2. **Vulnerabilities in computerized counting:** Yet, no computerized vote counting device can be guaranteed to be tamper-proof. The Indian EVM relies on the implementation of computer logic in computer chips and circuitry rather than on hundreds of thousands of lines of computer software code. The chips were intended to be read-only—once manufactured to perform a certain computational task, the chips cannot be reprogrammed to perform another. They can, however, be replaced by other chips at any time in the long cycle of use of the EVMS. Further, the machines can contain undetected errors or intentional changes to the circuit designs at the time of manufacture.
3. **Two plausible attacks:**
    - Wolchok *et al* (2010)[1] describe and demonstrate the placement and use of a dishonest display board with a built-in wireless receiver controlled through wireless signalling. In the absence of wireless instructions, it will behave honestly, displaying the correct vote totals.
    - In response to an earlier announcement by the Election Commission (EC) inviting the public to demonstrate that EVMs can be hacked, Amaldev[2] describes the use of a small specially-designed device at one end of the cable connecting ballot and control units. While the Wolchok *et al* attack would need to be carried out before the device is sealed, the Amaldev attack can be carried out even after the device is sealed.

---

[1] Scott Wolchok, Eric Wustrow J. Alex Halderman, Hari K. Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp "Security Analysis of India's Electronic Voting Machines" (video) *Proc. 17th ACM Conference on Computer and Communications Security CCS '10*, Chicago, October 2010. The display board, which contains the circuitry required to display the vote counts provided to it by the electronic counter, can be replaced by a dishonest display board at any time before the machine is first sealed for a particular election. It can then also be used in future elections. The dishonest display board contains circuitry to receive wireless instructions from the attacker, and to calculate new vote totals so as to provide the attacker's favorite candidate a win while arousing minimum suspicion.

[2] V. Amaldev, "How to Hack Indian EVMs", 30 April 2017.

4. **It is not about specific vulnerabilities**: Every so often one hears about a "new" vulnerability. For example, an RTI filing revealed in 2019 that the micro-controller chip used in EVMs is not one-time programmable[3] as claimed by the EC. The public does not know how to evaluate this risk to election security. On the one hand, there is little information in the public domain on the design of the Indian EVM[4], and it is not possible to independently verify the reassurances of the EC. On the other hand, the EC's case about the credibility of the EVM has been based on "trust us"[5], yet this is an example of an EC claim that has been proven to be false.

   The issue of EVM security has been made into a patchwork of known problems and whether these are being protected against. Every time a new problem comes to public view, especially when it is counter to an EC claim, public trust is diminished. Such a situation is particularly volatile and not conducive to trustworthy elections. A more stable scenario arises if election protection depends on public designs, processes and audits.

5. **Voting machine designs should be public**: It is not uncommon for computer security experts to miss vulnerabilities in their own designs[6]. For this reason, it is recommended that the design and implementation of any computerized voting system be widely observed and examined on a planned schedule. This makes it more likely that vulnerabilities are detected in the public domain, by experts, rather than left for detection by those wishing to do harm[7]. Once discovered, the vulneabilities can be addressed in a planned manner as well.

6. **Little transparency in EVM design:** The EC is relying on the secrecy of the design to

---

[3] Venkatesh Nayak, "What the EC Is Hesitant to Tell the Public About EVMs and VVPATs", The Wire, 22 May 2019

[4] The only information on the detailed design available is from statements from the EC, for example, press notes on 16 March 2017 and 8 August 2009 and the paper by Wolchok et al. Information on procedures is available through explanatory videos, such as, for example, EVM Training Film dated 10 March, 2014 and additional detailed documents.

[5] See, for example, (b), (d) and (f), section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding". In the same press note, the EC says: "The Election Commission would like to underline that it always had a firm conviction and complete satisfaction that EVMs could not be tampered with. Its faith on the machine has never wavered through the conduct of elections in the last many years".

[6] For example, the original Needham-Schroeder public key protocol (1978) is vulnerable to a man in the middle attack; one of the simplest attacks on the Indian EVM described by Wolchok et al is a man in the middle attack.

[7] As an example of transparency improving the design of security technology, the National Institute of Standards and Technology (NIST) held public competitions for the Advanced Encryption Standard (AES) block cipher and the Secure Hash Algorithm (SHA-3) in 1997 and 2007 respectively. AES and SHA-3 are cryptographic standards underpinning secure electronic commerce, internet banking and all online international financial transactions. Designs were solicited in a public competition; experts from all over the world submitted entries which were published online; experts then attempted to demonstrate security vulnerabilities in the entries; the vulnerabilities thus detected were published online; the final winning designs were chosen based on their security and efficiency.

provide security[8]. Security best practices, however, require the assumption that the design is known by the enemy[9], whether it is public or not.

7. **Independent Review Necessary**: Best practices in election integrity include the engagement of an independent team of experts to perform a security analysis, the results of which are made public. (Note that independent EVM testing as currently performed does not include security testing/analysis.)

   For example, in 2007, the Secretary of State, California, USA, ordered the Top-To-Bottom-Review, by noted academic and other experts, of all of the voting machine models certified for use in the state. The resulting detailed report on system vulnerabilities was made public, and action was taken against systems that were found to be insecure.

   Every time the EC has invited examination of Indian EVMs, however, the examination has been severely limited[10], preventing true security analysis and missing the opportunity to educate the public on the strengths and vulnerabilities of its voting technology.

8. **Technical checks and balances can be circumvented:** The EC points to technical reasons why the published attacks are not possible, and to procedures in place that would detect the attacks. These are useful and serve the purpose of providing some deterrence. They are not, however, sufficient by themselves—in part because they are lacking, and in part because it is not possible to detect all possible attacks.

   - **Functionality Tests and Mock Polls:** There are a number of tests in place to check the performance of the hardware at various stages in the manufacturing and maintenance cycle[11] and later, during First Level Checking (FLC)[12]. Candidate representatives participate in a number of mock polls[13]. However, a competent attacker would manipulate the hardware to detect when it is being tested[14]. Hardware manipulated at time of manufacture or afterward could provide testers

[8] See, for example, (b), (d) and (f), section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding".

[9] For example, Kerckhoffs' second principle states that the security of a system cannot depend on the design being secret; all security arguments must assume that those wishing to break system security would be able to determine the design, even if it is not public. See: Auguste Kerckhoffs, "La cryptographie militaire" *Journal des sciences militaires*, vol. IX, pp. 5–83, January 1883, pp. 161–191, February 1883. Peticolas, Fabien, *electronic version and English translation of "La cryptographie militaire"*.

[10] See, for example, the invitation of 20 May 2017.

[11] See, for example, (c), (e), (g) and (i) in section 7 of the EC's press note dated 16 March 2017, "Credibility of Electronic Voting Machines, Regarding".

[12] See section 9 (a-c) *ibid*.

[13] See section 9 (c, e, g, h)

[14] For example, Volkswagen pled guilty to the development and use of software to detect emissions control testing in its 2L Diesel cars, which used improved emission controls during testing as compared to normal use.

with the results they expected to see, yet perform differently when used in the election[15].

- **Randomization of EVMs:** EVMs are chosen at random for allocation to constituencies and polling booths, after they undergo the FLC and are sealed with special bands and signatures. The randomization procedure is performed in software; this is not a truly random process, but a pseudo-random process, which can be predicted by those who know the randomization algorithm and the parameters used. Additionally, the software generating the random numbers can be manipulated to produce a pre-determined set of numbers which will choose a pre-determined set of EVMs for a pre-determined location, and, even, booth. If the computer running the randomization software is on the internet, the randomization software can be manipulated easily. Even if it is not, however, the software can be manipulated without detection during manually-performed upgrades as well as at other times.
- **Candidate Order:** Candidate order is not known till the candidate list is finalized, by which time EVMs are already sealed. This is often provided as an argument for why EVMs cannot be rigged, as an attacker would not know what button would correspond to a vote for his favourite candidate. This is not a problem if the attacker has a means of signalling after the EVMs are sealed, as described earlier. Additionally, even in the absence of signalling, it is not a problem for someone who wishes to simply ensure that the true winner will not win—the dishonest hardware can be designed so as to exchange votes among all the candidates, for example.
- **Cryptography:** Cryptography can be used by one hardware module to confirm that the other module is what it claims to be, to prevent an attacker from inserting a dishonest module. However, the security of cryptography depends on the secrecy of key stored on the module, and this can often be detected through the use of sophisticated equipment by a determined attacker. Also changes in the data before encryption/digital signature and after decryption/verification of the digital signature will not be detected.

9. **EC's procedures can be circumvented:** The precautions of the EC can be circumvented, including by insiders such as maintenance engineers. It is also possible that all processes are not always followed as described (for example, VVPAT checks routinely unearth instances of mock election votes being included in the tally). Many irregularities came to light in the 2019 general election: unused EVMs were transported without security[16];

[15] Instructions to the dishonest hardware could be provided through the use of wireless signalling as by Wolchok *et al*, with the wireless receiver being a part of the dishonest hardware.

[16] Arnab Ganguly, "Uproar as EVMs moved in pvt vehicles; EC says they're unused", Mumbai Mirror, 22 May, 2019.

there was at least one complaint[17] of an EVM serial number not matching at counting time; an RTI filing revealed that 20 lakh EVMs[18] claimed to be delivered by the manufacturers are not in the possession of the EC. These belie the EC's claims of a tamper-proof process.

10. **EVMs cannot be assumed to be tamper-proof**: This is not because of a weakness in the EVM design per se (we do not know the design beyond that reflected in public information), but because no electronic system can be assumed to be tamper-proof. Additionally, the administrative procedures do not prevent all tampering as we have described above.
11. **Best practices require that voting systems be software/hardware-independent[19,20] and elections be evidence-based[21]:** The election process should be designed so that an undetected change in the voting system hardware or software cannot cause an undetected change in election outcome. This can be done through the generation of voter-verified evidence—in the form of paper records of the votes—and evidence that all the procedures were correctly performed[22].
12. **Regular generation and secure storage of VVPAT**: A complete VVPAT (each vote printed on paper) should be generated for each EVM in each election; the records should be stored securely, separate[23] from EVMs. As with secure EVM storage, the storage containers with VVPAT slips should be sealed and signed by representatives of all candidates. The use of paper VVPAT slips is not anywhere near as burdensome as the use of paper ballots, because each VVPAT slip lists a single candidate.
13. **Voter Verification**: Currently, VVPAT printers in India print the vote on a paper slip and display it to the voter for a few seconds, after which the slip falls into a storage container[24]. The voter is required to file an official complaint if the VVPAT slip is incorrect, with stringent punishment for false complaints. However, note that a dishonest EVM can avoid detection after the fact, and can, for example, behave honestly in demo mode. Stringent punishment to the voter in such a situation is

---

[17] Rajesh Kurup, "Urmila Matondkar files complaint over EVM discrepancies at Magathane polling station", Business Line, The Hindu, 23 May, 2019.

[18] Venkitesh Ramakrishnan, "'Missing' EVMs", Frontline, 24 May, 2019.

[19] Ronald L. Rivest and John P. Wack. "On the notion of `'software independence' in voting systems." (2006),

[20] Ronald L. Rivest. "On the notion of `software independence' in voting systems." *Philosophical Transactions of The Royal Society A* 366,1881 (2008) pp. 3759--3767.

[21] P.B. Stark and D.A. Wagner, "Evidence Based Elections", *IEEE Security and Privacy*, special issue on electronic voting, 2012.

[22] Many countries use paper in some form for their elections: 70% of the votes in the 2016 US election had a paper record. Neither Britain nor Germany use electronic voting for general elections. France and The Netherlands both hand-counted their most recent elections.

[23] See, for example, section 7.8.2 "Basic Characteristics of IV Systems", of the Voluntary Voting Systems Guidelines, Version 1 (2005), Volume 1.

[24] See, for example, Voter Verifiable Paper Audit Trail, training video.

counterproductive because it discourages voters from filing genuine complaints (as how can they be proven to be correct?). The correct protocol for generating the VVPAT is, however, as follows[25]: the vote is cast only after the voter has verified the printed slip. If the printed slip is incorrect, the voter cancels the vote and reports the problem, after which she is allowed to vote from another machine if she wishes. **This discrepancy with the correct protocol needs to be rectified if the VVPAT is to be of use in improving election integrity.**

14. **The VVPAT should be regularly audited**: It is not sufficient to generate VVPAT slips that are verified by voters, as the EVM may still record or count the vote incorrectly. The VVPAT slips need to be audited, or cross-checked. Audits involve the public, manual examination of a randomly-chosen sample of the slips to ensure that the announced outcome is correct, and pose a workload far smaller than that of a full hand count. A full hand count is performed if the audit reveals that there is a problem. **The design of a robust statistical audit also requires adherence to best practices, and audits should be designed by experts. Risk-limiting audits are strongly recommended**.

    Audits were performed in the general election of 2020 by cross-checking hand counts of the VVPAT slips with EVM counts. We consider how many EVMs should be cross-checked using India's current approach. Another approach is described by Mohanty et al[26].

    Abhay Bhatt Report: At the request of the Election Commission, Abhay Bhatt of Indian Statistical Institute, Delhi, and others provided a report describing how many EVMs should be cross-checked and why. The report recommends the cross-checking of only 479 EVMs across the country, independent of how many total EVMs there are. It says that, if a fraction of 2% or more of the EVMs *across the country* are faulty, cross-checking 479 chosen at random *across the country* will be sufficient to detect this fact with virtual certainty. This is a correct answer to the wrong question.

    The purpose of the cross-checking is to demonstrate that each constituency was correctly called. For this reason, the computation should be for each Lok Sabha constituency and not the entire country. We should ask how many EVMs need to be cross checked in a constituency to detect, for example, 2% faulty EVMs in that constituency. It is possible that only one constituency had faulty EVMs, but that there was a large enough number to change the outcome. A sample of 479 EVMs may not even include a single EVM from this constituency.

---

[25] "The voting system shall print and display a paper record of the voter ballot selections prior to the voter making his or her selections final by casting the ballot.", from section 7.9.1, page 137, Voluntary Voting Systems Guidelines, Version 1 (2005), Volume 1.

[26] Mohanty, V., N. Akinyokun, A. Conway, C. Culnane, P.B. Stark, and V. Teague, 2019. Auditing Indian Elections, Proceedings of E-Vote ID 2019. Lecture Notes in Computer Science, 11759, R. Krimmer, M. Volkamer, V. Cortier, B. Beckert, R. K¨usters, U. Serd¨ult and D. Duenas-Cid (Eds.) Springer Nature, Switzerland.

Cross-checking 5 EVMS per Assembly Constituency: The current approach of checking five EVMs per Assembly constituency[27] is sufficient to detect malfunctioning EVMs in wide margin contests but will not detect errors in narrow margin contests. For example, if about 1% of the EVMs in a Lok Sabha constituency are faulty, this fact will be detected only one-third of the time. Instead of auditing a fixed number of EVMs, the EC should audit as many EVMs as necessary to ensure that, if the outcome is incorrect, this fact is detected with a high pre-specified probability[28]. Additionally, if mismatches due to mock poll votes are detected, they need to be considered as errors in the cross check. At present, such mismatches are ignored; however, if these errors are made in all EVMs in a constituency, they could change an outcome with small margin and statistical estimates should take this into consideration.

15. **Legislation** will be required to deal with the case when the audit, and subsequent recount, reveal a different winner from the winner obtained from EVM counts. Legislation will also be required to regulate when, and if, a candidate can request a hand count. Best practices suggest that legislation be based on statistical principles, as opposed to the judgment of individual election officials, to the extent possible.
16. **E2E-V EVMs may be considered**: End-to-end-verifiable (E2E-V) voting systems[29] enable voters to independently verify the outcome of an election, without requiring them to trust election technology or election procedures, other than those performed in public on Election Day. It is possible that adding E2E-V capability—or some E2E-V techniques—to EVMs can improve their transparency, though this can only be definitively determined after a study of the constraints and use scenarios of Indian elections. E2E-V capability cannot, however, entirely replace the need for the VVPAT and its audit.
17. **Should paper ballots be used**: If recommendations 5, 7 and 11-15 above are implemented in their true spirit, it does not appear necessary to return to the use of paper ballots. The typical candidate list in Indian elections, as well as the number of voters, is large enough that paper ballots present inefficiencies and difficulty in election administration that can lead to disenfranchisement of voters in remote areas. The EVM, on the other hand, is far more efficient and portable and also helps prevent ballot stuffing. **However, if the VVPAT is not strengthened as described in recommendations 11-15, the vulnerability of EVMs will continue to pose a threat to election integrity and paper ballots may be preferred.**

---

[27] "VVPAT verification: Supreme Court orders counting of paper slips of five EVMs in every constituency", scroll.in, 8 April 2019.
[28] Poorvi L. Vora, "Can We Improve on the Integrity of our Elections?", https://www2.seas.gwu.edu/~poorvi/EVN/VVPAT-Cross-Checking.pdf 20 April 2020.
[29] Josh Benaloh, Ronald Rivest, Peter Y. A. Ryan, Philip Stark, Vanessa Teague, Poorvi Vora, 'End-to-end verifiability", arXiv:1504.03778, 15 April, 2015.

Biographies

Alok Choudhary is the Henry and Isabel Dever Professor of Electrical Engineering and Computer Science at Northwestern University. He also teaches at Kellogg School of Management, and is the founder, chairman and chief scientist of 4C Insights. He has received numerous prestigious awards including National Science Foundation's Presidential Young Investigator Award IEEE Engineering Foundation award, an IBM Faculty Development award, and an Intel Research Council award. He is a fellow of IEEE, ACM and American Academy of Sciences.

Choudhary has consulted for many companies including Publicis Group, Vivaki, Southwest, Intel, IBM, SPSS, Teradata, Microsoft, Sun Microsystems, Newsbank, Sony, Portland Group, Lucent, Oliver Weinmen, and Netezza. Alok Choudhary's work has appeared New York Times, Chicago Tribune, The Telegraph, The Investor Business Daily, ABC, PBS and many international media outlets all over the world.

Choudhary graduated with a PhD from University of Illinois, Urbana-Champaign in the field of Supercomputing. He has published more than 400 papers and graduated more than 35 PhDs. He gives talks in many international conferences. His research interests are in computer security, supercomputing, big-data science and algorithms their applications in marketing, medicine, physics, materials and climate understanding.

J. Alex Halderman is Professor of Computer Science and Engineering at the University of Michigan and Director of Michigan's Center for Computer Security and Society. His interests include computer and network security, Internet security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with law and international affairs. Named one of Popular Science's "Brilliant 10" for 2015, his recent projects include ZMap, Let's Encrypt, and the TLS Logjam and DROWN vulnerabilities.

A noted expert on electronic voting security, Prof. Halderman helped demonstrate the first voting machine virus, participated in California's "top-to-bottom" electronic voting review, and demonstrated vulnerabilities in India's EVMs. When Washington DC invited the public to test its pilot Internet voting system, Halderman demonstrated security vulnerabilities that would allow malicious entities to add and replace votes. His analysis received national attention and resulted in DC's decision not to use the system. With Vanessa Teague, he demonstrated serious security vulnerabilities in the iVote Internet voting system used by New South Wales, Australia.

In 2015, Halderman received the Alfred P. Sloan Fellowship, which is awarded to "early career scientists and scholars of outstanding promise" "in recognition of distinguished performance and a unique potential to make substantial contributions to their field". He holds a Ph.D. from Princeton University.

Douglas W. Jones is a computer scientist at the University of Iowa. Together with Barbara Simons, he published "Broken Ballots: Will Your Vote Count?". His involvement with electronic voting research began in late 1994, when he was appointed to the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems. He chaired the board from 1999 to 2003, and has testified before the United States Commission on Civil Rights, the United States House Committee on Science and the Federal Election Commission on voting issues. In 2005 he participated as an election observer for the presidential election in Kazakhstan. Jones was the technical advisor for HBO's documentary on electronic voting machine issues, "Hacking Democracy", that was released in 2006. He was a member of the ACCURATE electronic voting project from 2005 to 2011. On Dec. 11, 2009, the Election Assistance Commission appointed Douglas Jones to the Technical Guidelines Development Committee, where he served until 2012. Jones received a B.S. in physics from Carnegie Mellon University in 1973, and a M.S. and Ph.D. in computer science from the University of Illinois at Urbana-Champaign in 1976 and 1980 respectively.

Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Polytechnic School of Engineering and director of the Information Systems and Internet Security laboratory. He is one of the founding members of the Center for Interdisciplinary Studies in Security and Privacy (CRISSP), a collaborative initiative of multiple schools within NYU including NYU-Steinhardt, NYU-Wagner, NYU-Stern and NYU-Courant. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior. Memon earned a Bachelor of Engineering in Chemical Engineering and a Master of Science in Mathematics from Birla Institute of Technology and Science (BITS) in Pilani, India. He received a Master of Science in Computer Science and a PhD in Computer Science from the University of Nebraska.

Prof. Memon has published over 250 articles in journals and conference proceedings and holds a dozen patents in image compression and security. He has won several awards including the Jacobs Excellence in Education award and several best paper awards. He has been on the editorial boards of several journals and was the Editor-In-Chief of Transactions on Information Security and Forensics.

Memon is the co-founder of Digital Assembly and Vivic Networks, two early-stage start-ups in NYU-Poly's business incubators.

He is an IEEE fellow and a Distinguished Lecturer of the IEEE Signal Processing Society.

Bhagirath Narahari is the Associate Dean for Undergraduate Programs and Student Affairs and a Professor of Engineering and Applied Science in the Department of Computer Science in The School of Engineering and Applied Science at The George Washington University. Prof Narahari received his PhD in Computer Science from the University of Pennsylvania in 1987, and his Bachelors in Electrical Engineering from Birla Institute of Technology and Science, Pilani. Since 1987 he has been on the faculty in the School of Engineering and Applied Science at The George Washington University. From 1999 – 2002 he was the first Chair of

the Department of Computer Science, and he has been active in undergraduate education with over a dozen years' experience in undergraduate advising, curriculum development and has taught a number of undergraduate courses in Computer Science.

His research interests are in the areas of Software Security, Architecture support for trustworthy computing, Embedded Systems, Computer Architecture, Compiler optimization, Pervasive Computing, and Parallel Computing. Prof. Narahari has published several refereed articles in various areas of embedded systems, security, architecture, parallel processing and computer systems. His current research focuses on compiler, operating system and hardware support for software security, with projects funded by the National Science Foundation (NSF) and Air Force Office of Scientific Research (AFOSR). Prof. Narahari's prior research has been funded by the National Science Foundation, AFOSR, Rome Air Force Labs, NASA, NSA and America Online (AOL), and included research in power-aware computing, embedded systems, optimizing compilers, software systems and specification, and pervasive computing. His research projects have included both fundamental research and software deliverables including an open source research compiler infrastructure for the Intel Itanium processor.

Ronald L. Rivest is the Institute Professor of Computer Science in MIT's Dept. of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and is a leader of its Cryptography and Information Security Group. He is a founder of RSA Data Security and an inventor of the RSA public-key cryptosystem, and a co-founder of Verisign and of Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, voting systems, and algorithms. He is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. He is also on the EPIC Advisory Board.

Together with Adi Shamir and Len Adleman, Dr. Rivest was awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He also received, together with Shamir and Adleman, the 2002 ACM Turing Award and the 2009 NEC C&C Prize. He received an honorary degree from the University of Rome. He is a Fellow of the World Technology Network and a Finalist for the 2002 World Technology Award for Communications Technology. In 2005, he received the MITX Lifetime Achievement Award; in 2007, he received both the Computers, Freedom and Privacy Conference "Distinguished Innovator" award and the Marconi Prize. In 2008, he received an honorary doctorate from the Louvain School of Engineering at the Universite Catholique de Louvain (UCL). In 2010, he was awarded MIT's Kilian Faculty Achievement Award. He has extensive experience in cryptographic design and cryptanalysis, and served as a Director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and as a Director of the Financial Cryptography Association.

Philip B. Stark is the Associate Dean, Division of Mathematical and Physical Science at the University of California, Berkeley. Prof Stark is on the Board of Advisors of the US Election Assistance Commission. He developed the notion of "risk-limiting audits", which are now required by the state of Colorado (C.R.S. 1-7-515) and this work has led to audit-related legislation in California: California AB2023, SB360, AB44. He served on California Secretary of State Bowen's Post Election Audit Standards Working Group. Dr. Stark has published more than one hundred articles and books, served on the editorial board of several scientific journals, and lectured at universities and professional societies in seventeen countries. He has consulted for the U.S. Department of Justice, the Federal Trade Commission, the U.S. Department of Agriculture, the U.S. Census Bureau, the U.S. Department of Housing and Urban Development, the U.S. Department of Veterans Affairs, the California Attorney General, the California Highway Patrol, and the Illinois State Attorney. He has testified to the U.S. House of Representatives Subcommittee on the Census; the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments; the State of California Assembly Committee on Elections and Redistricting; and the State of California Senate Committee on Natural Resources. In 2011, Dr. Stark received the University of California Chancellor's Award for Public Service for Research in the Public Interest.

K V Subrahmanyam is a Professor in the Computer Science group at the Chennai Mathematical Institute (CMI). He has been with CMI since its early days, and has played a pivotal role in establishing it as a premier centre for research and teaching in Mathematical Sciences in India.

His research focus has been on Computational complexity. Since 2004 he has worked at the crossroads of group representation theory, algebraic geometry and computer science, with a view towards understanding hard lower bound problems in computational complexity theory.

He is also interested in combinatorial and continuous optimization, machine learning and cryptography, having taught these courses many times in CMI's graduate and undergraduate programmes. Subrahmanyam did his PhD at the Tata Institute for Fundamental Research, Mumbai and has a PhD degree in Computer Science from Bombay University. He has a B. Tech. in Computer Science from IIT Bombay and an M. S. in Electrical Engineering from Vanderbilt University, USA.

Vanessa Teague is a cryptographer based in Melbourne, Australia. She is the CEO of Thinking Cybersecurity and Adjunct Associate Professor at the Australian National University. Her research focuses primarily on cryptographic methods for achieving security and privacy, particularly for issues of public interest such as election integrity and the protection of government data. She was part of the team (with Chris Culnane and Ben Rubinstein) who discovered the easy re-identification of doctors and patients in the Medicare/PBS open dataset released by the Australian Department of Health. She has co-

designed numerous protocols for improved election integrity in e-voting systems, and co-discovered serious weaknesses in the cryptography of deployed e-voting systems in NSW, Western Australia and Switzerland.

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her research focus has been on end-to-end independently verifiable (E2E) voting systems which enable voters and observers to audit election outcomes without requiring them to rely on the trustworthiness of election technology or unobserved election processes. She has recently also worked on risk-limiting election tabulation audits.

Vora was a member of the team that deployed polling-place, paper-ballot-based, E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011, and of the team that developed remote voting E2E system Remotegrity and accessible voting variant Audiotegrity, used in 2011.

She has worked with the U.S. National Institute of Standards and Technology (NIST) on definitions of desired properties of E2E systems, and on information-theoretic models and measures of voting system security properties. She has been an Associate Editor for the IEEE Transactions on Information Forensics and Security.

Vora has Ph. D. and M.S. degrees in Electrical Engineering from North Carolina State University, an M.S. in Mathematics from Cornell University and a B. Tech. in Electrical and Electronics Engineering from IIT Bombay.

Prashant Bhushan

(TRUE COPY)

Can We Improve on the Integrity of our Elections?

Auditing India's Elections

Poorvi L. Vora
Department of Computer Science, The George Washington University
This draft: 21 April 2020

Abstract: This note describes why the current tabulation audit process for India elections: comparing manual vote counts with declared counts of 5 Electronic Voting Machines per assembly constituency is not sufficient.

The legitimacy of an election is directly related to its perceived transparency by all candidates and voters. For this reason, elections should be evidence-based and provide sufficient evidence to convince the losers and their supporters that they lost.

This writer has previously described how EVMs, like all other computerised or electronic vote-counters, can be tampered with. But, more importantly, all such vote counters are opaque to the public and reduce the transparency of an election. Thus, simply saying "it is so because the EVMs say so and they are tamper-proof" or "we test the EVMs and they are secure" is not sufficient. Voters and losing candidates should not have to trust an opaque machine and its counting mechanism, or an insider design, manufacture, testing and maintenance process.

For example, it is possible that the precautions of the EC are circumvented, including by insiders such as maintenance engineers. It is also possible that all processes are not followed as described (for example, VVPAT checks routinely unearth instances of mock election votes being included in the tally). Irregularities have come to light in the last few days: unused EVMs were transported without security; there was at least one complaint of an EVM serial number not matching at counting time; an RTI filing revealed that 20 lakh EVMs claimed to be delivered by the manufacturers are not in the possession of the EC; another reveals that the micro-controller chip used in EVMs is not one-time programmable as claimed by the EC. These belie the EC's claims of a tamper proof device and process.

It is also not fair to shrug off the issue of EVM security saying that it is always the losers who question EVMs. Rahul Gandhi voiced his concerns about EVMs even as the Congress saw large gains in the 2018 Assembly elections. The BJP itself claimed to be able to demonstrate EVM hacking in 2009 after a major loss in the general election. EVM security has been an issue of concern among various parties since then. And, finally, all the losing parties together represent a large fraction of the voters whose concerns are, by definition, legitimate.

Cross-checking EVMs is important

There is a simple solution to making the election extremely transparent while continuing to use EVMs. VVPAT slips, if securely stored, can be used as evidence and cross-checked to increase the transparency of the particular election. If the cross-checking corroborates the results shown by the EVMs, this would satisfy sceptics that the particular elections were not rigged. And, indeed, those saying EVMs are tamper-proof should not fear such cross-checking; if they are right, it can only buttress their argument. On the other hand, if the cross-checking does not corroborate the results, the VVPAT slips for that Lok Sabha constituency can be manually counted to determine who the true winner is.

The idea is not to fully manually count the election and ignore EVM counts, but to verify that the correct winner has been announced. The cross-checking requires far less effort than a full manual count would. However, if a cross-check fails, then it is best to do a full hand count of that Lok Sabha constituency.

Cross-checking of paper VVPAT slips has often been derided as a step backward and just another predictable distraction drummed up by the Opposition. In fact, it is an important step in ensuring that the results are correct, and in demonstrating this fact to the voters.

How many EVMs should be cross-checked?

At the request of the Election Commission, Abhay Bhatt of Indian Statistical Institute, Delhi, and others provided a report describing how many EVMs should be cross-checked and why. The report recommends the cross-checking of only 479 EVMs across the country, independent of how many total EVMs there are. It says that, if a fraction of 2% or more of the EVMs are faulty, cross-checking 479 chosen at random across the country will be sufficient to detect this fact with virtual certainty.

In response to a petition from the Opposition parties that the then standard of cross-checking one EVM per assembly constituency was not sufficient, the EC used the Bhatt Report to claim that their approach resulted in checking 4,125 EVMs over the entire country and was hence more than sufficient. However, the Supreme Court ordered the Election Commission to increase the number of cross-checked EVMs to five per Assembly constituency in order to assuage the concerns of the petitioners (this corresponds to 20,625 EVMs across the country). The court later turned down another petition by the Opposition parties to count 50% of EVMs per constituency, saying this was not necessary.

Members of civil society have asked for all the VVPAT slips to be counted.

That's a wide variety of recommendations. What should we do now? How many EVMs should we cross-check? Is there a rational explanation that might guide us in our choice?

The Chance of Detecting Incorrect Outcomes with Five Cross-Checks Per Assembly Constituency

The number of EVMs that need to be cross-checked depends on at least two variables.

First, it depends on the fraction of EVMs reporting incorrect counts. A larger fraction is more easily detected.

Second, it depends on what probability of detection is acceptable. If a lower probability is acceptable, fewer EVMs need to be cross-checked.

Using Election Commission data for the 2014 Lok Sabha election and scholarly contributions in the literature, we can make some rough calculations assuming all constituencies are average.

Using number of votes cast and balloting units used in the 2014 election, we estimate that, on average, about 3,024 EVMs are used per Lok Sabha constituency. The current procedures require that five EVMs are cross-checked from each Assembly constituency, which corresponds to about 38 per Lok Sabha constituency.

Table 1 presents approximate probabilities of detecting errors with this level of cross-checking; these numbers are intended to be approximate and we make no claims that they are exact numbers. They do, however, give us a sense of the order of magnitude of the probabilities and illustrate the approach being proposed.

We say that an error is detected if even a single EVM count does not match the hand count, after the hand count has been verified by recounting that batch of slips. Note that if the hand count does not match because some mock poll votes were not zeroed, it is still a detected error which should lead to a hand count of all machines for that constituency. If one wishes to ignore mismatches that are clearly because of mock polls, the number of EVMs that needs to be cross-checked needs to be larger.

Table 1: Chance of Detecting Errors using the Current Proposal of Five Cross-checked EVMs per Assembly Constituency

Misreporting EVMs in a Lok Sabha Constituency	Approximate Chance of Error Detection in that Constituency
25%	Virtually certain
20%	0.9998
10%	0.98
5%	Six of seven (0.86)
2%	One out of two (0.54)
1%	One out of three (0.33)

Comparing These Results to the Claims of the Bhatt Report

Why do the numbers in Table 1 diverge considerably from the Bhatt-Report recommendations (479 EVMs cross-checked across the country will detect a 2% rate of faulty EVMs with virtual certainty)? Table 1 says five EVMs cross-checked per assembly constituency, a number more than 40 times larger than 479, will detect the problem with probability only about a half?

First, the Bhatt report considers a 2% rate of faulty EVMs all across the country, while the above table considers it for a single Lok Sabha constituency. So, when the Bhatt Report assumes 2% EVMs are faulty, that is 543 times as many as are assumed in the table above. If about 16 lakh EVMs were used in the election, the Bhatt Report approach is proposed to detect if more than 32,000 were faulty, or, if roughly more than a crore votes (of about 60 crore cast) were potentially incorrect. It is not being proposed for the detection of fewer faulty EVMs, or tens of thousands of incorrect votes, which would be sufficient to swing a single Lok Sabha seat.

Second, and relatedly, the Bhatt Report does not explicitly say anything about faulty EVMs in a single constituency. It argues that there is no difference among constituencies that would be relevant to the working of the EVM and hence a constituency is not the unit to focus upon. it says the only kind of EVM faults assumed should be assumed to exist countrywide. If there is rigging in the elections, the election to every seat will be rigged by a similar fraction of the EVMs. It says this is because of all the precautionary measures taken by the EC, which prevent individual constituencies from being targeted.

This is a circular argument. The reason we are cross-checking the EVMs is to have a transparent process that does not depend on the EC's assurances, but is verified by the evidence. It is not the public's job to suggest a possible attack on EVM security that the EC will then refute. It is the EC's job to prove, through the VVPAT cross-checks, that the elections were correctly called. In designing the cross-checking process to prove that all went as they assure us it did, they cannot assume that most of it did! They may assume only that which can be verified publicly, such as a VVPAT count.

In a similar incorrect statement, the Bhatt Report claims that previous cross-checks of the VVPAT machines have not resulted in the detection of miscounts, and that this, too, provides statistical evidence that EVMs cannot be rigged. The field of election tabulation audits is well established, and it is understood there that each election is audited separately. It is not the technology that is being audited, but whether it functioned correctly and called this particular election correctly. In fact, the public does not know if the technology has changed between elections, or if existing malicious technology on the EVM has been activated between elections. Evidence from previous cross-checks, on totally different machines for totally different elections, should not be used as evidence for a current election.

The assumption that the unit to focus on is the entire country is a major flaw in the reasoning of the Bhatt Report. As a result, the report has provided the correct answer to the wrong question. Because the purpose of the cross-checking is to demonstrate that each constituency was correctly called, the unit should be a single Lok Sabha constituency.

Third, the Bhatt Report (correctly) says that the number of EVMs to be cross-checked is roughly independent of the total number of EVMs (yes, this is roughly true if not intuitive). Hence we may apply their result to the unit of the Lok Sabha constituency: in order to detect a 2% rate of faulty EVMs in a single Lok Sabha constituency with the same degree of virtual certainty as in the Bhatt Report, one needs to cross-check roughly 479 EVMs ***in that constituency***. (A quick glance at the table provided in the Bhatt Report shows us that the exact number is between 443 and 447, with the difference being due to the smaller number of EVMs in a single constituency compared to those used all over the country.)

Fourth, the converse of the third point above also holds. Five EVMs per Assembly constituency corresponds to an average of about 38 EVMs per Lok Sabha constituency. If 38 EVMs are cross-checked across the country, and the rate of faulty EVMs in the table are rates ***across the country***, the probabilities of detection should be approximately as in our table.

Relationship of Number of Misreporting EVMs to Election Margin

How should we evaluate the number of misreporting EVMs in Table 1? Can the election outcome be correct if, say, 5% of the EVMs misreport?

Observe that one vote moved from the winner to the loser changes the margin by two votes, because the winner's tally decreases by one and the loser's increases by as much.

Consider a simple scenario of two candidates getting most of the votes, and one-fifth of the votes in all the faulty EVMs are moved from winner to loser. Suppose that 10 lakh votes are cast in that constituency, 4000 EVMs used, each recording 250 votes. In this case a misreporting EVM rate of 5% corresponds to 200 misreporting EVMs, moving one-fifth of their votes each, a total of 10,000 votes, from the winner to the loser. This could change the outcome of a race with a margin of 20,000 votes or 2%. Similarly, 10% misreporting EVMs could change an election with a margin of 4% (roughly 40,000 votes in our example).

Assuming that one-fifth of votes are changed per misreporting EVM, we get the following plot for detection probability as a function of margin.

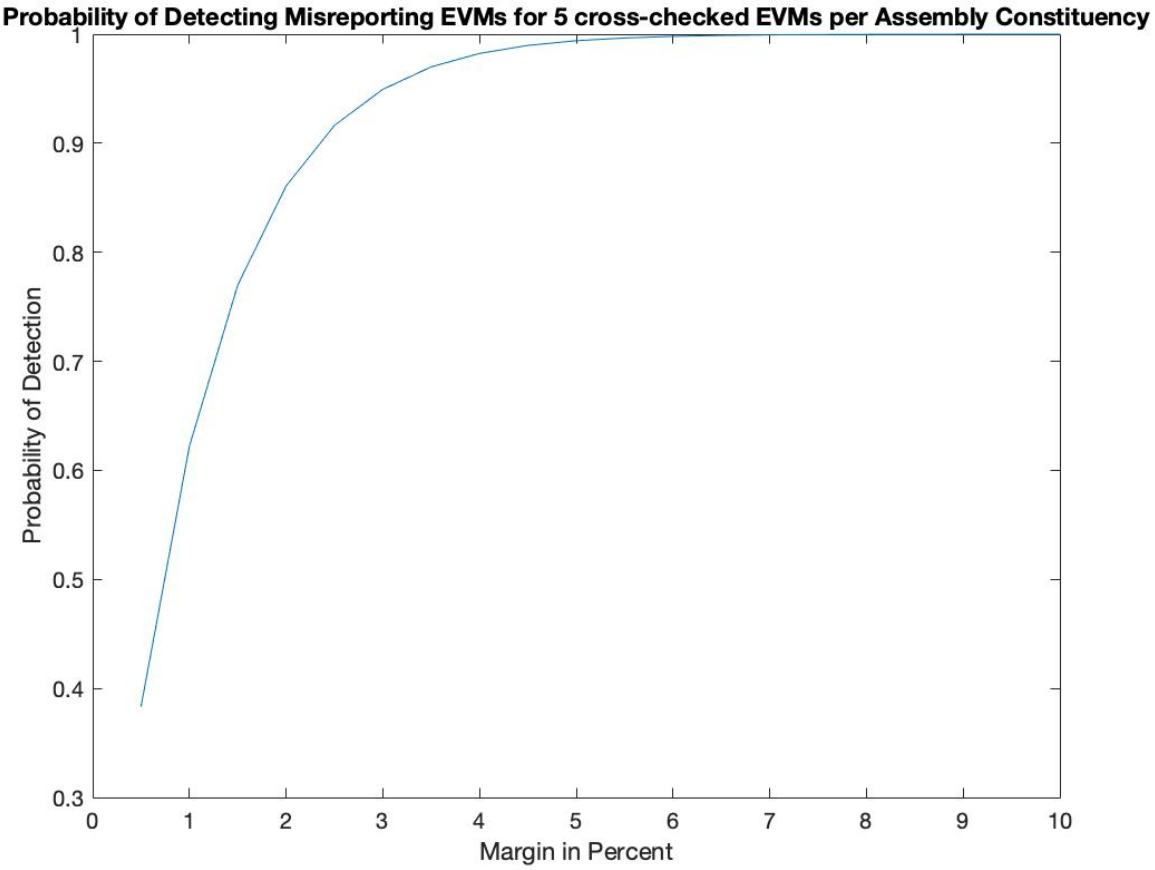


Figure A: Probability of detection as a function of margin when five EVMs are cross-checked per assembly constituency, and one-fifth of the votes in a faulty EVM are flipped from announced loser to announced winner

A brasher attempt to rig the election would change more votes per EVM and result in fewer misreporting EVMs (because each misreports by a greater amount), and a lower probability of detection through cross-checking. However, in such a case, the rigging might be more obvious from the announced tallies, which might appear very different from expected. For example, if all votes in an EVM were for a single candidate because votes for all other candidates were moved to this candidate, this could attract attention and suspicion.

Reasoning about how many EVMs to cross-check

The chances of detection in Figure A are not good enough for contests with narrow margins. How should we improve on our chances of detection?

The correct way to do this is to choose the number of cross-checked EVMs based on the margin of the constituency. If the margin is 10% (corresponding to 25% misreporting EVMs if each changes one-fifth of the votes from the loser to the winner), it is sufficient to check three EVMs per Assembly constituency, or about 20 per Lok Sabha constituency, for a detection probability

of 0.9987. In this case, it is not necessary to cross-check more, and the resources can be diverted towards closer elections.

The following table lists the approximate required number of cross-checked EVMs for some example margins, for a detection probability of at least 0.98 (which is smaller than the detection probability guaranteed by the Bhatt Report, but appears reasonable).

Table 2: Approximate number of cross-checked EVMs required per assembly constituency to detect rigging with probability 0.98 or more in Lok Sabha contests, assuming one-fifth of votes are flipped in faulty EVMs

Margin of Lok Sabha Contest	Number of Cross-Checked EVMs Needed Per Assembly Constituency for Detection Probability 0.98
10%	3
8%	3
4%	5
2%	10
1%	20
0.8%	25

Thus, the smaller the margin, the more EVMs we need to check. This is because fewer EVMs need to be rigged to change the election, and if we don't check a large number, we will miss the few that were rigged.

A more accurate approach than that we have described would take into consideration the variation in number of votes across EVNs. A completely different approach specially designed for the Indian election is described by Mohanty et al.

Other important aspects of the election audit

We can only rely on VVPAT cross-checking if the VVPAT slips do indeed represent the will of the voters.

Currently, there is a heavy penalty for voters who complain that their slip did not represent their vote if the EVM does not demonstrate the same behavior when it is tested by an official. This dissuades voters from complaining. On the other hand, if we accept all complaints, voters may choose to lie to call an election into doubt. One solution is to design the VVPAT machines so that

a voter may cancel her vote if the slip does not represent it correctly and she may vote again on a different machine if available.

The VVPAT slips must be securely stored between vote casting and cross-checking.

The EVMs chosen for cross-checking must be chosen at random; the current proposal of using lottery drawing by candidates and their representatives could serve this purpose.

The proposal to count VVPAT slips for each election is a very good one. It would be more effective for the purpose of checking the election outcome if more EVMs were cross-checked, and how many are cross-checked can be decided by the margin of the constituency using simple formulae such as those proposed in Aslan et al. More complicated approaches may be used if one wants to take into consideration the variation in the number of votes across EVNs.

Prashant Bhushan

(TRUE COPY)

ANNEXURE: R5

Electronic Voting and Democracy

Subodh Sharma

Email: *svs@cse.iitd.ac.in*

Computer Science and Engineering
(also associated with the School of Public Policy)
Indian Institute of Technology Delhi
New Delhi 110016

Abstract

What are the salient properties that electronic voting systems must satisfy in order to meet democratic principles? Are such requirements viable or are they of only theoretical interest? How would the ECI's EVM fare against such properties? These are some of the questions I shall attempt to answer in this deposition.

1 Introduction

India recently concluded the world's largest parliamentary election [Wu and Gettleman, 2019] with 543 constituencies and well over 1 million voters per constituency on the average. Complete polling with offline electronic voting machines (EVM) not only ensured efficiency of the polling process and timely announcement of results, but, from several accounts, also ensured that the election was fair [ET-Bureau, 2019, Purkayastha and Sinha, 2019]. Electronic voting perhaps is essential for managing elections of such size and complexity. However, the EVM solution [Election Commission of India, 2019a,b] was not verifiable therefore its guarantees could not be established [Shukla, 2018, Banerjee and Sharma, 2019], which inevitably generated disquiet during the elections [Vora, 2017, Venkataramakrishnan, 2019].

World-wide concerns with EVMs have resulted in their being discontinued in many countries. After several years of controversy, Netherlands abandoned electronic voting in 2007 [Goldsmith and Ruthrauff, 2007], deciding that the integrity of the democratic process was more important than efficiency. Similar considerations have led to their discontinuation in Germany [NDI, 2019], France [Reuters, 2017], Ireland [O'Halloran and O'Regan, 2010] and several others. Many in the USA have voiced their apprehensions [Mercuri, 2007, Schneier, 2018, Schwartz, 2018] against existing EVMs, and the Defense Advanced Research Project Agency (DARPA) has decided to design and build a secure open source voting system for the future [Zetter, 2019]. In a recent report, the national academies in the USA have recommended conducting elections with human readable paper ballots trails [National Academies of Sciences, Engineering and Medicine, 2018].

It is clear that any electronic voting system must satisfy certain minimum requirements before they can be accepted as instruments for enabling electoral democracy. It is worth noting that any set of technical requirements is, in fact, driven by only three obligations: (i) the losing candidate has to be provided with a convincing proof of their loss, (ii) the voter, should she demands, be supplied with the guarantee that her vote was indeed *cast-as-intended* (indicating that the voting machine has registered the vote correctly), *recorded-as-cast* (indicating the cast vote is correctly included in the final tally), and *counted-as-recorded* (indicating that final tally is correctly computed), iii) no vote should be recorded other than those for which a designated polling officer certifies the eligibility and identity checks of the voter, and iv) all votes are kept secret during and after polling.

These, in turn, dictate that any electronic voting system must establish the following three properties:

- **Correctness:** all votes are *recorded-as-intended* (composition of *cast-as-intended* and *recorded-as-cast*) and *counted-as-recorded*; and that there is no spurious vote injection.
- **Privacy:** voter secrecy at all stages of the voting process attacks (such as vote manipulation, injection, and deletion)

Achieving the above properties in a technical design is known to be notoriously challenging (due to the seemingly conflicting requirements of security and privacy). Above all, the demanding set of technical requirements cannot be put in a *paternalistic design* that takes away the understanding of the process of collection, recording and accounting of votes

from the voters. It is crucial for democracy that not only are elections fair, but that they also appear to be fair and do not depend on certification by experts and auditors. While banning electronic voting, the German Constitutional Court made the following observation [NDI, 2019]:

> The use of voting machines which electronically record the voters' votes and electronically ascertain the election result only meets the constitutional requirements if the essential steps of the voting and of the ascertainment of the result can be examined reliably and without any specialist knowledge of the subject [...]

In light of the above observations, we may be pressed to ask the following:

Q1 can one design systems or are there existing ones, such as paper ballots, that meet the above-discussed properties?

Q2 does the ECI's EVM meet the above-mentioned set of requirements? If not, can we identify the requirements on which they (may) fail?

Paper ballots have been the cornerstone of electoral democracy for over two centuries. No analysis on electronic voting systems, therefore, can be complete without a reflection on paper ballots first. While it may appear [Sampath, 2019] that paper ballots meet the democratic principles, on a deeper analysis it emerges that paper ballots cannot guarantee some crucial requirements listed above. Paper ballot based voting systems neither provide a guarantee to a voter that her vote is recorded as intended and counted as recorded (without loss of privacy), nor provide guarantees against vote injection and deletion to a losing candidate. Clearly, the correctness and security properties are not preserved.

In contrast, how do electronic voting systems fare? It may come as a surprise that design of electronic voting systems has been studied extensively in the field of computer science for over three decades with the answer to the first part of Q1 being in the positive. See [Bernhard et al., 2017] for a review. It is not clear whether such a rich literature was even referred to while designing the Indian EVM.

In the absence of any public information on the design of ECI's EVM, and a formal proof or even an informal statement on the best design practices adopted relating to the correctness, security and privacy aspects of the machine, one can only conclude the answer to Q2 to be in the negative.

In the following text, I will attempt to present a distilled set of principles from the literature which abstractly map to the above mentioned requirements. Thereafter, I will present an argument on why ECI's EVMs appear on a weak footing in relation to some of these key principles. Subsequently, I will briefly discuss two recent and popular electronic voting protocols as examples of robust designs before concluding this written deposition.

2 Trust assumptions and key democratic principles in electronic voting

2.1 (No) Trust requirement for correctness

Democratic principles demand that it should not be necessary to trust any authorities, individually or collectively, for the correctness of the election process. Moreover, every component of the election process should be publicly auditable without requiring trust on any special auditors or experts.

Polling also requires strict identity verification of voters against a voter list for all votes, and must rely either on digital authentication or on offline identity verification by a polling officer. In the absence of a de-duplicated digital voter identity system, trust on the latter is unavoidable for eligibility checking. However, this trust must be publicly recorded, and we require the polling officers to certify each valid vote.

2.2 Trust requirement for voter secrecy

In any polling system *voter secrecy* must be preserved at all times. Hence, voting systems must never issue a receipt for the cast vote to a voter to ensure that a voter is never able to prove to a coercer or a potential vote buyer who they voted for [Benaloh and Tuinstra, 1994]. *Secrecy* and *receipt-freeness* are necessary conditions for *coercion-free voting*. *Receipt-freeness* however does not preclude issuing a token receipt to a voter from which no information about who they voted for can be gleaned.

All electronic voting systems need to trust the hardware security and privacy implementations - for example using trusted execution environments [Sabt et al., 2015] - and also the custody chain of authorities for not compromising voter secrecy. The protocol itself must guarantee not to leak information.

2.3 Key democratic principles

Universal verifiability: A voting system is *universally verifiable* if it can provide provable recorded-as-cast and counted-as-recorded guarantees for every vote, either deterministically or with a high probability. Universal verifiability implies that a system is auditable.

Individual verifiability: *Individually verifiable* usually implies [Cortier and Lallemand, 2018, Castelló, 2016] that every voter can verify that their vote is *cast-as-intended* and is recorded in the final list to be tallied. It turns out that individual verifiability is essential for voter secrecy [Cortier and Lallemand, 2018].

Ideally, one may want a stronger version of individual verifiability where a voter can proactively seek a sound and complete proof that their vote is also *recorded-as-intended* and *counted-as-recorded*. The proof of individual verifiability should be available on demand, and if it depends on a global universally verifiable component, then that component should be publicly auditable without requiring any special auditors. In other words, every voter should be able to trace their vote to the tally for their chosen candidate and verify the tally. Individual verifiability is *necessary* to establish that a cast vote is *non-repudiable*, *i.e.*, a voter cannot later claim that their vote was not recorded or counted correctly. It is also worth noting that universal verifiability does not imply individual verifiability, therefore preserving individual verifiability is necessary in its own right.

Such individual verifiability is the very root of voter confidence in electoral democarcy.

Dispute resolution: Effective dispute resolution requires a process for clear determination in favour of either the voter or the election authority in case of a challenge, without compromising voter secrecy. Central to dispute resolution is the non-repudiability of a cast vote. Non-repudiability of a cast vote cannot be established without the election authority being able to provide a sound proof of recorded-as-intended, or compromising on voter secrecy. It is also worth noting that universal verifiability does not always establish the non-repudiability of a cast vote without relying on instruments beyond the control of an individual voter (such as publicly auditable processes), or without compromising voter secrecy.

Finally, dispute resolution also requires non-repudiability of the verification receipts issued to voters by the election and polling authorities. This, in turn, requires all receipts to be duly signed.

Software independence: A voting system is *software-independent* if an undetected change or error in its software cannot cause an undetectable change or error in an election outcome [Rivest, 2008]. Software independence is a necessary condition for universal verifiability, because hardware-software verifiability of a system such as an EVM is almost surely an intractable (at least NP-Hard) problem. [Mercuri, 1992].

A typical EVM consists of a push-button user interface for voters to cast votes, a memory card to store the cast votes, and the software performing the recording and accounting operations running on a CPU. An EVM system composed from its components can exist in one of a very large number of states, which, in most cases, is an exponential function of the configuration parameters. either software or hardware may occur in a manner that is not deterministically reproducible, which necessitates examination of *all* the states that the system can be in. (These are not systematic failures like due to hacking, and can only cause denial of service type of faults) Examination of such large systems is an intractable problem, which often compels the examiners to rely on weaker forms of verification such as quality assurance (QA) methods – for instance, testing. However, well documented studies have shown that such weaker notions of verification can only detect a fraction of software errors (follows a common maxim that tests do not constitute a proof). Even if through weaker verification procedures one could ascertain the correctness of software to a reasonable degree, it is still inadequate. Ken Thompson, in his 1984 Turing award speech, illustrated that even with software programs shown to be correct the effort is far from over. One could insert a back-door (Trojan) into the hardware thereby facilitating exploits which remain undetectable. Thus, hardware specification, down to the chip level, along with the formal specification of all the side-channels must also be revealed and examined. In particular, it may be impossible to determine with reasonable amount of computation or testing whether such systems can ever reach a compromised state, perhaps due to hacking, where the democratic principles are violated.

Finding faults in such large composed systems is either impossible in general or highly expensive. Thus, the correctness of an E2E (end-to-end) verifiable voting systems should best not depend on the hardware or software used, and must be established solely from the output computed at various stages.

Protection against spurious vote injection: A voting system must also be free of spurious vote injection, at all times before, during or after polling. A voting system must guarantee that no votes are recorded and tallied other than those

approved by the polling officer. Universal verifiability does not usually guarantee against spurious vote injection by collusion of authorities.

Bare-handed voting: It has also been advocated that a voter should have zero digital computing available at voting time [Chaum, 2004]. The reasons for *bare-handed* voting are twofold. First, it is unfair to rely on voters to be able to compute cryptographic functions - or even digitally sign - when they may not have the agency or necessary understanding of the process. Second, it is unreasonable to assume that voters can have access to trusted computing platforms that will not leak information [Rivest, 2001a, Adida, 2006]. For example, commodity laptops and handhelds, which a voter may own but not have complete understanding of, certainly cannot be trusted either for correctness of cryptographic computations or for privacy of voting. The *secure platform problem* [Rivest, 2001b] effectively rules out internet voting [Chaum, 2004, Rivest, 2001a,b, Mercuri, 2007], and *bare-handed* voting systems must necessarily be polling booth protocols.

Large aggregation: Finally, making the vote tally of an EVM or a polling booth - typically of a few thousand voters - public may enable profiling of a locality or a community. Hence, it is essential to aggregate the votes over several polling booths and EVMs leading up to perhaps even an entire constituency before making the tally public. *Large aggregations* are essential for community privacy, and necessitates hiding the polling officers' identities, yet requiring the polling officers to certify each recorded vote.

3 A Comment on EVMs and VVPATs

Any EVM based solution that relies on hardware and software integrity, with or without voter-verified paper audit trails (VVPAT) [Mercuri, 1992, Election Commission of India, 2019a], is not software independent and is hence not universally verifiable. Besides, VVPAT only ensures that the electronic vote count matches that of the paper audit trail, and that by itself provides no guarantee against spurious vote injection or deletion in both post the polling process. Thus, the fundamental principle of correctness cannot be established for software/hardware dependent EVM based voting systems. Reliance on ad hoc and unverifiable processes such as in [Election Commission of India, 2019a, Purkayastha and Sinha, 2019] can only result in uncertain technological solutions for electoral democracy.

Even if EVMs were to be shown to be universally verifiable, in absence of individual verifiability the elections cannot offer any instrument through which they can convince the voter about her vote is cast as intended and counted as cast, without compromising the privacy of the cast vote.

A silver-lining, however, exists. Several E2E verifiable electronic voting protocols have been formulated that formally guarantee many of the principles discussed in the previous section. In the following section, I will cover two such protocols that are either direct-recording electronic (DRE) or optical scanning based electronic voting systems which have been in existence prior to the 2019 elections in India.

4 Some existing E2E voting protocols

4.1 Scantegrity

Scantegrity [Chaum et al., 2008] is an E2E universally verifiable voting protocol which is identical to optical scan voting systems with an additional feature that voters can take home a receipt from which no privacy information is leaked. The ballots are pre-prepared as shown in Figure 1, where the candidate to letter code mapping is randomized in each ballot. Each voter after casting her vote tears off the perforated top right corner of the ballot which has a unique serial number and notes down the letter code corresponding to the choice.

Each voter also has an option to do a cast-or-audit challenge [Benaloh, 2006]. In case of a challenge the voter retains that unmarked blank ballot and is issued a fresh one for voting. At a later point of time the voter can demand an audit of the correctness of the ballot encryption, i.e., the correctness of the candidate to letter code mapping for the ballot serial number for the challenged ballot. A statistically significant number of voter challenges provide a probabilistic universal guarantee that the mappings are correct.

The chosen code letter against the serial number for all cast votes are published on a public bulletin board without the candidate names (Figure 2). A voter can verify that her vote is cast-as-intended - for the letter code - by looking up the row in the bulletin board marked with her serial number. An anonymous but a verifiable mapping between the actual vote and the receipt serial number is maintained by a special component called *mixnet* [Chaum, 1981, Chaum et al., 2008] (Figure 2). A mixnet is similar to a switchboard that applies cryptographic operations to conceal the path of messages

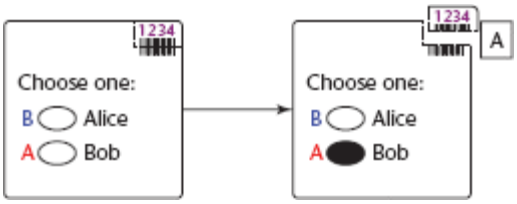


Figure 1: Scantegrity Ballot (from [Chaum et al., 2008])

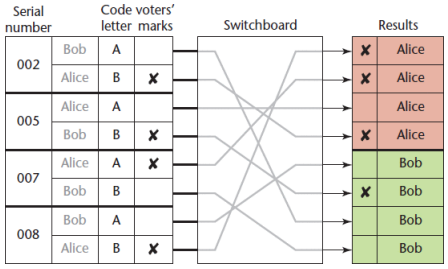


Figure 2: Mixnet (from [Chaum et al., 2008])

through the network. A typical mixnet can have many layers, each layer leading to cryptographic concealment. A voter can trace an encoded receipt only up to the input of the mixnet. Thereafter they can only verify partial correctness by examining parts of a mixnet that are trusted to be randomly chosen by an auditor and are revealed publicly. For every path, at least one part is kept hidden to preserve voter secrecy. The public audit of large parts of the mixnet for a sufficient number of voters provide a probabilistic guarantee and ensure universal verifiability. The final result of the mixnet is publicly displayed on another bulletin board and anybody can verify the tally.

Individual verifiability is only partial in the protocol because the voter cannot trace her vote to the final tally and must rely on universally verifiable guarantees (thus, recorded-as-cast guarantee is not available). Prêt à voter [Ryan et al., 2009] is a system quite similar to Scantegrity in principle which has been tested in several public elections.

4.2 Starvote

Starvote [Bell et al., 2013] is an E2E DRE voting system offering similar guarantees as Scantegrity, however, its methods of hiding the vote and preserving privacy and universal verifiability are different.

The voter casts her vote in a voting terminal with GUI (for clear sight voters) or auditory UI (for visually handicapped voters). After the vote is selected, the terminal performs three actions: (i) its prints a take-home receipt that identifies a short cryptographic digest that serves as the *commitment* of the vote along with some additional meta-data such as the time of the vote, the terminal used for casting the vote, etc., (ii) it prints a paper ballot with a random serial number along with the summary of the vote in clear text, which serves as a voter verified paper record. The voter after reviewing the second receipt can either cast the ballot (drop it in a box) or use the current choice as a challenge-and-audit action [Benaloh, 2006] to convince herself later of the correctness of the cryptographic encoding of her vote, and (iii) the terminal sends the encrypted data to the election commission's office.

The encrypted votes are posted on a public bulletin board. The voters can verify the presence of their votes on the bulletin board by matching the cryptographic digest on their take-home receipts with specific rows in the bulletin board. The tallying of the cryptographic votes is performed by the election authority using a special *homomorphic* property of cryptographic operations. In other words, the homomorphic property on encrypted data allows the election authority to perform counting on encrypted votes without ever requiring to decrypt the votes. Anybody can verify the homomorphic tallying.

The protocol is universally verifiable. However, the universal verifiability is only partial because a voter can only have a universal statistical guarantee that her vote was correctly encoded.

4.3 Discussion

While protocols such as Scantegrity and Starvote preserve properties like universal verifiability and software independence, they do not offer non-repudiation on cast votes; in particular, Scantegrity does not guarantee recorded-as-cast property and Starvote does not preserve cast-as-intended property. Therefore, in such class of protocols the individual verifiability guarantee is met only partially. Both these systems are also vulnerable to spurious vote injection post-election through insider attacks or collusion among authorities. There have been recent works to partially strengthen the protocols against these weaknesses.

For a recent DRE protocol that provides complete individual verifiability for both cast-as-intended and counted-as-cast guarantees, and ensures that there can be no spurious vote injection, see [Agrawal et al., 2019].

In comparison the ECI's EVM lacks critical properties such as software independence, universal and individual verifiability.

5 Conclusions

The use of EVMs in Indian election has indeed demonstrated credible gains in efficiency with respect to the polling and counting processes. It is the fatalistic claims of the kind – since the EVMs have not been hacked so far, therefore, they are safe – that require attention. That a system has not been hacked yet does not give formal assurance of its infallibility. The burden of establishing trust either through verifiable proofs or through best practices lies with the designers and the election authority. Since neither ECI's EVM designs nor verifiable proofs have been made open, the critical question of which correctness properties are satisfied by EVMs in India remains open. Ensuring security by obfuscation may be legitimate way for enterprises operating for profit but cannot be applied to instruments that enable democracies to function.

References

Ben Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, MIT, Cambridge, MA, USA, 2006. AAI0810143.

Prashant Agrawal, Kabir Tomer, Subodh Sharma, and Subhashis Banerjee. An individually verifiable voting protocol with complete cast-as-intended and counted-as-cast guarantees, 2019. URL https://arxiv.org/abs/1908.09557.

Subhashis Banerjee and Subodh Sharma. The best way to vote. https://indianexpress.com/article/opinion/columns/evm-lok-sabha-elections-general-elections-2019-election-commission-5605737/, March 2019. [Online March 1, 2019].

Susan Bell, Josh Benaloh, Michael D. Byrne, Dana Debeauvoir, Bryce Eakin, Philip Kortum, Neal McBurnett, Olivier Pereira, Philip B. Stark, Dan S. Wallach, Gail Fisher, Julian Montoya, Michelle Parker, and Michael Winn. Star-vote: A secure, transparent, auditable, and reliable voting system. In *2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13)*, Washington, D.C., 2013. USENIX Association. URL https://www.usenix.org/conference/evtwote13/workshop-program/presentation/bell.

Josh Benaloh. Simple verifiable elections. In *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006 on Electronic Voting Technology Workshop*, EVT'06, pages 5–5, Berkeley, CA, USA, 2006. USENIX Association. URL http://dl.acm.org/citation.cfm?id=1251003.1251008.

Josh Benaloh and Dwight Tuinstra. Receipt-free secret-ballot elections (extended abstract). In *Proceedings of the Twenty-sixth Annual ACM Symposium on Theory of Computing*, STOC '94, pages 544–553, New York, NY, USA, 1994. ACM. ISBN 0-89791-663-8. doi: 10.1145/195058.195407. URL http://doi.acm.org/10.1145/195058.195407.

Matthew Bernhard, Josh Benaloh, J. Alex Halderman, Ronald L. Rivest, Peter Y. A. Ryan, Philip B. Stark, Vanessa Teague, Poorvi L. Vora, and Dan S. Wallach. Public evidence from secret ballots. In *Electronic Voting - Second International Joint Conference, E-Vote-ID 2017, Bregenz, Austria, October 24-27, 2017, Proceedings*, pages 84–109, 2017. doi: 10.1007/978-3-319-68687-5_6. URL https://doi.org/10.1007/978-3-319-68687-5_6.

Sandra Guasch Castelló. *Individual Verifiability in Electronic Voting*. PhD thesis, Universitat Politècnica de Catalunya, Barcelona, 2016. URL https://upcommons.upc.edu/bitstream/handle/2117/96245/TSGC1de1.pdf.

D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora. Scantegrity: End-to-end voter-verifiable optical-scan voting. *IEEE Security and Privacy*, 6(3):40–46, May 2008. ISSN 1540-7993. doi: 10.1109/MSP.2008.70.

David Chaum. Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1):38–47, January 2004. ISSN 1540-7993. doi: 10.1109/MSECP.2004.1264852. URL http://dx.doi.org/10.1109/MSECP.2004.1264852.

David L. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–90, February 1981. ISSN 0001-0782. doi: 10.1145/358549.358563. URL http://doi.acm.org/10.1145/358549.358563.

Véronique Cortier and Joseph Lallemand. Voting: You can't have privacy without individual verifiability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 53–66, New York, NY, USA, 2018. Association for Computing Machinery. ISBN 9781450356930. doi: 10.1145/3243734.3243762. URL https://doi.org/10.1145/3243734.3243762.

Election Commission of India. Manual on Electronic Voting Machine and VVPAT. https://eci.gov.in/files/file/9230-manual-on-electronic-voting-machine-and-vvpat/, 2019a. [Accessed June 10, 2019].

Election Commission of India. Status Paper on EVM (Edition - 3). https://eci.gov.in/files/file/8756-status-paper-on-evm-edition-3/, 2019b. [Accessed June 10, 2019].

ET-Bureau. EVM-VVPAT pass test in Lok Sabha polls. https://economictimes.indiatimes.com/news/elections/lok-sabha/india/evm-vvpat-pass-test-in-lok-sabha-polls/articleshow/69469579.cms, May 2019. [Online May 23, 2019].

Ben Goldsmith and Holly Ruthrauff. Case Study Report on Electronic Voting in the Netherlands. Technical report, National Democratic Institute (NDI), 2007.

Rebecca Mercuri. Statement on Electronic Voting. http://www.notablesoftware.com/RMstatement.html, 2007. [Accessed June 6, 2019].

Rebecca T. Mercuri. Physical verifiability of computer systems. In *In International Computer Virus and Security Conference*, 1992. URL http://www.notablesoftware.com/PENN2008/PhysVerify.pdf.

National Academies of Sciences, Engineering and Medicine. *Securing the Vote: Protecting American Democracy*. The National Academies Press, Washington, DC, 2018. ISBN 978-0-309-47647-8. doi: 10.17226/25120. URL https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy.

NDI. The Constitutionality of Electronic Voting in Germany. https://www.ndi.org/e-voting-guide/examples/constitutionality-of-electronic-voting-germany, 2019. [Accessed June 8, 2019].

Marie O'Halloran and Michael O'Regan. E-voting machines to be disposed of. https://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193, 2010. [Online October 6, 2010].

Prabir Purkayastha and Bappa Sinha. There is No Ghost in the Indian EVM. https://www.theindiaforum.in/article/there-no-ghost-indian-electronic-voting-machine, 2019. [Online April 5, 2019].

Reuters. France drops electronic voting for citizens abroad over cybersecurity fears. https://www.reuters.com/article/us-france-election-cyber-idUSKBN16D233, 2017. [Online March 6, 2017].

Ronald L. Rivest. Re: Security in Voting Technology. http://people.csail.mit.edu/rivest/rivest-may-24-01-testimony.txt, 2001a. [Accessed April 29, 2019].

Ronald L. Rivest. Electronic Voting. https://people.csail.mit.edu/rivest/Rivest-ElectronicVoting.pdf, 2001b. [Accessed April 29, 2019].

Ronald L. Rivest. On the notion of software independence in voting systems. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 366(1881):3759–3767, 2008. doi: 10.1098/rsta.2008.0149. URL https://royalsocietypublishing.org/doi/abs/10.1098/rsta.2008.0149.

Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à voter: A voter-verifiable voting system. *Trans. Info. For. Sec.*, 4(4):662–673, December 2009. ISSN 1556-6013. doi: 10.1109/TIFS.2009.2033233. URL http://dx.doi.org/10.1109/TIFS.2009.2033233.

M. Sabt, M. Achemlal, and A. Bouabdallah. Trusted execution environment: What it is, and what it is not. In *2015 IEEE Trustcom/BigDataSE/ISPA*, volume 1, pages 57–64, 2015.

G. Sampath. Why evms must go, 2019. URL https://www.thehindu.com/opinion/op-ed/why-evms-must-go/article26053761.ece.

Bruce Schneier. American elections are too easy to hack. We must take action now. https://www.theguardian.com/commentisfree/2018/apr/18/american-elections-hack-bruce-scheier, 2018. [Online April 18, 2018].

Jen Schwartz. The Vulnerabilities of Our Voting Machines. *Scientific American*, November 2018. URL https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/. [Online November 1, 2018].

Sandeep K. Shukla. Editorial: To use or not to? embedded systems for voting. *ACM Trans. Embed. Comput. Syst.*, 17 (3):58:1–58:2, May 2018. ISSN 1539-9087. doi: 10.1145/3206342. URL http://doi.acm.org/10.1145/3206342.

Rohan Venkataramakrishnan. Scroll Explainer: All you need to know about the latest EVM controversy. https://scroll.in/article/924241/scroll-explainer-all-you-need-to-know-about-the-latest-evm-controversy, May 2019. [Online May 22, 2019].

Poorvi L Vora. The great EVM debate: Convincing the losers that they lost. https://scroll.in/article/832003/the-great-evm-debate-convincing-the-losers-that-they-lost, March 2017. [Online March 17, 2017].

Jin Wu and Jeffrey Gettleman. India Election 2019: A Simple Guide to the World's Largest Vote. https://www.nytimes.com/interactive/2019/world/asia/india-election.html, May 2019. [Online May 22, 2019].

Kim Zetter. DARPA Is Building a $10 Million, Open Source, Secure Voting System. https://www.vice.com/en_us/article/yw84q7/darpa-is-building-a-dollar10-million-open-source-secure-voting-system, 2019. [Online March 14, 2019].

Prashant Bhushan
(TRUE COPY)

ANNEXURE: R6

To use or not to use? Electronic Voting Machines in Indian Elections.

Sandeep K. Shukla

Electronic Voting Machines (EVMs) are a very commonly discussed example of an embedded computing system which has also been at the center of political storm in India in the recent days. A number of allegations have surfaced that the EVMs are being reprogrammed or tampered with during elections to favor candidates of a specific political party. Given that EVMs are very classical embedded systems with simple microcontrollers whose program instructions are burnt into a ROM, and cast vote counts are stored in an EPROM, and few peripherals, one would think that it would be easy to verify by experts to indubitably establish their tamper proof design, and implementations. However, looking at various aspect of this simple yet very critical embedded system, it seems a lot more research is required on multiple aspects of the democratic franchise that are dispensed through these simple systems. It should be mentioned also that recently in response to 'right-to-information' query, one of the manufacturers divulged that new generation of Indian EVM are no longer having program instructions burnt into ROM but they are using a specific microprocessor with writable memory. This raises lot more questions than one would have raised with the previous generation EVMs. Furthermore, one of the two manufacturers refused to even entertain the query – raising further suspicion.

Before coming to the Indian case, let me focus on some other countries. In the Netherlands, electronic voting machines were abandoned in 2007 after several years of controversy regarding the security of the voting data, the machines, as well as the privacy of the voter. The engagement of civil society, computer experts and others paved the way to experimentation that showed the ease with which one can replace the memory chips in those machines in less than five minutes, allowing manipulation, thereby possibly subverting democracy. More concerning was the fact that with simple radio receivers, people could see variations in electro-magnetic signals that would allow one to detect who a voter is casting the vote for – from outside the polling station. After some iterations in the design, other such side channel attacks were found in certain versions of the machine, and eventually honoring the fact that integrity of the democratic process is more sacrosanct than efficiency – the Netherlands abandoned the electronic voting [1].

In 2009, the federal constitutional court of Germany ruled that electronic voting is unconstitutional [2]. The court ruled "*The use of Nedap electronic voting machines violated the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law)* ***that requires that all essential steps in the elections are subject to public examinability*** *unless other constitutional interests justify an exception.*" This is very significant. Given that **the legitimacy of democratic processes depends on the public's trust in the processes, any member of the public should be able to examine, if he/she desires so, to test and verify every step** – including the functioning of the voting machines, their design, the security and safety safe guards, and measures to secure their franchise.

If the voting machine design, software, or the security proofs are not possible to verify by members of the public, there is enough reason to worry about safeguarding our democracy.

Ireland also abandoned electronic voting in 2004. In the United states, 27 states are using electronic voting machines of which 15 are using verifiable audit trail. However, given the issues surrounding the hacking incidents during the last presidential election in the united states, there is reasonable doubt whether it is prudent to continue the electronic machine-based voting.

Coming back to the Indian case, the voting machines are quite simple, with a ballot unit, a control unit, display unit, and the wires connecting them. While the software is kept under extreme confidentiality with the government sector companies who manufacture these machines, the machine instructions were burnt into a ROM in the previous generation EVMs with the claim that it cannot be changed. The microcontroller being used is simple, and the memory units are connected with simple protocol. In 2010, a group of security experts got hold of a unit and showed that there are numerous ways to tamper with these machines within matters of few minutes [3]. One can replace the microcontroller, the memory units, and even the PCB board with relative ease provided physical access is possible. Also, if the EPROM is replaced with an attacker's chosen instructions, the behavior of the machine could be changed, including how it responds to pre-poll mock polling phase vs. real polling phase. Further, the display unit can be replaced, and clip on radio frequency devices may be used to control the behavior of the programs. Of course, the Indian authorities now have responded by adding mutual authentication between the components, and also doing some redesign. The design of the latest one uses MK61FX512VMD12 microcontroller from an MNC – which is of US origin. Moreover, this chip has programmable FLASH memory. Although, if the JTAG pins are fused, and memory lock bit is set – it cannot be written to. Unfortunately, it turns out neither Election Commission nor the Government has any appetite to get this design checked by cyber security experts in various IITs even though the technical expert committee formed by EC has not a single cyber security expert. The EC's claim is that the technical committee bereft of any expert in cyber security has certified it – so we no longer need any further check by outside experts.

Given the cloak of secrecy about the design, the program, and even the mechanisms of authentication – ***security by obscurity seems to be their goal***. Another defense is that the EVMs are very well protected during its storage, transfer, and randomized methods for allocating them to polling booths. Unfortunately, given the large population, and various uncertainties during a nationwide polling process, many of these safe guards might be violated if properly orchestrated. If none of these happen, even then, the fact that all the steps associated with the electronic voting machine design, manufacturing, and security studies are not subject to the verification and testing by the common people, and experts – there are scope of doubt about the security of the entire process. With the current advances in data science and exfiltration of personal data as exemplified in the Cambridge Analytica/Facebook case, it is not inconceivable that data analytics can pin point exactly which polling stations need to be tampered with, leaving the rest as it is –

and still manipulate the outcomes of the election. Therefore, it might be possible to manipulate only a few of the EVMS per parliamentary constituency to tamper with the results of that constituency. Which booths to target can be decided by appropriate use of data science on demographic data. This is not to say that such manipulations do happen, but the citizens should have a right to be fully convinced that it does not. Only way to do this is to provide copies of the machines to experts at various Indian institutes and have them thoroughly test the machines for security, side channels, programmability etc.

EC in the past sent out challenge to community to hack EVMs by inviting teams to their headquarters but they severely restrict the kind of tests that the teams can do – for example, using of oscilloscope on the pins by opening the boxes are not allowed. Therefore, side channel analysis, checking whether the micro-controller JTAG pins are fused etc – cannot be checked. It seems that only tests allowed are pressing buttons in order to change results. However, even if there are 10 buttons, there are 2^10 possible combinations, and each such combination has a factorial number of permutations to test – which is not possible to try for any one. Therefore, these 'come-and-hack' events are more of an eye wash than real honest attempt to convince the citizens about the security of these machines.

So as cyber security researchers, it seems to be incumbent on us to figure out systems whose safety and security can be verified by anyone – while it is secure enough without the need for obscurity/secrecy of the algorithms, designs, methods etc. That is the only way, electronic voting machines can be made acceptable to a democratic nation. Creating a cloak of secrecy to protect from tampering never works – all security researchers would agree.

This is an important need that embedded systems community can attempt to cater to, and at the same time, save the democratic election process in every democratic jurisdiction. If experts can show to anyone interested the risk, the potential attack surfaces, the side channel vulnerabilities, and make every bit of software/firmware, architecture, protocols open, and check the plausibility of exploitations that still may remain in the fully vetted system – that will put the population at ease regarding their enfranchisement – even with systems they do not fully understand.

I, therefore, request all readers to think about this problem, and demand EVM designs to be transparent and open, have experts to test them, do their risk analysis, before EVM is accepted as the instrument of our democracy.

1. https://www.ndi.org/sites/default/files/5_Netherlands.pdf
2. http://www.dw.com/en/german-court-rules-e-voting-unconstitutional/a-4069101
3. https://indiaevm.org/evm_tr2010-jul29.pdf

Prashant Bhushan

(TRUE COPY)

INDIAN STATISTICAL INSTITUTE

Shri Durgam Giri
Senior Administrative Officer &
CPIO

203 BARRACKPORE TRUNK ROAD
KOLKATA 700 108, INDIA
Fax : +(91)(33) 2577 6033
E-mail : g.durgam@gmail.com

No CAF/21-A/62/2018-19/ 012
03 April, 2019

Dr. Krishanu Maulik
13 Ekdalia Place,
Kolkata - 700019

Sub. : Your RTI application dated 13.03.2019, received by this office on 13.03.2019

Dear Sir,

This refers to your RTI application dated 13.03.2019, received by this office on 13.03.2019, the information sought, are furnished below :

Sl. No.	Information sought	Information supplied
1.	Certified copy of the communication from the ECI to ISI requesting a report on VVPAT	Copy enclosed.
2.	Certified copy of the office order of ISI forming a committee to prepare the report.	No information held.
3.	Name and designation of the members of the committee.	
4.	Number of times the committee has met, with date and location of the meeting.	
5.	Certified copies of the proceedings of such meeting.	Not held in this office.

Your RTI application dated 13.03.2019, received by this office on 13.03.2019, is disposed of. The First Appeal, if any, against the reply of the CPIO may be made to the First Appellate Authority within 30 days from the receipt of reply from the CPIO. The name and address of The First Appellate Authority is given below:

Brig J N Pandey
Chief Executive (A&F) & FAA of the Institute
203, B.T. Road, Kolkata – 700 108
Phone: +91 33 2575-2251
e-mail: ceaf@isical.ac.in

Yours sincerely,

(Durgam Giri)
Senior Administrative Officer & CPIO

ELECTION COMMISSION OF INDIA
NIRVACHAN SADAN, ASHOKA ROAD, NEW DELHI-110001

No.51/8/VVPAT-ISI/2018-EMS Dated: 14th August, 2018

To,

Prof Bhat,
Head, Indian Statistical Institute (Delhi Centre),
New Delhi

Subject: **Mandatory verification of VVPAT slip count with electronic result during counting of votes in elections to the Parliament and State Legislative Assemblies: Statistical principles - regarding**

Sir,

With reference to the captioned subject and in continuation of the discussion during the meeting with Sh Sudeep Jain, Dy Election Commissioner on 08.08.2018, I am directed to state that the Election Commission of India is Constitutionally mandated with direction, superintendence and control of elections to the Parliament and various State Legislative Assemblies in the country. Over the last two decades, the Commission has successfully conducted various general and bye elections through Electronic Voting Machines (EVMs) based voting and counting. Since 2013, the Commission has also deployed Voter Verifiable Paper Audit Trail (VVPAT) machines along with EVMs for additional verifiability and transparency in the voting process. The Commission is committed to 100% deployment of VVPATs with EVMs at all polling stations in all future elections to the Parliament and State Assemblies.

In order to further enhance the credibility and transparency of the EVM-VVPAT based election process, as also to address the demands of certain political parties regarding VVPAT paper trail counting, the Commission has already decided to undertake VVPAT slip verification of 1 (one) randomly selected polling station in each Assembly Constituency during the counting process. As a consequence of this decision, to date VVPAT slip verification has already been done in respect of 843 polling stations across various States/UTs during the General and Bye election conducted during the last year. It is recorded with satisfaction that the slip verification has matched with the electronic count in all the cases.

However, there are intermittent demands from certain sections of the political firmament to increase the counting of VVPAT slips during every election and the request varies from 25% to 100% slip counting. As can be duly appreciated, there has to be a convincing logical rationale rooted, *inter alia*, in sound statistical foundation for examining

and processing such requests The Commission, as always, is keen to engage and involve all the stakeholders in the various aspects of election management and adopts a constructive and collaborative approach in resolving and addressing various issues, including the present matter regarding VVPAT slip count

Since, Indian Statistical Institute is the most notable and reputed national institution devoted to research, teaching and application of statistics and sampling knowledge in the country, the Commission considers it expedient and desirable that your cooperation and expertise is solicited in addressing the matter of VVPAT slip verification, being essentially a statistical issue Your vast technical resources and domain expertise will be very useful and instrumental in systematically analysing the whole issue and arriving at mathematically sound, statistically robust and practically cogent solutions to the raging debate about the number/percentage of VVPAT slip counts to be undertaken during the elections

In view of the same, it is requested that your kind convenience may please be conveyed for associating with the Commission and collaborating towards addressing the issues as elaborated above Any additional information or supplementary material in the matter, if so desired, may please be indicated

Thanking you,

Yours sincerely,

(NIKHIL KUMAR) 10/7/18
Director

INDIAN STATISTICAL INSTITUTE
203 BARRACKPORE TRUNK ROAD
KOLKATA 700 108

OFFICE ORDER NO. D.O./2016/382 DATED 10 JUNE 2016

All programmes other than the regular degree/diploma courses undertaken by the Institute or its scientists involving external agencies will henceforth be taken up by the Cell for Cooperation with Academia, Industry and Research Labs (C-CAIR). The Cell will comprise the following members:

1.	Professor Bhargab B. Bhattacharya	... Chairperson
2.	Professor Ayanendranath Basu	... Vice-Chairperson
3.	Professor Dilip Saha	... Member
4.	Dr. Prasun Das	... Member
5.	Dr. Utpal Garain	... Member
6.	Dr. Ansuman Banerjee	... Member
7.	Dr. Anil K. Ghosh	... Member
8.	Dr. Soumyanetra Munshi	... Member
9.	Head, Delhi Centre or his nominee	... Member
10.	Head, Bangalore Centre or his nominee	... Member
11.	Head, Chennai Centre or his nominee	... Member
12.	Dr. Raghunath Chatterjee	... Convener

Responsibilities

The Committee will be responsible for matters related to the following :

- Initiating collaborations/student exchanges/MoUs with other Universities/Institutes or with any external/government agencies including research labs;
- Reviewing project proposals, and proposals for collaborations submitted by the scientific workers; this will include funding proposals to be sent to government agencies or private organizations. The Cell should consult other relevant committees to decide on related issues;
- Collaborations with Industries;
- Establishing and promoting incubation efforts

The Committee will also be responsible for the following

- Formulating well-defined procedures for submission, review/sanction of all such proposals;
- Formulating a policy for IP-sharing;
- Reviewing the policies on Income Generating/Non-Income Generating/Consultancy projects, associated leave rules, and patents;
- Review the policy for income sharing and usage policy among the Institute, the Department and the Division as applicable;
- Formulating policies of incubation.

Contd. 2/-

General Guidelines

All proposals will be submitted to the Chairperson (or Vice-Chairperson), C-CAIR Cell. These will be reviewed by the Committee and recommended to the Director, strictly following the well-laid out procedures, by the C-CAIR Cell. Any deviation has to be forwarded to the Director with specific recommendation and justification. The decision of the Director on such matters will be final.

All policies formulated by the Committee, and any change thereafter, must be sanctioned by the Director.

The existing policies procedures will continue to apply till new policies are formulated.

It is expected that all policies are well-laid out within six months of the issue of this order. Thereafter the different Centres (other than the Head quarter) will form their own Cells, with the Director's approval, Chaired by the Centre Head and with at least one member each from Head quarter and other Centre (from the corresponding C-CAIR Cell). The Cells in the Centres will function in exactly the same way as laid out for the C-CAIR Cell in this order.

This order supersedes the Office Order No. D.O./2015/509 dated 10 August 2015.

S Bandyopadhyay

(Sanghamitra Bandyopadhyay)
Director

Copy to : All Faculty Members
All Professors-in-Charge/Head, SQC & OR Division
Head of Centres
All Heads of Departments/Sections/Units including outlying centres/branches
Chief Executive (A&F)
Dy. Chief Executive (F)
Director's Office.

Prashant Bhushan

(TRUE COPY)

Comments on the presentation "on Testing of EVM via VVPAT Slip-verification: Sample Issue "made before the Election Commissioner of India on 24th August 2018 by Abhay G. Bhatt and Rajeeva L. Karandikar

[Dr. SK Nath – 25 August, 2018]

The MAIN issue before the public was whether selection of ONE (1) EVM machine per Constituency was enough to prove that there is no difference between EVM count vis a vis VVPAT slip count within a constituency. In other words, whether there is scope of suspicion about the trustworthiness of EVM machine. But instead of formulating issue in its right perspective, the presenters set up the issue as below (Please refer to the slide on Notation):

Population – All EVMs used in an election

N – the size of the population – Total number of polling stations.

Comment: There is confusion about the definition used. The presenters may please define what is the POPULATION – no of EVM machines deployed or total number of polling booths. Two are not the same. In the first line the presenters have defined the Population as "All EVMs used in an election" whereas "N" has been defined as total number polling booth. Secondly, THIS ISSUE IS ABOUT SELECTION OF POLLING BOOTH PER CONSTITUENCY WHY THEY HAVE STUDIED all **polling stations for any election**.

In subsequent slides the presenters set up two questions namely,

1) Should the sample size depend on the population size?
2) What is a reasonable sample size or sampling fraction?

Let us look at the basic formulation of determination of Sample size as per any standard literature on Sample Survey is as follows assuming the Population size infinite.

$n = Z^2 \times \frac{pq}{e^2}$ ……(i)

Where n = sample size (no. of polling booths to be determined), p = the proportion of polling booths where total EVM counts do not match with that of VVPAT slip counts and e = the margin of error – generally it is taken as 5% or less. Z = the level of confidence. For Gaussian distribution it is 1.96 at 95% level of confidence.

Obviously, this formulation is not dependent on N which is the total number polling booths in a constituency (or, election as defined by the presenters). BUT WHEN THE "N" IS finite, IT IS NECESSARY TO APPLY FOR "fpc" – finite population correction which is a **function of N**.

IN PRACTICAL TERMS IF WE USE ABOVE FORMULATION WHERE "POPULATION" IS THE TOTAL NUMBER OF BOOTHS WITHIN A CONSTITUENCY, THE SAMPLE SIZE(n) WILL BE DEPENDENT ON "POPULATION SIZE(N)". BUT WHERE ANY STUDY IS MADE TAKING *ALL CONSTITUENCIES TOGETHER WITHIN A STATE OR COUNTRY OR TOTAL EVM MACHINES DEPLOYED IN AN ELECTION, THE SAMPLE SIZE WILL NOT BE DEPENDENT ON THE SIZE OF POPULATION as done by the presenters*

Let us now go to the second question, namely, what is a reasonable sample size or sampling fraction.

The pertinent question is whether the sample is to determined according to constituencies or all constituencies together for an election. The election commission of India in their circular number 51/8/VVPAT-INST/2018-EMS dated 13th February 2018, it has been clearly mentioned that one (1) polling booth (station) per Assembly constituency will be selected for verification of EVM counts with VVPAT counts. THIS IS UNDERSTANDABLE SINCE THE

PUBLIC DEMAND IS KNOW THE TRUST WORTHINESS OF EVM DEPLOYED IN EACH CONSTITUENCY.

Thus, the issue is whether selection of one (1) polling booth is sufficient or not. And if not, what should be the estimated value of "n" – the number of sample polling booths to be selected. THUS, THE FORMULATION OF THE ISSUE AS PRESENTED BY THE PRESENTERS IS NOT APPLICABLE.

Here it is observed that the presenters instead of using the formulation for determining the sample size as per (i) above, they preferred to compute probabilities based some past data where 843 EVM machines were chosen and found ZERO mismatch with VVPAT count. IT IS NOT CLEAR WHAT MADE THE PRESENTERS TO CHOOSE 843 EVMS TO PROVE THEIR HYPOTHESIS.

In the last two slides, they have computed the estimated number of EVM machines to be selected in an election (although this is the subject of discussion) using past data with some formulation without any reference and using value of parameters.

The presenters have computed n = 479 Polling booths for an election. The presenters in their concluding lecture wanted to justify that had this 479 been allocated over all constituencies within a state and then the effective sample size per constituency will be much lower than 1. In other words of the presenters, the sample size of one (1) per constituency as decided by the office of Election Commission vide their letter under reference is more than justified.

Now let us calculate the "margin of error" or risk we may find with sample size =1 within a constituency with p=.02 (that means when the defective EVM is just 2%)

(margin of error)^2 = Z^2 x pq /n = $(1.96)^2$ x (.02) x (.98) /1 = .0747936 using the formula at (i)

Means the "Margin of Error" is 27.35% . This will increase with higher value of "p". Will anyone in the world accept such high level of error?

Let us now come out with the fallacy in the presentation.

The analysis made by the presenters is too simplistic and according to their formulation, even for the country as a whole the value of n= will be 479 AND it is done for a single Constituency the value of n will again be 479.

AN IMPORTANT ISSUE WHICH WAS NOT CONSIDERED:

Whatever be the size of "n", the outcome of counts between EVMs and VVPAT may vary from polling booth to polling booth in respect of each party if party was analysis is done. THIS IS NATURAL AND NO CONCLUSION CANNOT BE DONE ABOUT TRUSTWORTHYNESS OF ELECTION PROCESS. Mind that if a fresh sample of "n" polling booths are chosen one may get opposite result. In other words, if all (or majority) EVM machines show higher figure as compared to VVPAT count in respect of a political Party (say X) it does not necessarily prove any biasness of EVMs. In such situation, it is necessary to conduct **"Statistical Test of Significance**" to prove whether the EVMs are biased in favour of a political party. The method of Testing has already been circulated.

Sampling Design and Test of Hypothesis for VVPAT based Auditing of EVM

By

Dr. S.K.Nath

(Fmr. Director-General, Central Statistical Organisation- **26 August, 2018]**

1.Introduction:

The Election Commission of India has recently decided to use VVPAT machines with each EVM machine during election of all Parliament and State Legislative Assemblies. According to modus operandi for auditing EC has decided that after declaration of results of an election, one VVPAT machine will be randomly selected in each constituency and the VVPAT paper slips will be counted and to be compared with the count of EVM machine with which it was interfaced during polling in a polling booth.

Many has raised about the efficacy of the sampling design as suggested by EC. It may be noted that whenever any decision is taken based on sampling, it is necessary to observe two important issues namely, size of sample (here VVPAT machine per Constituency minus defective machines) and the sampling design. Unless these are as per proper Statistical theory, there will be enough room for a wrong decision / wrong suspicion about EVMs. And this can safe guarded using the Statistical theory of "Testing of Hypothesis".

Before we took up this exercise, it was felt necessary to have certain back ground information from experienced Bureaucrats who actually conducted Elections and have the knowledge of the status of VVPAT based auditing tried by the Election Commission in recently concluded election of State Assemblies in Karnataka, Tripura and Gujarat. It is also felt necessary to know the experience of those Senior Engineers who were deployed to various Constituencies to provide technical support in case of any machine fault be it EVM machine or VVPAT machine.

From my discussions with stakeholders, we could gather extremely important information. Some of these are enumerated below:

i) 15 to 20% of VVPAT machines became "out of order" during the polling at the polling station itself or subsequently. On enquiry, it is also noted that these machines malfunctioned due to much heat generated inside the machines resulting damaging the "Thermal paper" used as "VVPAT paper slips. Secondly, the reflection of light above VVPAT machines made VVPAT "sensor" malfunctioning in some cases.

ii) About 5% EVM machines found to have certain technical problem mostly during the poll.

Besides, machine fault, following are other reasons which may cause mismatch of EVM counts with VVPAT paper trails as per onsite observation of a Senior Engineer from ECIL who was on duty during polling of last election of Tripura etc.

It is also learnt that before commencement of actual polling, the Presiding officer concerned is supposed to give a Demo of functioning of EVM before all **political party representatives** by physically pressing each BUTTON for a fixed number of times and placing before them the result of "counts" of VVPAT paper trails and that of EVM. After the Demo, the paper slips are to be destroyed and both the EVM and VVPAT machined are to be "**initialized**" and sealed by the presiding officer. In case the EVM machine is sealed without "initializing", the memory of the EVM will keep the "demo-counts" stored. This can the source of mismatching of "counts" during auditing.

Based on above inputs, the following Sampling design has been formulated

2. Sampling Design:

Suppose there are "N" number of polling booths in a constituency and each polling has one or more than one EVM (since it is learnt if any EVM malfunctions the machine is sealed and a new EVM is used for rest

of polling process). And in a particular constituency the total number of EVMs deployed will be higher than "N" - the no. of polling booths.

Notations used: Let N = be the size of population which is the total number of Polling stations(booths) within a constituency.

Let n = be the sample size for the purpose of auditing.

As per the ORDER of EC dated 13th February 2018 on "mandatory verification of VVPAT paper slips", only one Polling Station will be selected per constituency namely, n=1

The question is whether the sample size "n"=1 is statistically valid sample size.

In the following paragraph, we will explain the basic methodology followed for sample selection.

3.Methodology:

Suppose:
There are k candidates contesting in a constituency
A polling booth in the constituency has P voters
i-th candidate got x_{1i} votes as per EVM count and x_{2i} votes as per VVPAT paper slips
O_1 is the total no. of NOTA votes, absentees and cancelled votes as per EVM counting
O_2 is the total no. of NOTA votes, absentees and cancelled votes as per VVPAT print-outs

Then ideally,

$$\sum_{i=1}^{k} x_{1i} + O_1 = \sum_{i=1}^{k} x_{2i} + O_2$$

This may not happen due to various reasons as stated above and but it is necessary to verify whether the difference between two sets of "counts" are due to RANDOM effect or due to faulty EVM . Random effect may include non-

initialization of EVMs before commencement of polling at a polling booth during an election, as mentioned at 1(ii) above or other formalities.

Suppose:

α = proportion of EVMs is presumed to be defective (as found during auditing)

$\beta = 1 - \alpha$ = proportion of EVM machines having no problem.

Since Statistics deals with chance variable there may be some error in making decision based on "sample" even under "Random Sampling". Thus, we attach a level of "CONFIDENCE" linked to our decision (it may be 95% or 99%, say) so that one can say the statistical result is at least 95% (or 99%) correct. These figures are called "confidence level". For the purpose of auditing it is better to take higher confidence level namely, 99%

Now in order to find out the sample size (n out of N as defined above)

n= minimum sample of polling booths required for auditing for decision making substantiated by Statistical theory;

According to Statistical methodology (can be found in any book on Sample survey or UN publication), the minimum sample size (n) is given below presuming "N" is quite large:

$$n = Z^2 \times \frac{\alpha\beta}{e^2}$$

where Z = standard normal deviate and

e = degree of accuracy required often known as "margin of error"

[design effect = 1 since the sample design uni-stage Simple Random Sampling without replacement (SRSWOR)]

In case, where the value of "N" is small or finite, finite population correction will be used namely,

The finite population corrected sample size (n') is given by $n' = n\ X\ FPC$;

where FPC= $\{(N-n)/(N-1)\}^{1/2}$

Hereafter we shall call fpc corrected n' as "n" for the sake of simplicity.

Table: Finite population corrected Sample size with 99% confidence level

Probable number of Polling Booths within a constituency	Margin of error = 2%	Estimate of Sample size with e=2%	Margin of error =5%	Estimate of Sample size with e=5%
(1)	(2)	(3)	(4)	(5)
200	2%	69	5%	24
220	2%	82	5%	24
240	2%	92	5%	24
260	2%	99	5%	25
280	2%	105	5%	25
300	2%	110	5%	25
320	2%	114	5%	25
340	2%	118	5%	25
350	2%	121	5%	25

(Note: Minimum value of α has been used for above calculation. With Higher value of α, the estimates of sample size "n" will go up.)

Conclusion: It is a matter of decision of EC to choose the "margin of error" as 2% or 5% accordingly, the sample size will depend.

4.Statistical Testing of Hypothesis

Since share of votes in respect of political party "Y" as per two machines (EVM and VVPAT) may (or may not also) vary in both directions, it is not DESIRABLE to come out with a final conclusion on the basis of outcome of verification based on sample size proposed. As mentioned in the beginning, the mismatch between EVM counts with VVPAT counts could be due to several reasons other than faulty EVMs.

It may be noted that if a fresh sample of "n" polling booths are chosen one may get even opposite result. In other words, if all (or majority) EVM machines show higher figure as compared to VVPAT count in respect of a political Party (say X) it does not necessarily prove any biasness of EVMs. In such situation, it is

necessary to conduct **"Statistical Test of Significance"** to prove whether the EVMs are biased in favour of a political party. The method of Testing of Hypothesis is an instrument for finding out the truth.

Let us now work on proportion of votes recorded in favour of a candidate "Y" by two different machines

Let p_1 = is the proportion of VOTES received as per EVM counts in respect of "Y" candidate as compared total vote cast in EVM

and p_2 = is the proportion of VOTES received as per VVPAT counts in respect of "Y" candidate as compared total paper slips found in VVPAT.

We may now come across following situation:

i) EVM proportion of Votes are more: $p_1 > p_2$

ii) TTVAT proportion of Votes are more: $p_1 < p_2$

iii) EVM and VVPAT proportions are equal: $p_1 = p_2$

Where $p_1 = x_1/n_1$

where x_1 = Total votes received by "Y" candidate as per count of all EVMs

and n_1 = Total number of votes cast in favour of all candidates as per EVMs

Where $p_2 = x_2/n_2$

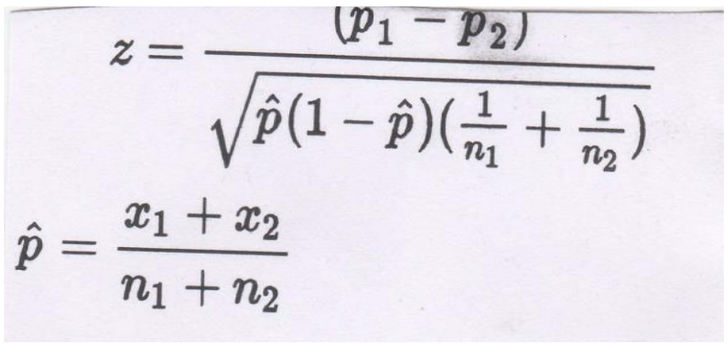
x_2= Total votes received by "Y" candidate as per count of paper slips of VVPAT

n_2 = Total number of votes cast in favour of all candidates as per VVPAT slips

(Please note that n_1 and n_2 above are different from *sample size (n) we have talked earlier*)

Now in order to derive at a conclusion that both EVMs and VVPATs machines are reliable, we will use the following Statistical Test for which our NULL Hypothesis will be $H_0(P_1 = P_2)$ which we will test against the alternative Hypothesis $H_1(P_1 \neq P_2)$, where P1 and P_2 are the TRUE values of p_1 and p_2 which are UNKNOWN

To Test we will calculate a test-statistic (not statistics) as below for testing of sample proportions:



$$z = \frac{(p_1 - p_2)}{\sqrt{\hat{p}(1-\hat{p})(\frac{1}{n_1} + \frac{1}{n_2})}}$$

$$\hat{p} = \frac{x_1 + x_2}{n_1 + n_2}$$

Now accept the null Hypothesis $H_0(P_1 = P_2)$ if the value of $Z < 1.96$. That means the count of EVM machines for the is NOT BIASED towards the candidate "Y". Otherwise, there is every reason to suspect the EVMs concerned.

Such test can be done for other parties and also for other constituencies wherever there is question of doubt expressed by any political parties.

6. Is there any need for stratification?

The way the sampling design has been explained above there is no need for any stratification.

Brief-Bio of Expert - Dr. Swaraj Kumar Nath

Dr. Nath is MSc in Statistics (Gold Medalist) from Calcutta University. He did his PhD in development of innovative models for measurement of "Export Swing" technology.

Joined Indian Statistical Service in 1971. Former Director-General, Central Statistical Organisation and Chief Economic Census Commissioner of India. Did pioneering work in Computerisation of Foreign Trade Statistics. Worked with National Sample Survey of India.

Active member of many Expert groups of United Nations, World Bank, SIAP, Japan. After his superannuation he has been working as International Consultant to UNFAO, UNIDO, WTO, UNSIAP, UNDP, World Bank, ILO, ESCAP, GIZ, ADB, SAARC, PARIS21(OECD).

Important assignments/contributions: "Sampling Advisor" to UNDP (Georgia) and ILO and assisted Russia in conducting multiple surveys in an integrated form. Pioneering work on developing model for "Global Value Chain" for FAO/UNIDO/WTO and creation of SAARCSTAT under SAARC. Setting up Ghana Statistical Training Centre. Developing blue print for "Implementation of Human Rights in Turkmenistan" for UNDP and online Gender database "G-datashop" for SAARC'

Recently he developed "costing model" for development of Integrated Land ports on India-Bangladesh and India-Nepal borders as ADB Consultant.

Prashant Bhushan

(TRUE COPY)

ANNEXURE: R9

Policy Watch

No. 7

Winning Voter Confidence: Fixing India's Faulty VVPAT-based Audit of EVMs

K. Ashok Vardhan Shetty

THE HINDU CENTRE
for
Politics and Public Policy

The Hindu Centre for Politics and Public Policy, Chennai, is an independent platform for exploration of ideas and public policies. As a public policy resource, our aim is to help the public increase its awareness of its political, social and moral choices. The Hindu Centre believes that informed citizens can exercise their democratic rights better.

In accordance with this mission, The Hindu Centre's publications are intended to explain and highlight issues and themes that are the subject of public debate, and aid the public in making informed judgments on issues of public importance.

Cover Photo: View of an Election Counting Centre during the 2018 Assembly Elections in Bengaluru on May 15, 2018. Photo: Sampath Kumar G P

Winning Voter Confidence:
Fixing India's Faulty VVPAT-based Audit of EVMs

K. Ashok Vardhan Shetty

TABLE OF CONTENTS

ABSTRACT

As the world's largest democracy gears up for a season of elections, including the 2019 General Election, there is an urgent need to examine the integrity of the electoral process. Electronic Voting Machines (EVMs) are 'black boxes' in which it is impossible for voters to verify whether their votes have been recorded correctly, and counting mistakes and frauds are undetectable and unchallengeable.

The 'voter verified paper audit trail' (VVPAT) is an additional verifiable record of every vote cast that allows for a partial or total recount independent of the EVM's electronic count. It is a critical safeguard that can help detect counting mistakes and frauds that would otherwise go undetected. The success of the VVPAT audit, however, depends on a proper, statistically acceptable, and administratively viable sample plan.

The Election Commission of India (ECI)'s prescription of a *uniform* sample size of just *"one polling station (i.e. one EVM) per Assembly Constituency"* for all Assembly Constituencies and all States stirs up an avoidable controversy and diminishes voter confidence. The ECI has not made public as to how it arrived at this sample size, and it has also *not clearly specified the population to which this sample size relates*. The latter is important because in the event of a defective EVM turning up in the sample, the hand counting of VVPAT slips will have to be done for all the remaining EVMs of the *specified population*.

In this Policy Watch, **K. Ashok Vardhan Shetty**, a former Indian Administrative Service (IAS) officer, demonstrates that the sample size prescribed by the ECI for VVPAT Audit is a statistical howler that fails to conform to fundamental sampling principles, leading to very high margins of error which are unacceptable in a democracy. By failing to detect outcome-altering miscounts due to EVM malfunction or fraud, it defeats the very purpose of introducing VVPAT. Spending hundreds of crores of rupees on procurement of VVPAT units makes little sense if their utilisation for audit purposes is reduced to an exercise in tokenism.

This report suggests statistically correct—and administratively viable—sample sizes to eliminate the risk of electoral fraud and infuse public confidence in the electoral process. It suggests ways in which the ECI can set the controversy at rest and make a beginning with the elections for 5 States whose counting is scheduled for December 11, 2018.

I. INTRODUCTION

"Statistical thinking will one day be as necessary for efficient citizenship as the ability to read and write."[1]

H.G. Wells
[1866-1946]

Electronic Voting Machines (EVMs) have many advantages including ease of operation, reduction of invalid votes cast and the speeding up of counting. But they also have some glaring disadvantages. EVMs are 'black boxes' in which it is impossible for voters to verify whether their votes have been recorded and counted correctly. There is always some risk of the votes cast being lost due to equipment malfunction. Electronic recounting is meaningless because it will simply yield the same total. Contrary to the claim by the Election Commission of India (ECI), even under election conditions and with all the security features and administrative safeguards in place, it is still possible for a determined attacker, acting in collusion with insiders, to tamper with EVMs and steal votes on a scale large enough to change election outcomes[2]. The problem with EVMs is that counting mistakes and frauds are undetectable and the losers are left with no means to challenge the results.

It follows that EVMs are not fully reliable and there should be an additional verifiable physical record of every vote cast. This is called the *'voter verified paper audit trail'* (VVPAT). After a voter casts his vote, he gets to view for a few seconds - before it drops into a box - a printed paper slip so that he can verify if his vote has been recorded correctly. It provides a back-up in case of loss of votes due to equipment malfunction, and allows for a partial or total recount of the paper slips independent of the electronic count. In 2013, the Supreme Court passed an order mandating the use of EVMs with VVPAT units and directed the ECI to implement them in a phased manner.

The importance of conceptual clarity

VVPAT is an additional safeguard, a very critical, and final safeguard, which can help detect counting mistakes and frauds that would otherwise go undetected. But VVPAT, by itself, cannot

prevent EVM malfunction or tampering. If it is to have any real security value, it should be backed by a proper *sampling process*. This involves 4 steps:

(1) Defining the *population*[3] clearly in terms of 'population units' (polling stations or EVMs) and 'population boundaries' (e.g. Assembly Constituency, Parliamentary Constituency, State, country). The population size varies depending upon how the boundaries are set.

(2) Determining the correct sample size, or what is called the *statistically significant sample size,* of EVMs whose VVPAT slips will be hand counted. The sample size should not only be statistically sound but also administratively viable.

(3) *Random sampling* of the EVMs, preferably by draw of lots by the candidates or their authorised representatives on the counting day.

(4) A *'decision rule'*, based on the sample results, to determine whether the election results can be declared or the hand counting of VVPAT slips should be done for all the remaining EVMs of the population. The latter entails additional time and effort but is justified by the need to declare the election results correctly without any outcome-altering miscounts due to EVM malfunction or fraud. Two types of decision rules are possible:

   a) Comparison of the EVM electronic count and the VVPAT hand count for the sample of EVMs to verify if *(i) the two totals tally,* and *(ii) the votes secured by the leading candidate tally*. If both tally, then there is no problem and the election results based on the EVM count can be declared[4]. But if any one or both do not tally, then there is a problem and the hand counting of VVPAT slips should be done for all the remaining EVMs of the population and the election results declared only on the basis of the VVPAT count.

   b) Adoption of *"Lot Acceptance Sampling*", a statistical quality control technique widely used in industry and trade the world over for assuring the quality of incoming and outgoing goods. The decision, based on *counting the number of defectives in a sample*, can be to accept the lot, reject the lot, or even, for sequential sampling schemes, to take another sample and then repeat the decision process.

   An 'acceptance number' - 'c' - is specified. If the number of defectives found in the sample is less than or equal to 'c', the lot is accepted; otherwise, the lot is rejected. Unlike industry and trade where the presence of a few defectives in the sample may be tolerated depending upon the size of the lot and the quality norms, in the election context, the acceptance number 'c' will have to be *zero*.

   In other words, the election results can be declared only if no 'defective EVM'[5] is found in the randomly drawn sample of EVMs. If even a single defective EVM is detected in the

sample[6], the hand counting of VVPAT slips should be done for all the remaining EVMs of the population and the election results declared only on the basis of the VVPAT count.

The second option is preferable and easier to implement. For the rest of this paper, it will be assumed that this decision rule will be followed.

Unfortunately, the issue of sampling procedure for VVPAT-based audit of EVMs has received scant attention by policy-makers, the academic community, and most importantly, the voting public in India until recently[7]. This Policy Watch aims to point out the statistical weakness of the procedure that is in place and make the case for statistically significant sample sizes that are also administratively viable. VVPAT-based audits are the final check and remedy against electoral fraud. The ECI, which oversees the largest electoral exercise in the democratic world should ensure that this audit is both infallible and statistically acceptable, and correctly reflect voter-choice.

The error of uniform sample size

The ECI has courted controversy by prescribing a *uniform* sample size of *"one polling station (i.e. one EVM) per Assembly Constituency"* for all Assembly Constituencies and all States. This sample size was adopted in the Assembly Elections for Gujarat and Himachal Pradesh held in November-December 2017; for Meghalaya, Nagaland and Tripura held in February 2018; and for Karnataka held in May 2018.

For reasons best known to it, the ECI has not made public as to how it arrived at this sample size, and it has also *not clearly specified the population to which this sample size relates*. The latter is important because in the event of a defective EVM turning up in the sample, the hand counting of VVPAT slips will have to be done for all the remaining EVMs of the *specified population*.

A mistake with grave consequences

As we shall demonstrate shortly, the sample size prescribed by the ECI is a statistical howler that fails to conform to scrutiny of statistical principles, leading to very high margins of error which are unacceptable in a democracy. It is open to legal challenge on this score. It defeats the very purpose of introducing VVPAT and is fraught with all the risks of conducting elections with paperless EVMs.

In something as important as ensuring the integrity of the election process – a process which in any case takes about 2-3 months from the date of announcement to the date of counting – a delay of a few hours or even a couple of days in hand counting VVPAT slips of a larger sample of EVMs should not matter at all. Spending hundreds of crores of rupees on procurement of VVPAT units makes little sense if their utilisation for audit purposes is reduced to an exercise in tokenism. This could result in the easily avoidable perception that the ECI is afraid that pro-active implementation of VVPAT may show up many EVMs to be defective and raise a question mark about the sanctity of the election process.

II. SOME ODDITIES OF STATISTICAL SAMPLING

"The mind is not designed to grasp the laws of probability, even though the laws rule the universe."[8]

Steven Pinker

[Johnstone Family Professor of Psychology, Harvard University]

Statistical sampling is fundamental to almost all of our understanding of the world. It provides a means of gaining information about a population without the need to examine the population in its entirety. The latter is usually neither cost-effective nor practicable. No estimate taken from a sample is expected to be exact, and there is likely to be some difference between the sample estimate and the actual population value. 'Confidence level' is how certain one wants to be that the population value is within the sample estimate and its associated margin of error. The purpose of statistical sampling is to draw conclusions about a *suitably defined population* on the basis of the *most economic sample* for a *specified level of confidence* in the results.

If I were to tell a layperson that (for a given set of parameters) the sample size required for a population size of one lakh is 458 but the sample size required for a population size of one crore (100 times greater) is only 459, he is likely to think that I am mistaken. It seems counter-intuitive but that is the way statistical sampling theory works! As population size (N) increases, the sample size (n) also increases but at a much slower rate and 'hits a plateau' beyond some point so that *further increases in population size have no effect on the sample size*. The following example illustrates how sample size varies with population size.

Let us assume that one per cent of the EVMs used in an election are defective. [It must be remembered that a 'defective EVM', according to our definition, is one which has a *mismatch* between the EVM count and the VVPAT count]. Random samples are drawn *without replacement*.[9] Detecting a defective EVM is treated as a 'success'. The sample sizes required, for various population sizes, *for 99 per cent probability of detecting at least one defective EVM* are shown in **Table 1**, and are also displayed graphically in **Chart 1**. [All Tables and Charts compiled by author.]

Table 1

How Sample Size varies with Population Size

Population Size (N)	*Sample Size (n)*	*% of n to N*
100	99	99
200	180	90
500	300	60
1,000	368	36.8
2,000	410	20.5
5,000	438	8.76
10,000	448	4.48
20,000	453	2.27
50,000	457	0.91
1,00,000	458	0.46
2,00,000	458	0.23
10,00,000	459	0.05
20,00,000	459	0.02
1,00,00,000	459	0.005

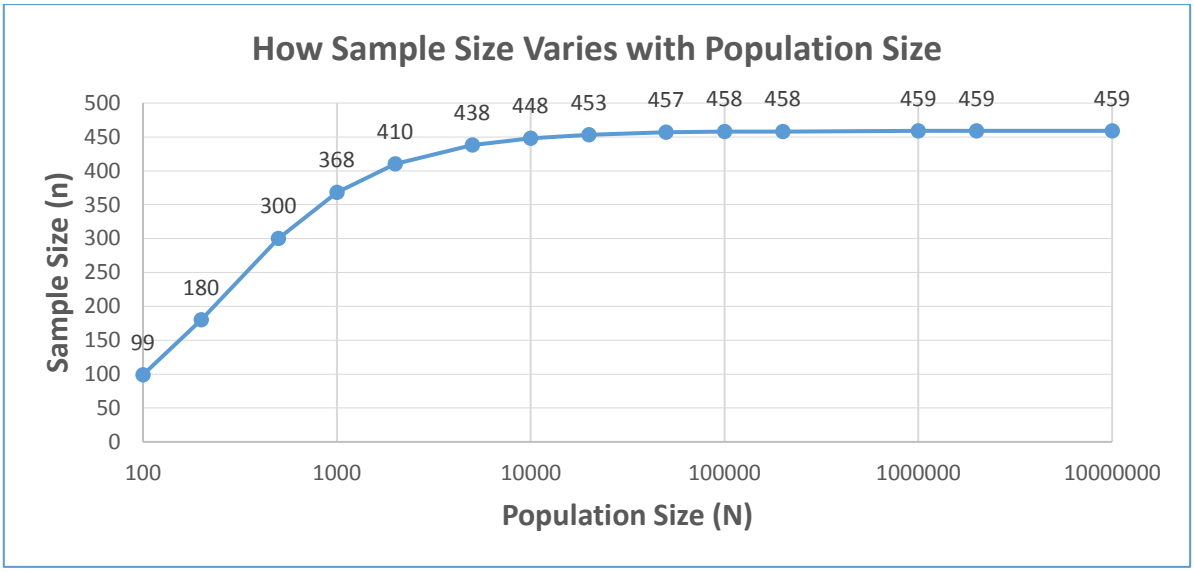
Source: Compiled by author using Hypergeometric Distribution.

It is seen that when the population size of EVMs is 100, the sample size is 99 i.e. *it is nearly as big as the population size*. When the population size is 1,000, the sample size is 368 and when the population size is 10,000, the sample size is 448. But the 'sampling fraction' (n/N) i.e. the sample size relative to the population size is seen to decrease rapidly. The sample size then 'hits a plateau' and increases to only 458 for a population size of one lakh; to only 459 for a population size of ten lakhs, and remains at 459 even for a population size of one crore. *In other words, for big populations, the population size is irrelevant to sample size.*

Chart 1 makes the point clearer. [To avoid the crowding of figures at the lower end and for ease of visualisation, the figures are plotted on a logarithmic scale]. In this particular example, it is seen that *increase of population size beyond about 10,000 (N/n > 20) has little or no impact on the sample size.*

Chart 1

Graphic Representation of Table 1



The figures in **Table 1** also tell us how *statistical sampling is superior to arbitrary, non-statistical sampling* such as, say, a flat "10 per cent sample" (n=0.1N). With statistical sampling, the sample size required is 99 for a population size of one hundred, and just 459 for a population size of one crore. But with a flat "10 per cent sample", for a population size of one hundred, the sample size is 10 which is too small and statistically incorrect; and for a population size of one crore, it is 10 lakhs which is too big and administratively impractical. Thus, a flat "10 per cent sample" is utterly wrong for small population sizes and is utterly inefficient for very big population sizes.

As Robert Schlaifer, author of a classic text on Statistics, puts it:

> "One of the most common 'vulgar errors' concerning sampling is the belief that the reliability of a sample depends upon its percentage relationship to the population. Many businessmen operate sampling inspection plans which call for inspection of a certain percentage of each lot – usually 10 per cent. . . however, this policy is completely misguided: unless the sample takes in a really substantial fraction of the population, its reliability depends on its absolute rather than its relative size."[10]

The relevance of the foregoing discussion to VVPAT-based audit of EVMs should be obvious. In the election context, *depending upon how the population is defined, the population size can vary widely as shown in* **Table 2** below.

Table 2

How population is defined and its effect on population size

Population Boundary	*Population Size (N) (Number of EVMs)*
Assembly Constituency	≈ 30 to 300
Parliamentary Constituency	≈ 300 to 1800
A State as a whole	Ranging from 589 (Sikkim) to 1,50,000 (U.P) For 9 States N < 10,000 For 20 States N > 10,000
India as a whole	≈ 10,00,000

≈ is the symbol for 'approximately equal'.

The importance of defining the 'population'

Studying the figures in **Table 1** and **Table 2** together, it is obvious that if the EVMs used in an *Assembly Constituency* are defined as the population, the population size (N) will be very small; the sampling fraction (n/N) will be very big; and the sample size (n) will vary considerably across Assembly Constituencies. The same is true if the EVMs used in a *Parliamentary Constituency* are defined as the population.

If the EVMs in a State as a whole are defined as the population, there is considerable variation in population size from the very small (Sikkim) to the very big (Uttar Pradesh). For the nine smaller States with population size less than 10,000 EVMs, the sampling fraction (n/N) will be quite big and the sample size will vary considerably across the States. For the 20 bigger States with population size greater than 10,000 EVMs, the sample size will 'hit a plateau' in the 450s and further increase in population size will have little or no effect on it.

If the EVMs used in India as a whole are defined as the population, due to the 'plateau effect', the sample size is just one more than that for U.P.

Chapter 4 will elaborate upon these points and explain why the uniform sample size of "one EVM per Assembly Constituency" for all Assembly Constituencies and all States presently adopted by the ECI is completely off the mark, and with serious implications.

The ECI's critics have not fared any better. They are also guilty of committing the 'vulgar error' (to use Robert Schlaifer's telling phrase) of demanding arbitrary, non-statistical sample sizes like

"10 per cent of the EVMs per Assembly Constituency" for VVPAT-based audit of EVMs. This is precisely what Congress leader Kamal Nath did in a writ petition filed before the Supreme Court[11].

Other critics of the ECI have demanded "15 per cent samples" and even "25 per cent samples" under the mistaken impression that a "bigger percentage" guarantees greater accuracy of results. It does not. What guarantees greater accuracy of results is a statistically significant sample size based on a properly defined population and the appropriate probability distribution model.

III. HYPERGEOMETRIC DISTRIBUTION MODEL: AN EXACT FIT FOR EVM SAMPLING

"Probability theory is nothing more than common sense reduced to calculation".

Pierre-Simon Laplace
[French Mathematician, 1749-1827]

Consider the following two problems:
A: There are 100 fish in a pond. 95 of them are grey and five are green. The fish are caught without replacement. The characteristic of interest here is a green fish, catching which is treated as a 'success'. If we catch a random sample of, say, three fish, what is the probability that the sample will contain at least one green fish?

B: There are 100 EVMs in an Assembly Constituency. 95 of them are good while five are defective. The characteristic of interest here is a defective EVM, detecting which is treated as a 'success'. If we pick a random sample of, say, three EVMs, what is the probability that the sample will contain at least one defective EVM?

Problems *A* and *B* are exactly equivalent. They are both classic examples of what is called a *Hypergeometric Probability Distribution*. The probabilities can be calculated using the standard formula for Hypergeometric Distribution[12] or using Excel or an online calculator[13] or any of the statistical analysis software.

The answer to problems *A* and *B* is that there is only a 14.4 per cent probability of the sample size of three having at least one 'success'[14].
If we wish to be 99 per cent sure of having at least one 'success', then the sample size should be increased to 59[15].

The Hypergeometric Distribution model is an 'exact fit' to the EVM problem and should form the basis of the sampling plan for VVPAT-based audit of EVMs[16].

In the fish problem, if the number of green fish in the pond is large, say, 50 out of 100, then it is easy to catch a green fish even if you cast the net narrow. But if the number of green fish in the

pond is very small, say, only five out of 100, then you will have to cast the net much wider in order to catch a green fish.

Therefore, with the Hypergeometric Distribution, as the proportion (P) of the 'characteristic of interest' in the population decreases, the sample size (n) required for detecting at least one 'success' increases. Applied to VVPAT-based audit of EVMs, it means that *the sample size (n) required for detecting defective EVMs is the biggest when the proportion of defective EVMs (P) is assumed to be very small and it gets smaller when P gets bigger*. **Table 3** and **Chart 2** (compiled by the author) make this point clear.

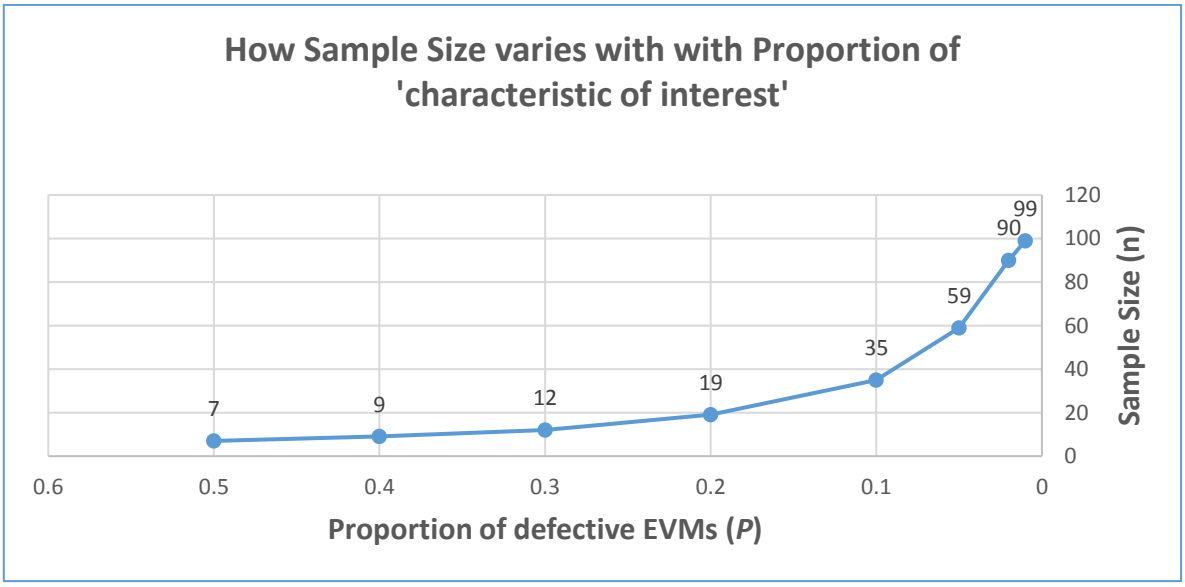
Table 3

How Sample Size varies with the Proportion of the 'characteristic of interest'

Population Size (N) = 100 EVMs.

Proportion of defective EVMs (P)	Number of defective EVMs in the population	Sample Size (n) required for 99% probability of detecting at least one defective EVM in the sample
0.50	50	7
0.40	40	9
0.30	30	12
0.20	20	19
0.10	10	35
0.05	5	59
0.02	2	90
0.01	1	99

Chart 2



In the case of EVMs employed in an election, the proportion of defective EVMs (P*)* is *unknown*. It may be zero or 0.01 or 0.02 or 0.10 or whatever. The ECI thinks that P is zero or very close to zero. But just because EVM tampering didn't take place in the past, we can't assume that it won't take place sometime in the future. So even if P was zero or very close to zero in the past, there is no guarantee that it won't be high in the next election. Any debate on the precise value of P is bound to be uninformed and therefore, inconclusive as each one's guess would be as good as the other's.

With the Hypergeometric Distribution model, the debate about the precise value of P is inconsequential because the sample size is the greatest when P is very close to 0 (which is what ECI claims it is), and it becomes lesser as P increases. *So, the sample size calculated for P = 0.01 (one per cent) will hold good for all higher proportions of defectives. It therefore obviates the need to make questionable assumptions about the value of P or estimate it based on the data of past trials which may or may not be fully reliable.*

When can rigging be 'successful'

A question may be asked as to why we should not assume a value for P that is less than one per cent*,* as then the sample size required will be even bigger. *The following thought experiment will show that the actual value of P required for the successful rigging of an election, even in a neck-to-neck contest, needs to be much higher than one per cent.*

In India, the average number of polling stations (N.B. There is one EVM per polling station) per Assembly Constituency is around 240. The actual number of polling stations in an Assembly Constituency varies widely from State to State and sometimes even within a State - from about less than 30 to about 300-plus polling stations. In what follows, the figures are hypothetical but the logic holds good, even if we assume different sets of figures.

On an average, a polling station has about 900 voters attached to it out of whom about 65 per cent may vote. That means about 600 votes may be cast in a typical EVM. Not all of the votes can be 'stolen' (i.e. transferred to the winning candidate) by tampering with the EVM. There are *practical limits* to the maximum percentage of votes of an EVM that may be 'stolen' without attracting the ECI's adverse attention. Let us assume that this is about 20 per cent of the votes cast i.e. 120 votes. Consider an Assembly Constituency where the election is expected to be very close. Let us assume that the contest is only between the candidates of the two main parties and the rest don't matter,

and that the votes are 'stolen' only from the rival candidate of the other main party. Clearly, it is not sufficient to tamper with just one EVM to be sure of victory when the number of votes that can be 'stolen' is only 120.

A potential attacker may have to tamper with at least five EVMs in an Assembly Constituency to 'steal' at least (120 x 5) = 600 votes from his rival candidate, which would make him reasonably sure of victory. Even in a large-sized Assembly Constituency with 300 EVMs, five EVMs work out to 1.5 per cent of the total EVMs; for an average-sized Assembly Constituency with 240 EVMs, it is 2.1 per cent of the total; for an Assembly Constituency with 100 EVMs, it is five per cent of the total; for even smaller Assembly Constituencies, the percentage is much higher.

So, our assumption of "one per cent defective EVMs" as the value for P is itself on the lower side, and will yield the most conservative (i.e. biggest) sample size that is adequate for our purpose. Let us recall that for higher values of P, the sample size required is *smaller*.

IV. THE 'ONE EVM PER ASSEMBLY CONSTITUENCY' FALLACY

"A statistical analysis, properly conducted, is a delicate dissection of uncertainties, a surgery of suppositions."[17]

– M.J. Moroney

[*Facts from Figures, 1951, p 3*]

In Statistics, there are no hard-and-fast rules as to how a population should be defined except that (i) the boundaries of the population should clearly separate items which are of interest to us from items which are not, and (ii) the sampling process is administratively viable.

We now proceed to show that whereas the boundaries for the population of EVMs can be an *Assembly Constituency,* or a *Parliamentary Constituency,* or *a State as a whole,* or *India as a whole*, only one of these populations [a State as a whole] is administratively viable.

It must be remembered that in the event of a defective EVM turning up in the chosen sample of 'n' EVMs, *the hand counting of VVPAT slips will have to be done for all the remaining (N – n) EVMs forming part of the population.*

Let:

- W_n represent the administrative workload involved in hand counting VVPAT slips for the chosen sample of 'n' EVMs, and
- $W_{(N-n)}$ represent the administrative workload involved in hand counting VVPAT slips of all the remaining (N–n) EVMs in the population.

There has to be a trade-off between W_n and $W_{(N-n)}$. As we shall demonstrate presently, if W_n is small, $W_{(N-n)}$ is big and *vice versa*. Both cannot be small. *The ECI is at liberty to define 'population' suitably as long as it is commonsensical and represents the right balance between the administrative workloads W_n and $W_{(N-n)}$.*

In all the scenarios that follow, we assume a very low proportion of defective EVMs (P = one per cent or 0.01) and work out the sample sizes required, using the Hypergeometric Distribution model, for 99 per cent probability that the sample will detect at least one defective EVM.

1. **EVMs of an Assembly Constituency as 'population'**: Let us assume four hypothetical Assembly Constituencies A, B, C and D with 50, 100, 200 and 300 polling stations (EVMs) in them respectively. The results are shown in **Table 4.**

Table 4

Sample Sizes if EVMs of an ASSEMBLY CONSTITUENCY are the Population

Assembly Constituency	Population Size (N) [Total number of polling stations in the constituency]	Number of defective EVMs in the population @ P = 0.01	Sample Size (n) required	% of n to N	*Probability* that the *ECI - prescribed sample size* of "one EVM per Assembly Constituency" *will fail to detect a defective EVM*
A	50	1#	50	**100**	**98%**
B	100	1	99	**99**	**99%**
C	200	2	180	**90**	**99%**
D	300	3	235	**78.3**	**99%**

- rounded off to the next highest integer.

EVMs employed in an Assembly Constituency would seem to be the logical choice of 'population' for Assembly Elections. But it is seen that *the resulting sample sizes are nearly as big as the respective population sizes leaving little or no scope for statistical sampling*! We may as well have paper ballots and count them 100 per cent instead of having EVMs and hand-counting the VVPAT slips of between 78.3 per cent and 100 per cent of EVMs in each Assembly Constituency!

Moreover, in the event of a 'defective EVM' turning up in the chosen sample, the number of the remaining EVMs in the population whose VVPAT slips need to be counted i.e. (N – n) is very less in this case. But this advantage is more than negated by the fact that the sample sizes are nearly

as big as the population sizes. In other words, workload W_n is enormous even if workload $W_{(N-n)}$ is very less.

So, EVMs used in an Assembly Constituency are not an appropriate choice for 'population'.

The last column of **Table 4** shows why the ECI-prescribed sample size of "one EVM per Assembly Constituency" is utterly wrong. *The probability that the sample will not detect a defective EVM is 99 per cent!*[18] (It is 98% for Assembly Constituency A only because of the rounding off).

2. **EVMs of a Parliamentary Constituency as 'population'**: A Parliamentary Constituency typically comprises about six Assembly Constituencies and may have between 300 and 1800 polling stations. Consider four hypothetical Parliamentary Constituencies P, Q, R and S with 300, 600, 1200 and 1800 polling stations in them. The results are shown in **Table 5**.

Table 5

Sample Sizes if EVMs of a PARLIAMENTARY CONSTITUENCY are the Population

Parliamentary Constituency	Population Size (N) [Total number of polling stations in the constituency]	Number of defective EVMs in the population @ P = 0.01	Sample Size (n) required	% of n to N	*Probability* that the *ECI - prescribed sample size* of "one EVM per Assembly Constituency" # *will fail to detect a defective EVM.*
P	300	3	235	**78.3**	**94.1%**
Q	600	6	321	**53.5**	**94.1%**
R	1200	12	381	**31.75**	**94.1%**
S	1800	18	405	**22.5**	**94.1%**

- This works out to a sample size of six EVMs per Parliamentary Constituency as per ECI norms.

EVMs employed in a Parliamentary Constituency would seem to be the *logical* choice for 'population' for Parliamentary Elections. But it is seen that the resulting sample sizes are very big relative to the respective population sizes and do not serve the purpose of statistical sampling i.e. workload W_n involved in the hand counting of VVPAT slips for the chosen sample size (n) is enormous. In the event of a defective EVM turning up in the chosen sample, the number of the

remaining EVMs in the population whose VVPAT slips need to be counted, (N – n), is also quite large i.e. workload $W_{(N-n)}$ is also considerable.

So, EVMs of Parliamentary Constituency are not an appropriate choice for 'population'. It is not administratively viable on both counts [W_n as well as $W_{(N-n)}$]. The last column of **Table 5** shows why the ECI-prescribed sample size of "one EVM per Assembly Constituency" is seriously wrong even in this case. *The probability that it will fail to detect a defective EVM is 94.1 per cent.*

3. **EVMs used in a State as a whole as 'population'**: Let us consider the five States that will have Assembly Elections in November-December 2018 – Mizoram, Chhattisgarh, Telangana, Rajasthan, and Madhya Pradesh. The results are shown in **Table 6**.

Table 6

Sample Sizes if EVMs of a STATE AS A WHOLE are the Population

State	Number of Assembly Constituencies	Population Size (N) [Total number of polling stations in the State]	Sample Size (n) required for the State as a whole	% of n to N	Average Number of EVMs per Assembly Constituency whose VVPAT slips should be hand counted	*Probability* that the *ECI-prescribed sample size* of "one EVM per Assembly Constituency" # *will fail to detect a defective EVM*
Mizoram	40	1164	370	**31.79**	**10**	**65.6%**
Chhattisgarh	90	23672	455	**1.92**	**5**	**40.3%**
Telangana	119	32574	455	**1.40**	**4**	**30.1%**
Rajasthan	200	51796	457	**0.88**	**2**	**13.3%**
Madhya Pradesh	230	65341	457	**0.70**	**2**	**9.9%**

- This works out to a sample size of 40 EVMs for Mizoram as a whole, 90 EVMs for Chhattisgarh as a whole, 119 EVMs for Telangana as a whole, and so on as per ECI norms.

As the population size of EVMs is very small for Mizoram, the sampling fraction (n/N) is big but this is inevitable. For the remaining 4 States, the sampling fraction is very reasonable and is administratively viable. The average number of EVMs to be hand counted per Assembly Constituency is also indicated (fractions rounded off to the *next higher integer*). It is seen that the administrative workload W_n involved in the hand counting of VVPAT slips for the chosen sample size is minimal.

Since the sample size is for *a State as a whole*, in the event of a defective EVM turning up in the chosen sample, the VVPAT slips of all the remaining EVMs in the population (*throughout the State*) will need to be hand counted and not just EVMs of the particular Assembly Constituency in which the defective EVM was detected. The workload $W_{(N-n)}$ involved in the hand counting of VVPAT slips for the remaining (N – n) EVMs is considerable. As already indicated, there has to be a trade-off between W_n and $W_{(N-n)}$; both can't be small. Whereas W_n is unavoidable, $W_{(N-n)}$ is contingent upon a defective EVM being discovered which may be rare. It is preferable to have a small or reasonable W_n and a large $W_{(N-n)}$ than *vice versa*.

Moreover, the purpose of VVPAT is not just to detect fraud but also to deter it. The knowledge that if a defective EVM turns up, full hand count of VVPAT slips of all EVMs will be done is a sufficient deterrent for any likely fraudster. It will also put pressure on the two EVM manufacturers (Bharat Electronics Limited and Electronics Corporation of India Limited) to improve the quality of their EVMs and VVPAT-units so that instances of malfunctioning of EVM or VVPAT unit are negligible.

The average number of EVMs to be hand counted per Assembly Constituency, which is just 'two for Rajasthan and Madhya Pradesh, may seem 'very small' and create a doubt in the mind of a layperson about its correctness. But when it is remembered that the sample size is for the "State as a whole" [457 for both States] and that the discovery of even a single defective EVM *anywhere in the State* among the sample of 457 will entail the hand counting of VVPAT slips of all the remaining EVMs in all the Assembly Constituencies of the State, our layperson will realise that the sample size is correct.

The last column of **Table 6** shows why the ECI-prescribed sample size of "one EVM per Assembly Constituency" is seriously wrong even in this case. *The probability that it will fail to detect a defective EVM varies from 9.9 per cent for Madhya Pradesh to 65.6 per cent for Mizoram.*

4. **EVMs of India as 'population'**: The results are shown in **Table 7**:

Table 7

Sample Size if INDIA AS A WHOLE is the Population

Unit	Number of Assembly Constituencies in India	Population Size (N) [Total number of polling stations in India]	Sample Size (n) required for India as a whole	% of n to N	Average Number of EVMs per Assembly Constituency whose VVPAT slips should be hand counted	*Probability* that the ECI-prescribed sample size of "one EVM per Assembly Constituency" # *will fail to detect a defective EVM*
INDIA	4120	10,00,000	459	**0.045**	0.11 [rounded off to **1**].	Almost **ZERO**

- This works out to a sample size of 4,120 EVMs (after the rounding off) for India as a whole.

It would appear that the ECI has arrived at its sample size of "one EVM per Assembly Constituency" by treating EVMs in India as a whole as 'population'. The ECI-prescribed sample size will work correctly only in this case. But the ECI as well as its statistical advisors seem to have overlooked two crucial aspects: *First,* since the sample size is for '*India as a whole'*, in the event of a defective EVM turning up in the chosen sample, the VVPAT slips of all the remaining EVMs in the population (*i.e. throughout India*) will need to be hand counted*, and not just EVMs of the particular Assembly Constituency in which the defective EVM was detected.* Can the ECI keep the declaration of results throughout India on hold and order the hand counting of all the remaining 99.96 per cent of EVMs in the country? Surely not. When EVMs used in the country as a whole are treated as the 'population', W_n becomes very small but this small sample size comes at a big 'price', viz. $W_{(N-n)}$ is too large and just not administratively viable in the event of a defective EVM turning up in a sample anywhere in the country.

Second, EVMs employed in 'India as a whole' can be treated as the 'population' *only for an all-India Parliamentary Election; not for individual State Assembly Elections.* When we have an Assembly Election for Mizoram or Telangana or Madhya Pradesh, the ECI should treat only the EVMs used in the 'State as a whole' as the 'population'. In that case, the sample size should be 370 for Mizoram; 455 for Telangana; and 457 for Madhya Pradesh which works out to an average of 10 EVMs per Assembly Constituency for Mizoram; four for Telangana; and two for Madhya Pradesh. *So, the ECI-prescribed sample size of "one EVM per Assembly Constituency" which may be appropriate for 'India as a whole' is illogical and inappropriate if used for Assembly Elections. So EVMs used in the country as a whole are also not an appropriate choice for 'population'.*

What should the ECI do?

As already stated, the ECI is at liberty to define the 'population' suitably as long as it is logical, statistically sound, administratively viable, and represents a proper trade-off between W_n and $W_{(N-n)}$. It is evident from the foregoing discussion that EVMs used in 'Assembly Constituency', 'Parliamentary Constituency' or 'the country as a whole' are NOT suitable choices for 'population'. *The only suitable choice, both for Assembly and Parliamentary Elections, are EVMs used in 'a State as a whole'.*

Is the ECI worried that the administrative workload $W_{(N-n)}$ involved in the hand counting of VVPAT slips *all over a State* on discovery of a stray defective EVM anywhere in the State is too much? It shouldn't be worried for 2 reasons:

(i) The ECI's present sample size holds good only when EVMs used in 'India as a whole' are treated as the 'population'. In the event of a defective EVM turning up anywhere in India, the hand counting of VVPAT slips must be done for VVPATs of all EVMs *in all constituencies throughout India*. In other words, the *status quo* is much worse.

(ii) The ECI has claimed 'perfect tallying' between EVM electronic counts and VVPAT hand counts in 843 constituencies in the past Assembly elections where VVPAT-units were deployed and its sample size of "one EVM per Assembly Constituency" was adopted. If this was indeed the case, the ECI has nothing to worry about as the biggest sample size for a State is only 458. But the correctness of the ECI's claim is open to question. *First,* there is a *bias in sample selection* when the defective VVPAT units that couldn't be replaced are left out from the population from which the sample of one EVM per Assembly Constituency is chosen. Since the percentage of defective VVPAT units on polling day was reportedly as large as 20 per cent, and *the polling went ahead in many of these polling stations without the VVPAT units*, the legitimacy of the population is open to question. *Second,* the ECI's minuscule sample size of "one EVM per Assembly Constituency" had very high margins of error and would have missed out on many defective EVMs which a larger, statistically sound sample may have detected.

If the ECI wants greater accuracy, it should go in for a sample size that will have **99.9 per cent** probability of detecting at least one defective EVM. The sample sizes for the five States are indicated in **Table 8**.

Table 8

Sample Sizes using A STATE AS A WHOLE as the Population

Percentage of defective EVMs (P) is assumed as 1%.

Probability of detecting at least one defective EVM is chosen as ***99.9%.***

State	Number of Assembly Constituencies	Population Size (N) [Total number of polling stations in the State]	Sample Size (n) required for the State as a whole	% of n to N	Average Number of EVMs per Assembly Constituency whose VVPAT slips should be hand counted
Mizoram	40	1164	508	**43.64**	**13**
Chattisgarh	90	23672	677	**2.86**	**8**
Telengana	119	32574	680	**2.09**	**6**
Rajasthan	200	51796	683	**1.32**	**4**
Madhya Pradesh	230	65341	685	**1.05**	**3**

The sample sizes and the *average* number of EVMs per Assembly Constituency whose VVPAT slips are to be hand counted are relatively greater in this case but are still reasonable and administratively viable.

Sample size determination is not a purely statistical exercise. Since elections are the bedrock of democracy and the *perceptions* of political parties and voters are important, the ECI would do well to opt for 99.9 per cent probability that the sample will detect at least one defective EVM.

The average number of EVMs to be hand counted per Assembly Constituency have been indicated in **Table 6** and **Table 8** so as to give an 'order-of-magnitude' figure vis-a-vis the present figure of one EVM per constituency. Since the sample is for a State as a whole and since the number of polling stations per Assembly Constituency may vary widely even within a State, the ECI may apportion the total sample among the various Assembly Constituencies *in proportion to the number of polling stations in each constituency and round off fractions to the next higher integer.* The rounding-off is likely to increase the sample size for each constituency slightly which is a good thing.

The State-wise sample sizes required have been worked out and are shown in **Annexure I** (for 99% probability of detecting at least one defective EVM) and **Annexure II** (for 99.9% probability).

It is best that the ECI do the necessary calculations and communicate to the Chief Electoral Officer (CEO) of each State the sample size for hand counting of EVMs' VVPAT slips (1) for the State as a whole, and (2) for each Assembly Constituency. Unless there is a significant change in the number of polling stations, the ECI should permanently 'fix' the sample size for the State as a whole and for each Assembly Constituency for all future elections.

There may be a problem for by-elections where an Assembly Constituency or a Parliamentary Constituency will have to be taken as the population and the sampling fraction for VVPAT-based audit will be very large as seen in **Table 4** and **Table 5**. But the ECI usually groups together several Assembly Constituencies and Parliamentary Constituencies for which by-elections have to be conducted. *The total EVMs used in all these by-elections put together* may be taken as the population which will yield an administratively viable sample size for VVPAT-based audit.

V. ECI MUST SET THE CONTROVERSY AT REST

"There are two possible ways to approach phenomena. The first is to rule out the extraordinary and focus on the "normal." The examiner leaves aside "outliers" and studies ordinary cases. The second approach is to consider that in order to understand a phenomenon, one needs to first consider the extremes - particularly if, like the Black Swan, they carry an extraordinary cumulative effect."[19]

- Nassim Nicholas Taleb

[Distinguished Professor of Risk Engineering, NYU Tandon School of Engineering]

Most people expect all swans to be white because that's what their experience tells them; a black swan is by definition a surprise. According to Nassim Nicholas Taleb, a "Black Swan Event" is characterized by the following three attributes. *First,* it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. *Second*, it carries an extreme impact. *Third,* it will seem obvious in hindsight with people asking why the warning signs were not noticed sooner. In sum: rarity, extreme impact, and retrospective (though not prospective) predictability.

The Great Depression of 1929, the precipitous demise of the Soviet bloc during 1989-91, the global financial crisis of 2008, and the Punjab National Bank-Nirav Modi scam of 2018 were some typical Black Swan Events. History is replete with them. Our inability to predict the course of history is due to our inability to predict Black Swan Events. According to Taleb, no matter how hard we try, it is very likely that the next Black Swan Event will also take us by surprise. So, while we should prepare for the specific threats that we envision we should not forget to also prepare for the unexpected.

Rigging of an election through EVM fraud fits Taleb's depiction of a Black Swan Event. The "unexpected" that the ECI should prepare for is EVM fraud. It may have a very low (but non-zero) probability and it may be unpredictable in terms of time and place. However, if EVM fraud were to occur, the damage to the sanctity of the electoral process will be immense. There is no point in regretting or rationalising after the event.

What is worse, without a credible VVPAT-based audit of EVMs, the fraud may be undetectable and may be carried on with impunity. The ECI should, therefore, move out from its comfort zone

and focus on "outlier" events like EVM fraud. The risk of EVM fraud, howsoever remote, is something the political parties and voters of India will never accept – not because they overestimate the risk but because the cost of the catastrophe is too dreadful to contemplate.

More than 100 years after H.G. Wells wrote that statistical understanding will one day be as necessary for efficient citizenship as reading and writing, a shocking lack of statistical understanding continues to persist among citizens in India today. The ECI prescribing a patently wrong sample size of "one EVM per Assembly Constituency" for all Assembly Constituencies in all States and managing to get away with such a statistical howler for so long is a case in point.

It is important that the ECI must set the controversy at rest and implement the Supreme Court's order of 2013 properly both in letter and spirit. It should adopt the statistically correct sample sizes of EVMs for hand counting VVPAT slips, suggested in this paper, starting from the Assembly Elections for Mizoram, Chhattisgarh, Telangana, Rajasthan, and Madhya Pradesh due in November–December 2018. If the ECI persists with its statistically incorrect sample, an adverse inference is liable to be drawn against it and it may lose the perception battle in the minds of the political parties and voters.

Annexure I

State-wise Sample Sizes for 99% probability that the sample will detect at least one defective EVM

EVMs in the State as a whole are assumed as 'population'
Percentage of defective EVMs (P) is assumed as 1%.

Sl.No.	State	Number of Assembly Constituencies in the State	Population Size (N) = Total Number of Polling Stations (EVMs) in the State	Sample Size (n) for the State	*Average* Number@ of EVMs whose VVPAT slips are to be hand counted *per Assembly Constituency*
1	Sikkim	32	589	**315**	10
2	Mizoram	40	1164	**370**	10
3	Goa	40	1642	**409**	11
4	Nagaland	60	2194	**413**	7
5	Arunachal Pradesh	60	2562	**414**	7
6	Manipur	60	2794	**422**	8
7	Meghalaya	60	3082	**424**	8
8	Tripura	60	3174	**424**	8
9	Himachal Pradesh	68	7521	**446**	7
10	Jammu & Kashmir	87	10035	**450**	6
11	Uttarakhand	70	10854	**450**	7
12	Haryana	90	16357	**451**	6
13	Kerala	140	21498	**454**	4
14	Punjab	117	22615	**454**	4
15	Chhattisgarh	90	23672	**454**	6
16	Jharkhand	81	24803	**455**	6
17	Assam	126	24890	**455**	4
18	Telangana	119	32574	**455**	4
19	Odisha	147	35959	**455**	4
20	Andhra Pradesh	175	39970	**456**	3
21	Gujarat	182	50128	**457**	3
22	Rajasthan	200	51796	**457**	3
23	Karnataka	224	56696	**457**	3
24	Bihar	243	65337	**457**	2
25	Madhya Pradesh	230	65341	**457**	2
26	Tamil Nadu	234	65616	**457**	2
27	West Bengal	294	77247	**458**	2
28	Maharashtra	288	91329	**458**	2
29	Uttar Pradesh	403	150000	**458**	2
INDIA		4120	About 10,00,000	**459**	1

@ - Rounded off to the next higher integer.

Annexure II

State-wise Sample Sizes for 99.9% Probability that the sample will detect at least one defective EVM

EVMs in the State as a whole are assumed as 'population'
Percentage of defective EVMs (P) is assumed as 1%.

Sl. No.	State	Number of Assembly Constituencies in the State	Population Size (N) = Total Number of Polling Stations (EVMs) in the State	Sample Size (n) for the State	*Average* Number@ of EVMs *whose VVPAT slips are to be hand counted per Assembly Constituency*
1	Sikkim	32	589	**461**	15
2	Mizoram	40	1164	**508**	13
3	Goa	40	1642	**574**	15
4	Nagaland	60	2194	**589**	10
5	Arunachal Pradesh	60	2562	**595**	10
6	Manipur	60	2794	**608**	11
7	Meghalaya	60	3082	**613**	11
8	Tripura	60	3174	**614**	11
9	Himachal Pradesh	68	7521	**659**	10
10	Jammu & Kashmir	87	10035	**667**	8
11	Uttarakhand	70	10854	**669**	10
12	Haryana	90	16357	**672**	8
13	Kerala	140	21498	**677**	5
14	Punjab	117	22615	**678**	6
15	Chhattisgarh	90	23672	**679**	8
16	Jharkhand	81	24803	**678**	9
17	Assam	126	24890	**678**	6
18	Telangana	119	32574	**680**	6
19	Odisha	147	35959	**680**	5
20	Andhra Pradesh	175	39970	**681**	4
21	Gujarat	182	50128	**683**	4
22	Rajasthan	200	51796	**683**	4
23	Karnataka	224	56696	**684**	4
24	Bihar	243	65337	**685**	3
25	Madhya Pradesh	230	65341	**685**	3
26	Tamil Nadu	234	65616	**684**	3
27	West Bengal	294	77247	**685**	3
28	Maharashtra	288	91329	**685**	3
29	Uttar Pradesh	403	150000	**686**	2
INDIA		4120	About 10,00,000	**688**	1

@ - Rounded off to the next higher integer.

Endnotes

[1] In his presidential address to the American Statistical Association in 1950, Samuel S. Wilks said, "Perhaps H.G. Wells was right when he said 'Statistical thinking will one day be as necessary for efficient citizenship as the ability to read and write.'" The quote was then published in the Association's journal in 1951. This is the form in which it is popularly quoted. But H.G.Wells' original quote which appeared in his book *"Mankind in the Making"* (1903) was as follows: "The great body of physical science, a great deal of the essential fact of financial science, and endless social and political problems are only accessible and only thinkable to those who have had a sound training in mathematical analysis, and the time may not be very remote when it will be understood that for complete initiation as an efficient citizen of one of the new great complex world-wide States that are now developing, it is as necessary to be able to compute, to think in averages and maxima and minima, as it is now to be able to read and write."

[2] Shetty, K.A.V. 2018. *"Making Electronic Voting Machines Tamper-proof: Some Administrative and Technical Suggestions*", The Hindu Centre for Politics and Public Policy, Policy Watch No. 6, published on August 30, 2018 and updated on October 3, 2018. Please see Chapter VI *"The Vulnerability of Indian EVMs"*, Chapter VII *"Three Security Loopholes"* and Chapter VIII *"ECI's Administrative Safeguards are not Foolproof"*.

[3] In Statistics, the *population*, or *universe*, refers to the complete set of elements (persons or objects) that possess some common characteristic which is of interest to the researcher. e.g. all persons with HIV-AIDS in a city; all EVMs used in an election, etc. A *sample* is a subset of the population consisting of one or more elements drawn from the population. Based on the sample results, the researcher can make inferences or extrapolations from the sample to the population.

[4] Let us assume that 300 EVMs were used in an election. A sample of three EVMs is drawn randomly. As per the EVM electronic count, let the total votes polled in these three EVMs put together be 1,800 and the votes secured by the leading candidate be 600. If the hand count of VVPAT slips for these three EVMs also yields the same total of 1,800 votes and the same number of 600 votes for the leading candidate, then there is no possibility of any EVM malfunction or fraud. The results of the election (for 300 EVMs put together) can be declared based on their EVM electronic count.

[5] A 'defective EVM' is defined as one which has a mismatch between the 'EVM count' and the 'VVPAT count'. The mismatch may be due to EVM malfunction or EVM tampering or VVPAT-unit malfunction or mistakes in the hand counting of VVPAT slips. In the event of a mismatch, *at least one recounting* of the VVPAT slips of the particular EVM may have to be done to rule out mistakes in hand counting. The VVPAT total as per the recount should tally either with the EVM count or the previous VVPAT count. If it doesn't tally with either, further recounts should be done until the last VVPAT count matches either with the EVM count or one of the previous VVPAT counts.

[6] Should the discrepancy of even a single vote or single digit votes between the EVM count and VVPAT count (even after following the recount procedure stated in Endnote 5 above) lead to the designation of the EVM as 'defective'? Ideally, *yes*. Or, should the ECI ignore minor discrepancies of *not more than, say, five votes* in order to avoid the huge administrative workload of hand counting VVPAT slips of all the remaining EVMs of the population? Whether to ignore such minor discrepancies or not in cases where there will be no change in election outcomes is a *policy decision* to be made by the ECI in consultation with various political parties and other stakeholders.

[7] Chapter 5 titled *"Perfunctory Implementation of VVPAT"* of Policy Watch no. 6 *"Making Electronic Voting Machines Tamper-proof: Some Administrative and Technical Suggestions*" written by the author was one of the first papers in India to deal with the issue of sampling plan of EVMs for VVPAT-based audit. In that paper, sample sizes were calculated using ready reckoners based on the Normal Distribution model. The Normal Distribution model is a reasonably 'good fit' to the EVM problem but the Hypergeometric Distribution model (which is used in the present paper) is even better for the following three reasons:

(i) It is an 'exact fit' to the EVM problem;
(ii) It yields a more economic (i.e. smaller) sample size; and
(iii) In the Normal Distribution model – for a given confidence level and a given margin of error – the sample size is maximum when the 'Proportion of defectives' (P) in the population is assumed to be 0.5 and decreases significantly as the value of P decreases and approaches zero. But in the Hypergeometric Distribution, the exact reverse is the case i.e., the sample size is maximum when P is close to zero and decreases significantly as P increases. So, irrespective of what the true value of P is, if we calculate the sample size for P very close to zero such as P = 0.01 (which is what the ECI thinks it is), then this holds good for all the other scenarios where P is higher. We do not need to make any questionable assumptions about the value of P as in the Normal Distribution model nor do we need to extrapolate trends based on questionable past empirical data.

[8] Pinker, S. 1997. *"How the Mind Works",* W.W.Norton & Co.

[9] When a sample is drawn *without replacement from a finite population*, the probability of occurrence of the various outcomes is given by the *Hypergeometric Probability Distribution* model.

Note: A 'probability distribution' is a mathematical function that gives the probability of occurrence of different possible outcomes in an experiment. The simplest case is the 'uniform distribution' in which all outcomes have an equal probability of occurrence. Apart from Hypergeometric Distribution, Binomial Distribution, Poisson Distribution, and Normal Distribution are some of the most commonly used probability distribution models.

[10] Schlaifer, R. (1959) *"Probability and Statistics for Business Decisions – An Introduction to Managerial Economics under Uncertainty"*, McGraw-Hill Book Company, Inc.

[11] Supreme Court of India, 2018. Writ Petition (civil) no. 935 of 2018 in *Kamal Nath vs Election Commission of India*. Oct. 12.

[12] In Hypergeometric Distribution, the probability of finding 'x' successes in a sample of size 'n' drawn from a population of size 'N' with 'M' successes is given by the formula:

$$\text{Prob}\ (x, n, M, N) \quad = \quad \frac{{}_{M}C_{x} \ . \ {}_{(N-M)}C_{(n-x)}}{{}_{N}C_{n}}$$

[13] The online Casio calculator available at https://keisan.casio.com/exec/system/1180573201 is very useful for calculating probabilities under Hypergeometric Distribution. Enter the known values of population size (N) and 'successes' in the population (M), where M = N*P where P is the 'proportion of the characteristic of interest'. Try out different values of sample size (n) in the calculator such that the probability that x = 0 (of not finding any 'success' in the sample) is *less than the specified level*, say, less than 0.01 or 0.001; or, which is the same thing, the probability of finding at least one 'success' in the sample is greater than 0.99 or 0.999.

[14] In the online Casio calculator referred to above, enter N = 100, M = 5, n = 3, x = 0 (not finding even a single 'success'). The probability of 'x = 0' is 0.856. Or, the probability of getting at least one 'success' is [1 – 0.856] = 0.144 i.e. 14.4%.

[15] In the same calculator, enter N = 100, M = 5, x = 0 (not finding even a single 'success'). Enter increasing values of 'n' till the probability of 'x = 0' becomes less than 0.01. It is seen that the probability of 'x = 0' is 0.011 for n = 58, and is 0.0099 for n = 59. So, with a sample size of 59, the probability of not getting a single 'success' is less than 1%. Or, the probability of getting at least one 'success' is 99%.

[16] The superiority of the Hypergeometric Distribution model to the Normal Distribution model has already been discussed in Endnote 7. The Binomial Distribution is applicable to *infinite populations* or where the samples are taken *with replacement*. In Binomial Distribution, the sample size (n) is *independent* of the population size (N) and depends on the proportion of the characteristic of interest (P) and the confidence level (C). The formula for sample size is:

n = ln (1 – C) / ln (1 – P) where 'ln' stands for natural logarithm.

For C = 0.99 and P = 0.01, n = ln (1-0.99) / ln (1-0.01) = ln (0.01) / ln (0.99) = 458.21, rounded off to 459 (the next highest integer).

Only the Hypergeometric Distribution gives the correct, economic sample sizes *for finite populations*. In the example discussed in pages 2-4 (please see Table 1), with Hypergeometric Distribution, n = 448 when N = 10,000; n = 457 when N = 50,000; n = 458 when N = 1,00,000 and n= 459 when N = 5,00,000. So, as the population size (N) increases, the sample size (n) as per the Hypergeometric Distribution model approaches the value given by the Binomial Distribution model (459). The Binomial Distribution model is a reasonably 'good fit' when the population size is very large but is not suitable for smaller, finite populations.

[17] **Moroney, M.J. 1951**. *"Facts from Figures"*, Penguin, London.

[18] In the online Casio calculator in end note 11, enter N = 300, M = 3, n = 1 and x = 0. The probability of x = 0 (i.e. of not finding a single 'success') is 0.99. That is, the ECI-prescribed sample size will miss a defective EVM 99% of the time. Repeat the calculations for N = 200, N = 100 and N = 50 to get the figures for the last column of Table 4.

[19] **Taleb, N, N. 2007**. "The Black Swan: The Impact of the Highly Improbable", *Random House*.

About the Author

K. Ashok Vardhan Shetty is a former Vice-Chancellor of the Indian Maritime University, Chennai, a Central University under the Ministry of Shipping. Before assuming charge as the Vice-Chancellor, Shetty was a member of the Indian Administrative Service (IAS), Tamil Nadu Cadre, of the 1983 batch. He held a number of key assignments including Registrar, University of Madras, Director of Collegiate Education; District Collector, Viluppuram; Director of Rural Development; Managing Director, Tamil Nadu State Marketing Corporation, (TASMAC); Secretary, Chief Minister's Secretariat; Principal Secretary, Rural Development and Panchayat Raj Department; Principal Secretary, Municipal Administration and Water Supply, among others. Successful project implementation was his forte. He was commended by the Government of Tamil Nadu several times.

Shetty has published several articles on public administration, management, E-Government, popular science, and popular mathematics in leading English and Tamil newspapers such as The Hindu, The Hindu - Tamil, The Hindustan Times, Indian Express, The Hindu BusinessLine, and (the now defunct magazine) Science Today. His earlier contribution to The Hindu Centre for Politics and Public Policy can be accessed at "Making Electronic Voting Machines Tamper-proof: Some Administrative and Technical Suggestions".

He can be contacted at shetty25@hotmail.com

Prashant Bhushan
(TRUE COPY)

THE HINDU CENTRE
for
Politics and Public Policy

ANNEXURE: R10

A Hitchhiker's Guide to Electronic Voting Machines and VVPATs

18.04.2019, Antar Bandyopadhyay, Krishanu Maulik and Rahul Roy, *The Wire*

In Douglas Adams's irreverent sci-fi classic *The Hitchhiker's Guide to the Galaxy*, the supercomputer Deep Thought, after spending seven-and-a-half million years on it, derives the 'Answer to the Ultimate Question of Life, the Universe and Everything'. It is the number 42.

Deep Thought also clarifies that the answer is meaningless because the people who programmed the computer didn't actually know what the question was.

Closer to home, a few judges of our Supreme Court and many renowned lawyers sought to understand the meaning of the number '479', obtained ostensibly from an Indian Statistical Institute report to the Election Commission of India. The three learned authors of this report spent seven-and-a-half months to come up with this number, which indicates the number of EVMs that should be randomly checked with VVPAT.

On a careful reading of the report, we now understand the question to which the answer is 479.

It is the answer to a question of statistical quality-control. Indeed, this would have been the same answer to the question of how many pencils need to be checked to ensure that in a pencil factory, the weekly production of 15 lakh pencils doesn't have more than 2% defects – or in other words, whether the EVMs when they were produced had manufacturing defects or not.

Before we move to other aspects of this report, we first point out a fundamental flaw in the assumptions on which this report is based. The report considers all the EVMs of India to be a single population, among which defects have to be searched. India does not have a presidential system of elections. Instead, we choose representatives in each constituency to send to Parliament.

In such a model, a voter from a particular constituency has to be satisfied that their representative has legitimately won the elections and the result is not because of machine tampering. Thus, the random checks have to be done among the machines at constituency-level, which constitutes the relevant population.

Once this fact is noted, then following the 'hypergeometric model' of the report, and assuming 1,500 EVM-VVPATs in each constituency with 2% having defects, one comes to a figure of approximately 350 per constituency as the number of EVMs whose VVPATs have to be tallied. This gives an overall number for the country of around 2 lakh of randomly selected EVMs whose VVPATs have to be cross-checked.

However, this number of 350 per constituency, which is arrived at from the hypergeometric model used in the report, is flawed.

Indeed suppose that there are 15 lakh voters in each of two distinct constituencies 'A' and 'B'. Also assume that in constituency A the winning margin is 1.5 lakh votes, while in constituency B the winning margin is 15,000 votes, and this is not an unrealistic scenario, as a perusal of past election data will suggest. It is not rocket science to realise that even a small error may change the outcome in constituency B, while it will need a larger error to change the outcome in constituency A.

For constituency B, tampering of 7,500 votes is enough to change the outcome, while for constituency A there has to be tampering of 75,000 votes. In percentages terms, an error in the count of 0.5% of the electorate of constituency B is enough to change the outcome, whereas in constituency A the percentage required is 5%.

Thus the number of samples to be checked for constituency B has to be much larger than that for constituency A. Indeed the sample size has to depend on the size of the winning margin. A 'one size fits all' cannot be a solution as is done in the said report where a uniform 2% error is used.

A quick calculation, assuming there are 1,500 EVMs in the constituencies (each EVM on an average handles 1000 votes), it will be enough to check 150 VVPATs for the constituency 'A', while to

obtain a precision given in the report, it will be required to check about 950 VVPATs for the constituency 'B'.

The report also proceeds to give a sequential scheme of checking in case of mismatch between the VVPAT and the EVM counts. If there is only one mismatch in the 479 randomly selected EVMs, the report suggests that an extra 128 EVMs be randomly selected and their VVPATs checked for mismatches. If there are two mismatches in the original 479 and the additional 128, then another extra 110 are to be selected and their VVPATs tallied to check for mismatches, etc.

Again, clearly, if there is a mismatch in an EVM used in a particular constituency, in the random choice of the EVMs for the additional checks, the chosen machines may come from completely different constituencies. This hardly makes any sense.

There is one more fallacy of checking a fixed number (1 or 5) of EVM-VVPATs for each assembly segment of a parliamentary constituency. For example, each parliamentary constituency in UP has five assembly segments and hence, assuming five VVPATs are to be verified per assembly segment, we need to check 25 machines.

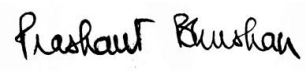
On the other hand, Mizoram has one parliamentary constituency with 40 assembly segments, leading to checking of 200 of them. Given the objection of the ECI about the difficult terrain, checking 200 machines in Mizoram should have been a bigger concern than checking only five in UP. An even more interesting conundrum arises in the five parliamentary seats in the union territories without any assembly.

Recall what professor P.C. Mahalanobis said to the 125th meeting of the American Statistical Association, about the difficulty of applying "Statistics as a Key Technology" to the official systems in India. The Father of Indian Statistics lamented: "The very idea of having crosschecks is frightening as conflicting results arising from independent checks would be 'confusing' and must be resisted and is being resisted even today."

How correct and contextual Mahalanobis sounds, even 54 years later.

Antar Bandyopadhyay, Krishanu Maulik and Rahul Roy work at the Theoretical Statistics and Mathematics Division of the Indian Statistical Institute. The views expressed here are personal.

SOURCE:
https://thewire.in/government/a-hitchhikers-guide-to-electronic-voting-machines-and-vvpats



(TRUE COPY)

HEADNOTES:

1. **The principle of the public nature of elections emerging from Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law (Grundgesetz – GG) requires that all essential steps in the elections are subject to public examinability unless other constitutional interests justify an exception.**
2. **When electronic voting machines are deployed, it must be possible for the citizen to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge.**

Judgment of the Second Senate of 3 March 2009
on the basis of the oral hearing of 28 October 2008
– 2 BvC 3/07, 2 BvC 4/07 –

in the proceedings regarding the complaints requesting the scrutiny of an election

I. of Dr. W...

- authorised representative: 1. Prof. Dr. ...,
2. lawyers ...

– against the resolution of the German Bundestag of 14 December 2006 – WP 145/05 – (Bundestag document (Bundestagsdrucksache – BTDrucks) 16/3600) – 2 BvC 3/07 –,

II. of Prof. Dr. W...

- authorised representative: Prof. Dr. ...

– against the resolution of the German Bundestag of 14 December 2006 – WP 108/05 – (Bundestag document 16/3600) – 2 BvC 4/07 –.

RULING:

1. The Ordinance on the Deployment of Voting Machines in Elections to the German Bundestag and of the Members of the European Parliament from the Federal Republic of Germany (Federal Voting Machine Ordinance (Bundeswahlgeräteverordnung – BWahlGV)) of 3 September 1975 (Federal Law Gazette (Bundesgesetzblatt – BGBl) I p. 2459) in the version of the Ordinance Amending the Federal Voting Machine Ordinance and the European Election Code (Verordnung zur Änderung der Bundeswahlgeräteverordnung und der Europawahlordnung) of 20 April 1999 (Federal Law Gazette I p. 749) is not compatible with Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law insofar as it does not ensure monitoring that complies with the constitutional principle of the public nature of elections.
2. The use of the electronic voting machines of N.V. Nederlandsche Apparatenfabriek (Nedap) of type ESD1, hardware versions 01.02, 01.03 and 01.04, as well as of type ESD2, hardware version 01.01, in the elections to the 16th German Bundestag was not compatible with Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law.
3. The complaints requesting the scrutiny of an election are rejected in other respects.
4. The Federal Republic of Germany is ordered to reimburse to the complainant re 1. the full amount of the necessary expenses from these proceedings and to reimburse to the complainant re 2. three-quarters of his necessary expenses

GROUNDS:

A.

The complaints requesting the scrutiny of an election relate to the permissibility of the deployment of computer-controlled voting machines, which are also referred to as electronic voting machines or "election computers", in the elections to the 16th German *Bundestag*. 2

I.

1. Roughly two million persons eligible to vote in Brandenburg, Hesse, North Rhine-Westphalia, Rhineland-Palatinate and Saxony-Anhalt cast their votes in the elections to the 16th German *Bundestag* via computer-controlled voting machines which are manufactured by the Dutch company Nedap and have been sold in Germany since 1999 as a central component of the "Integral Election System" (IWS) of H. GmbH. The type designations of these voting machines are composed of a name for the device generation (ESD1 or ESD2), as well as in each case of a version number for the hardware (HW) and for the software (SW). The types ESD1 (HW 1.02; SW 2.02), ESD1 (HW 1.02; SW 2.07), ESD1 (HW 1.03; SW 3.08), ESD1 (HW 1.04; SW 3.08) and ESD2 (HW 1.01; SW 3.08) have so far been used in elections to the German *Bundestag*. 3

These voting machines are controlled via a microprocessor and a software program. The votes cast are exclusively stored on an electronic storage medium and are counted electronically by the voting machine at the end of the election day. After the electronic ascertainment of the results, the voting machine shows the total votes cast for the respective electoral proposals; the results can be printed out via a printer that is integrated into the voting machine. The software program which controls the registration of the ballot and the ascertainment of the results is to be found on two electronic storage modules (so-called EPROMs; EPROM = Erasable Programmable Read-Only-Memory) which are installed in the device under a screwed-on cover and are secured by two seals applied by the manufacturer. The votes cast at the voting machine – including the linkages (first vote and connected second vote) – are stored on a removable cassette-like storage medium – the so-called vote storage module, also referred to as "electronic ballot box" (see Schönau, *Elektronische Demokratie*, 2007, p. 53). The data of the voting slips, the attribution of the individual keys to the electoral proposals, as well as the date of the election and the polling station, are also stored on the vote storage module. 4

The voting machines have a keypad ("the voter *tableau*") over which an insertion sheet is placed portraying a voting slip imitating the official voting slip. Above the key field one finds a display (LCD display) which guides the voter through the election procedure and enables him or her to examine her or her entries. The keypad and the LCD display are flanked by two vision-shielding panels on either side. On the reverse of the voting machine are the abovementioned printer and a slot for the vote storage 5

module. The voting machines are linked with a control unit on the returning committee's table. The control unit shows the returning committee the casting of the votes by the respective voter such that the display of the number of voters increases by one. After the voter has cast his or her votes, the voting machine is blocked for further balloting until the returning committee releases it for the next voter.

An element of the "Integral Election System" sold by H. is a programming and reading out device which enables the local authority to prepare the vote storage modules in conjunction with a personal computer prior to the elections and to read out the ballot information from the storage module after the election and to make it available for further data processing. The storage modules can be read out once more after the election day with the aid of a voting machine. The software of the "Integral Election System" also makes it possible to print the stored votes at a computer as voting slips with the corresponding crosses. 6

An individual identification number of the individual voting machine, as well as the version numbers of the hardware and the software, and two checksums which are constituted by a checksum algorithm contained in the voting machine software, can be shown and printed on the voting machine. These data can be compared with the information on the nameplate of the voting machine and in the declaration of identity. 7

2. An attempt was already made in Germany in the nineteen-sixties to replace the manual counting of the voting slips linked to the traditional election event using more rational methods and by deploying voting machines. According to § 35.3 of the Federal Electoral Act (*Bundeswahlgesetz – BWG*) of 7 May 1956 (Federal Law Gazette I p. 383 – Federal Electoral Act), the Federal Minister of the Interior was able to permit officially authorised vote counting devices to be used instead of voting slips. The Ordinance on the Use of Vote Counting Devices in Elections to the German *Bundestag* (*Verordnung über die Verwendung von Stimmenzählgeräten bei Wahlen zum Deutschen Bundestag*) of 24 August 1961 (Federal Law Gazette I p. 1618) was handed down on this basis. § 35.3 of the Federal Electoral Act was rescinded by means of the Act Amending the Federal Electoral Act (*Gesetz zur Änderung des Bundeswahlgesetzes*) of 24 June 1975 (Federal Law Gazette I p. 1593), and replaced by a more detailed provision on "balloting with voting machines", which since the promulgation of the new version of the Federal Electoral Act of 1 September 1975 (Federal Law Gazette I p. 2325) can be found in § 35 of the Federal Electoral Act. The Ordinance on the Deployment of Voting Machines in Elections to the German Bundestag (Federal Voting Machine Ordinance) (*Bundeswahlgeräteverordnung – BWahlGV*) of 3 September 1975 (Federal Law Gazette I p. 2459) provided in § 1 that mechanically or electrically driven voting machines may be used in elections to the German *Bundestag* if their type is authorised and their use was approved. 8

On the basis of the Ordinance on the Use of Vote Counting Devices of 24 August 1961 (Federal Law Gazette I p. 1618) and of the Federal Voting Machine Ordinance of 3 September 1975 (Federal Law Gazette I p. 2459), voting machines were initially 9

authorised and used in Germany which worked on the basis of (electro)mechanical counting devices (see Schreiber, *Handbuch des Wahlrechts zum Deutschen Bundestag*, 7th ed. 2002, *§ 35*, marginal no. 5). These voting machines worked mechanically; a count was mechanically increased by activating a button or by placing an election token in an opening allotted to the respective electoral proposal. They did not catch on since the cost of procuring, transporting, storing and maintaining the devices was compared to a relatively minor gain in time, and the devices could frequently only be deployed in elections with a small number of electoral proposals (see *Bundestag* document 8/94, p. 2).

These disadvantages were to be avoided by the deployment of electronic voting machines. In 1997, Nedap applied to the Federal Ministry of the Interior for a type approval for an electronic voting machine which it manufactured. The Federal Voting Machine Ordinance of 3 September 1975 (Federal Law Gazette I p. 2459), at that time most recently amended by Ordinance of 15 November 1989 (Federal Law Gazette I p. 1981) was not amenable to examine and approve such a device type. After the *Physikalisch-Technische Bundesanstalt*, referring to this circumstance in an examination report of 8 September 1998, had made a positive evaluation of the Nedap voting machine in technical terms and a test of the voting machine in Cologne had been assessed as satisfactory, the Federal Ministry of the Interior decided to make it possible to deploy computer-controlled voting machines in the European elections in June 1999. For this reason, amendments were also prepared to § 35 of the Federal Electoral Act and the Federal Voting Machine Ordinance for the deployment of computer-controlled voting machines in future *Bundestag* elections. 10

§ 35.1 of the Federal Electoral Act in the version promulgated on 23 July 1993 (Federal Law Gazette I p. 1288, 1594), most recently amended by Act of 1 July 1998 (Federal Law Gazette I p. 1698, 3431), applicable at that time was worded as follows: 11

Voting machines with separate counting devices may be used in place of voting slips, election envelopes and ballot boxes to make the casting and counting of the votes easier. 12

The words "with separate counting devices" were deleted with the Act on General and Representative Election Statistics in Elections to the German Bundestag and in the Election of Members of the European Parliament from the Federal Republic of Germany (*Gesetz über die allgemeine und die repräsentative Wahlstatistik bei der Wahl zum Deutschen Bundestag und bei der Wahl der Abgeordneten des Europäischen Parlaments aus der Bundesrepublik Deutschland*) of 21 May 1999 (Federal Law Gazette I p. 1023). The amendment to § 35 of the Federal Electoral Act was regarded as being necessary in order to be able to adjust the Federal Voting Machine Ordinance to technical developments in voting machines (see *Bundestag* document 14/401, p. 5). 13

The Ordinance Amending the Federal Voting Machine Ordinance and the European Election Code of 20 April 1999 (Federal Law Gazette I p. 749) already entered into 14

force on 24 April 1999 and amended a large number of provisions of the Federal Voting Machine Ordinance in order to create the preconditions for the deployment of computer-controlled voting machines. The words "including computer-controlled" were added in § 1 of the Federal Voting Machine Ordinance after the words "electrically driven". Further amendments were effected where the Federal Voting Machine Ordinance had previously used the term "counting devices". § 2.6 of the Federal Voting Machine Ordinance was added, obliging the manufacturer to enclose a declaration of identity.

3. § 35 of the Federal Electoral Act applied to the elections to the 16th German *Bundestag*, in the version of the Federal Electoral Act promulgated on 23 July 1993 (Federal Law Gazette I p. 1288, corrected p. 1594), most recently amended by the Eighth Competence Adjustment Ordinance (*Achte Zuständigkeitsanpassungsverordnung*) of 25 November 2003 (Federal Law Gazette I p. 2304). 15

The provision read as follows: 16

§ 35 17
Voting with voting machines

(1) Voting machines may be used in place of voting slips and ballot boxes to make it easier to cast and count the votes. 18

(2) Voting machines within the meaning of subsection 1 must guarantee that the ballot remains secret. Their type must be authorised for use in elections to the German *Bundestag* officially for individual elections or generally. The Federal Ministry of the Interior shall decide on authorisation on request by the manufacturer of the voting machine. The use of an officially authorised voting machine shall require approval by the Federal Ministry of the Interior. Approval may be issued for individual elections or in general terms. 19

(3) The Federal Ministry of the Interior is herewith empowered to hand down by means of a legal ordinance which shall not require the consent of the *Bundesrat* more detailed provisions regarding 20

1. the preconditions for the official approval of the type of voting machine, as well as for the withdrawal and revocation of approval, 21

2. the procedure for the official approval of the type, 22

3. the procedure for the examination of a voting machine for construction corresponding to the officially approved type, 23

4. the public testing of a voting machine prior to its use, 24

5. the procedure for the official authorisation of the use, as well as for the withdrawal and revocation of the authorisation, 25

6. the particularities related to the elections caused by the use of voting machines. 26

The legal ordinance shall be handed down in agreement with the Federal Ministry of Economics and Labour in cases falling under nos. 1 and 3. 27

(4) § 33.1 sentence 1 and§ 33.2 shall apply *mutatis mutandis* to the operation of a voting machine. 28

The provisions of the Federal Voting Machine Ordinance of 3 September 1975 (Federal Law Gazette I p. 2459), which were most recently amended by ordinance of 20 April 1999 (Federal Law Gazette I p. 749), relevant to the proceedings at hand, relate to the approval of voting machines and their deployment in elections. The voting machines require a type approval and a use authorisation (see § 1 of the Federal Voting Machine Ordinance). According to § 2.2 sentence 1 of the Federal Voting Machine Ordinance, the type approval may be granted if the voting machine corresponds to the Guidelines for the Construction of Voting Machines (*Richtlinien für die Bauart von Wahlgeräten*) according to Annex 1 to the Federal Voting Machine Ordinance. These guidelines regulate in particular the technical requirements to be made on the voting machines, and contain detailed stipulations for the identification, technical structure and functioning of the voting machines. Statements are made in this context on the portrayal of the electoral proposals, on operation and operability, on the ballot, on the storage of votes and on the creation of backups. The examination of the compliance of the voting machine with the above guidelines is a matter for the *Physikalisch-Technische Bundesanstalt*. 29

The use of approved-type voting machines requires authorisation prior to each election (§ 4.1 sentence 1 of the Federal Voting Machine Ordinance). Only those voting machines may be used which, once the election date has been set, have been examined by the manufacturer or the local authority using the operating manuals and maintenance regulations and with regard to which it has been ascertained that they are functional (§ 7.1 sentence 1 of the Federal Voting Machine Ordinance). In the constituencies in which voting machines are used, the local authority is to familiarise the head of the returning committee and his or her deputies with the voting machines prior to the elections and to familiarise them with their operation (§ 7.3 of the Federal Voting Machine Ordinance). Prior to the commencement of the election act, the local authority assigns the devices to the head of the returning committee with the necessary operating manuals and the declaration of the manufacturer according to § 2.6 of the Federal Voting Machine Ordinance that the device is constructed identically to the tested, approved type sample (see § 8 of the Federal Voting Machine Ordinance). Prior to the commencement of the ballot, the returning committee must ascertain amongst other things that the counting and storage devices are set to zero or have been erased (§ 10.1 no. 3 of the Federal Voting Machine Ordinance) and must close the voting machine needed (§ 10.2 of the Federal Voting Machine Ordinance). Prior to reading the displays of the votes counted by a voting machine, the number of the ballot records in the voter list is to be added to the number of election slips taken in and compared with the number of votes displayed (§ 13 of the Federal Voting Machine Ordinance). Deviations are to be noted and explained in the election record 30

(§ 13 sentence 3 of the Federal Voting Machine Ordinance). If the total of the counter results displayed does not tally with the number of the total votes cast as displayed, the returning committee must show the difference and note it in the election record (§ 14.5 of the Federal Voting Machine Ordinance). The head of the returning committee, the local authority and the district returning officer must ensure on completing the tasks of the returning committee and returning the voting machines that the voting machines used or the vote storage devices removed from them and the election record with the Annexes are not made available to unauthorised parties until the *Land* (state) returning officer has revoked the blocking and sealing of the voting machines and of the vote storage devices (see § 16.2 and § 17.3 of the Federal Voting Machine Ordinance).

4. The Federal Ministry of the Interior issued type approvals for the voting machines used in the elections to the 16th German *Bundestag*. On 15 August 2005, it announced the authorisation of the use of computer-controlled voting machines made by Nedap in the elections to the 16th German *Bundestag* with details on hardware versions, storage module types and software versions (Federal Gazette (*Bundesanzeiger*) no. 158 of 23 August 2005, pp. 12747-12748). Invoking company secrets of Nedap, the Ministry however refused to make available to the interested public documents which Nedap had provided to the *Physikalisch-Technische Bundesanstalt* for the examination of the samples, or test reports of the *Physikalisch-Technische Bundesanstalt*. 31

5. The decision as to whether voting machines are acquired, and in which constituencies they are used, is a matter for the towns and local authorities. As a reason for the acquisition and the deployment of voting machines, in addition to the more rapid calculation of the election result and to the anticipated cost savings, it is stated that it is virtually impossible to inadvertently cast invalid votes; cases of doubt as to the validity of individual votes because of ambiguous markings on the voting slip and unintended errors in counting the votes are said to be virtually ruled out (see Schreiber, *Handbuch des Wahlrechts zum Deutschen Bundestag*, 7th ed. 2002, *§ 35,* marginal no. 2). The recruitment of voluntary election assistants is also said to be made much easier because less time is needed to ascertain the election result (see Schönau, *Elektronische Demokratie*, 2007, p. 50). These advantages are said to be evident in particular in local elections, which in many *Länder* (states) were said to have been made more complex because of possibilities of cumulative voting and voting for candidates from different party lists. 32

II.

1. With their complaints requesting the scrutiny of an election, both complainants target the Federal Electoral Act and the Federal Voting Machine Ordinance insofar as they facilitate the deployment of computer-controlled voting machines. They complain of the authorisation of the use and deployment of the voting machines; furthermore, the type approvals which were issued for the Nedap voting machines used in the 33

Bundestag election are said to be unlawful. The complainant re 2. complains over and above this that the proceedings of the German *Bundestag* suffered from a number of faults.

a) aa) The complainant re 1. objected to the result of the elections to the 16th German *Bundestag* in 30 constituencies in Brandenburg, Hesse, North Rhine-Westphalia, Rhineland-Palatinate and Saxony-Anhalt referred to in greater detail. He moved to ascertain the constituencies in which computer-controlled voting machines had been used, and the number of the votes cast with these voting machines, and to repeat the elections in the constituencies concerned. The deployment of computer-controlled voting machines was said to have violated the principle of the public nature of elections and the principle of the official nature of elections. Over and above this, the voting machines were said not to be compatible with the Guidelines for the Construction of Voting Machines. 34

The principle of the public nature of elections was said to guarantee the proper implementation of the elections and the correct constitution of Parliament. The monitoring of the election act was said to have to encompass above all ensuring that the marking of the vote took place secretly and that the votes cast by the voters were inserted into the ballot box without a change, that the votes were not subsequently altered and that only the votes from the ballot box were counted at the end of the election. In the deployment of the voting machines complained of, effective monitoring by the public and by the returning committee were said to be prevented since a major part of the election act and the investigation and ascertainment of the election result were said to take place inside the voting machine. 35

If voting machines were deployed, it was said to only replace the public nature of elections possible in an election with voting slips if equivalent and publicly verifiable control mechanisms existed, such as a paper record of the votes cast printed by the voting machine which the voter could inspect. Corresponding control possibilities were however said not to be available to the public in deployment of the Nedap voting machines. 36

It was said not to be possible for the public to check the trustworthiness of the software installed in the voting machines. The examination by the *Physikalisch-Technische Bundesanstalt* and the type approval were said not to have taken place publicly; also, the voting machines were said not to be made available to the interested public for independent examination. The source code software of the voting machines was said not to be open. Ultimately, it was said also not to be possible to examine whether the copies of the software used in the polling stations were identical to the sample examined by the *Physikalisch-Technische Bundesanstalt* and whether they were free of manipulations. It was said to be possible to effect authentication by a chain of characters ("hash value") being calculated for each original program and the copy and then compared, so that agreement between the two values was said to document the authenticity of the software. This was however said not to be reliably 37

guaranteed in the voting machines which were the subject of the complaint since the checksums displayed and printed when the device was launched were calculated by the software installed in the voting machine itself, so that it was alleged not to be ruled out that the calculation of the checksums provided the expected chain of characters because of a prior deliberate manipulation of the software.

The particular danger in computer-controlled voting machines was said to lie in the fact that elections could be much more effectively influenced via manipulation of the software by the device manufacturer than in ballot box elections. For instance, it was said to be possible for faulty software to allot a certain share of the votes cast to a certain party regardless of the election decision by the respective voter or for the total votes cast to be divided among the parties standing for election according to a set proportion. Manipulations were said to be possible both by politically or financially motivated "insiders", in particular employees of the manufacturer, and by external third parties who gained access to the computers used by the manufacturer (for instance via viruses or trojans); they were said with regard to the complexity of the software used not always to be discovered even in careful quality control effected by the manufacturer. Although it was said to be necessary to prevent unauthorised access to the devices between the elections through suitable security measures, no such monitoring was said to take place in Germany; there were also said to be no suitable regulations in force that were able to guarantee protected storage of the voting machines. 38

It was said that the proceedings for the examination of the type sample by the *Physikalisch-Technische Bundesanstalt* and the approval of the type by the Federal Ministry of the Interior should be public as a part of the preparations for the elections. Any interests of the manufacturer in protecting its business secrets should be subordinate to the principle of democracy. For a lack of a possibility to check the device independently, the publication of the control documents and reports of the *Physikalisch-Technische Bundesanstalt* and of the source code of the voting machine software was said to be the only possibility in order to be able to judge the integrity of the elections. The non-publication of the control reports and documents and of the source code was hence said to constitute an electoral error. 39

It was said not to be compatible with the "principle of the official nature of the elections" that the functionality of the voting machines could only be examined by the manufacturer (§ 7.1 of the Federal Voting Machine Ordinance), and that there was no official control of freedom from manipulation of the voting machines. Over and above the declaration of identity, there was said to be no authentication of the software implemented on the individual voting machines, so that the election bodies had to rely on effective quality assurance by the manufacturer and on there being no manipulation after the examination had been carried out by the manufacturer. The tests carried out by the district returning officer in the context of preparation for the election and by the returning committee in the polling station were said not to be suited to recognise any manipulations. 40

The voting machines were said not to be compatible with the "Guidelines for the Construction of Voting Machines" (Annex 1 to § 2 of the Federal Voting Machine Ordinance). They neither complied with the general state-of-the-art, nor were they constructed in compliance with the rules of technology for systems with grievous consequences in case of misconduct (letter B no. 2.1subsection 1 of the Guidelines for the Construction of Voting Machines). In contravention of to letter B no. 1 item 2 of the Guidelines for the Construction of Voting Machines, the software used was said not to be clearly identifiable. 41

It is also said to be objectionable that § 35 of the Federal Electoral Act only calls for the ballot to be held in secret, but not for adherence to the other electoral principles. The examinability of the election result provided for in Article 41 of the Basic Law was said to be undermined if as a result of the type it were no longer to be possible to establish whether the outcome of the election had been reached lawfully. 42

bb) The complainant re 2. also submitted an objection to the elections to the 16th German *Bundestag*. 43

He takes the view that the deployment of the computer-controlled voting machines in at least 1,921 polling districts and 39 constituencies in five *Länder* had violated the principle of democracy, the principle of the rule of law and the principles of the public and official nature of elections. The deployment of the voting machines was said to violate the Federal Electoral Act and the Federal Voting Machine Ordinance from multiple points of view. Neither § 35 of the Federal Electoral Act, nor the Federal Voting Machine Ordinance, were said to comply with the constitutional principles of the law on elections of the public and official nature of elections. 44

The complainant re 2. moved *inter alia* for a finding that the election results in the constituencies designated by the complainant re 1., in the constituencies that were manifest from a "Customer overview [of Nedap] on the 2005 *Bundestag* election" provided by the Federal Statistical Office and in all other constituencies in which voting machines of the impugned nature might have been deployed, had come about unlawfully and were hence allegedly invalid. It was said that the elections needed to be repeated in these constituencies. Furthermore, the complainant re 2. applied for the publication of the examination documents of the *Physikalisch-Technische Bundesanstalt* regarding the voting machines to which the complaint referred, as well as for the holding of an oral hearing as soon as possible and the summons of specific witnesses and experts. 45

The more detailed statements of the complainant re 2. correspond to the objection submitted by the complainant re 1. 46

cc) The Federal Ministry of the Interior moved to reject the objections. 47

The public nature of the ballot was said to have been guaranteed in the deployment of the voting machines. The public was said to be able to check that only entitled voters were granted access to the voting booth. The returning committee was able to 48

check by reading the control unit that each voter had in fact voted and had only done so once. Moreover, it was said that the principle of the public nature of elections was not guaranteed without restriction. It was said to be in conflict with the goal of forming a viable people's representation in a short time. The Federal Electoral Act was said to attach greater significance to the goal of elections being held in good time and to ascertaining the outcome of the election within a reasonable time than to detailed monitoring by the public.

The public nature of the vote counting was said to have been guaranteed. The public was said to be able to check how the result of the constituency ascertained by the voting machine on conclusion of the election act was printed by the returning committee and included in the election record. The returning committee and each election observer were said to be able to compare the ballot records in the voter register and the valid and invalid first and second votes registered by the voting machine, and hence to ascertain whether the device had covered and added all the votes cast. It was said to be not possible to physically cover the individual votes; a totalling procedure which was verifiable for the public was however said not to be necessary since protection against falsification of the election result was said to be ensured by a number of other measures guaranteeing the reliability of the result as with ballot box elections. For instance, the voting machine was examined thoroughly prior to being approved by the *Physikalisch-Technische Bundesanstalt*. Comprehensive monitoring by local authorities and returning committees also took place in the run-up to the elections. The local ascertainment of the results was said to guarantee that manipulations on the part of individuals could at most impact the outcome of the election in the respective constituency. 49

Public monitoring was said to be only one factor among many in order to prevent irregularities in the elections, albeit an important one. No measure was said to be able to prevent manipulations or unintentional falsification of the election result by itself. All measures together were however said to guarantee very broad protection of the elections against election falsifications. 50

Since the principle of the public nature of elections had not been violated, it was said not to be necessary to bring forward the public nature of elections by publishing the control results of the *Physikalisch-Technische Bundesanstalt* and the source code for the voting machine software. The fundamentally public nature of the preparations for the election and of the election itself could be restricted for reasons of the protection of private data or of operational and business secrets. The type approval, the examinations of the voting machines by the *Physikalisch-Technische Bundesanstalt*, as well as the conclusive examination by the local authorities, were said to replace monitoring by the public in this respect. 51

The paper record called for by the complainants for subsequent checking of the storage of the votes was said to be by no means non-contentious in expert circles because of its disadvantages. It was said that such a record could be manipulated just 52

like any paper product. Further, it was impossible for a paper record to eliminate a lack of trust in the viability of the voting machine since it was created by the voting machine.

Since the preparation and implementation of the elections were said to be public tasks, it was said to be irrelevant whether this was actually expressed in a "principle of the official nature of the elections". It was only required that the state bodies provided the facilities and resources and took responsibility for organising the elections. It was said to be unobjectionable that private individuals effected individual actions; in this respect, the state bodies only had to carry out the monitoring required. For instance, the official voting slips were printed by private printers and the election notifications and postal voting documents were sent via private postal companies. It was said to always have been sufficient that the election authority classed the enterprises commissioned as trustworthy in each case. The same was said to apply to the manufacture and supply of voting machines with a declaration of identity of the manufacturer. 53

The voting machines were said to be compatible with the Guidelines for the Construction of Voting Machines. The voting machine software was said to be identifiable at any time by virtue of a comparison of the version number and the checksums with the information contained in the declaration of identity. Also the authenticity of the software was said to be guaranteed by a combination of protective measures. 54

Certainly, any electoral errors were said not to be relevant to mandates. Not concrete information had been put forward indicating that different election results had been achieved in specific polling stations because of the deployment of voting machines than would have been the case with a ballot box election. 55

dd) The German *Bundestag* rejected the election objections by resolution of 14 December 2006. The resolution recommendation of the Committee for the Scrutiny of Elections of 30 November 2006 (*Bundestag* document 16/3600, Annexes 1 and 2) considered the objections of both complainants to be manifestly unfounded. 56

The constitutionality of individual provisions of electoral law was said not to be amenable to a review by the German *Bundestag* since the German *Bundestag* and the Committee for the Scrutiny of Elections were not called on to find provisions of electoral law unconstitutional. 57

The deployment of the voting machines was said to have violated neither the concrete form given to the principle of the public nature of elections in non-constitutional law (§§ 10 and 31 of the Federal Electoral Act; § 54 of the Federal Electoral Code (*Bundeswahlordnung – BWO*), nor a principle of the public nature of elections going beyond this. The principle of the public nature of elections was said certainly not to entail each individual act being subject to an individual check. The public nature of the ballot was also said to be heavily restricted in postal voting. The election was said to be operated in the voting machines which were the subject of the complaint in princi- 58

ple in the same manner as in the ballot box election. Although marking of the voting slip and the ballot were carried out on one single device in the voting booth, the act of balloting was said to be transparent for the returning committee and the public since only the voter who had submitted his or her election notification card was able to vote using the voting machine.

In legal reality, when it came to the deployment of voting machines the concrete election act of voting was said to be in a conflict of interests between the principle of secret elections and that of the public nature of elections. It was said to be acceptable against this background that in the deployment of computer-controlled voting machines each sub-act of vote registration was not transparent to all. It was said to be one of the particularities of the advance in technology that one could presume that the systems deployed were viable if they had been examined in a special procedure prior to their deployment. This was said to be all the more valid given that the necessary monitoring took place in all other procedural steps, and hence the results that were obtained could be examined to determine their plausibility. The only decisive aspect was said to be whether the public had the fundamental possibility to become convinced of the viability of the election procedure. This was said to be accounted for by voting with voting machines: In particular, the public was able to check the printout of the result of the constituency ascertained by the voting machine and the transfer of the result into the election record, and hence the counting as a whole. By means of the comparison of the ballot records in the register of voters with the valid and invalid first and second votes registered by the device, as prescribed by § 14 of the Federal Voting Machine Ordinance, it was said also to be possible to check whether the voting machine had recorded all the votes and added them correctly. All the stored votes could be printed out as voting slips with the corresponding crosses and subsequently counted by hand. 59

The proceedings for type approval were said not to give rise to an election error. There was also said not to be a right to inspect the source code of the voting machine software with regard to the principle of the public nature of elections since the protection of the operational secrets of the manufacturer of the voting machines was said to outweigh the interest of the public in revealing the source code. 60

According to the convincing descriptions contained in the statement made by the Federal Ministry of the Interior, the voting machines which were the subject of the complaint were said to have complied with the provisions of the Federal Voting Machine Ordinance and with the Guidelines for the Construction of Voting Machines. According to the statements of the Federal Ministry of the Interior, manipulations were said to be theoretically possible, but hardly conceivable in practice. There were said to be no indications of deliberate manipulations or accidental alterations to the voting machines used in the *Bundestag* election forming the subject of the complaint. Even if none of the security measures mentioned were able by themselves to prevent manipulations, all the measures together were said to guarantee a very high degree of security against manipulation of the voting machines. 61

Where the complainant was complaining about a shift of state tasks towards private parties, this was said not to constitute an electoral error, even if the submission was assumed to be correct. In particular, the fact that the preparation and implementation of elections was a public task did not force the conclusion to be drawn that all necessary acts may only be carried out by officials. The necessary state control was said to be ensured. 62

Since no electoral error was therefore ascertainable, it was said not to be necessary to investigate any impact on the result of the ballot and on the distribution of seats in the German *Bundestag*. No oral hearing was set regarding the objection of the complainant re 2. according to § 6.1a no. 3 of the Law on the Scrutiny of Elections (*Wahlprüfungsgesetz – WahlPrüfG*), old version. 63

b) Both complainants have submitted a complaint requesting the scrutiny of an election to the Federal Constitutional Court (*Bundesverfassungsgericht*). 64

aa) The complainant re 1. moves to rescind the resolution of the German *Bundestag* of 14 December 2006 and to declare the elections to the 16th German *Bundestag* invalid in the constituencies referred to in the objection procedure insofar as computer-controlled voting machines were used there, and to order a repeat of the elections with voting slips and ballot boxes. Alternatively, he moves for a finding that the use of software-controlled voting machines in elections to the German *Bundestag* is not compatible with the Basic Law, furthermore as an alternative that the deployment of voting machines is not compatible with the Basic Law unless the transparency of the elections for the public, the examinability of the correctness of the election result and security against manipulation is guaranteed in a manner corresponding to elections with voting slips and ballot boxes. 65

The complainant re 1. repeats and expands his submission from the objection procedure, and submits the following as a supplement: 66

The deployment of the electronic voting machines, because of their technical and constructional security faults, was said to have violated the principles of electoral law set out in Article 38 of the Basic Law, the unwritten constitutional principles within electoral law of the public and official nature of elections, as well as the non-constitutional provisions of electoral law. 67

The public nature of the elections was also said to have been violated by virtue of the fact that the monitoring had been shifted to a non-public approval procedure and the publication of the examination results, examination documents, construction characteristics and of the source code of the devices had been refused. An evaluation of the votes cast that was verifiable by the public was said not to be possible because the individual votes could not be physically recorded. 68

The Federal Voting Machine Ordinance was said to contain serious faults insofar as it built on the principle of the declaration of identity; for there was said to be no monitoring as to whether the devices actually used corresponded to the software and 69

hardware checked by the *Physikalisch-Technische Bundesanstalt*.

It was said not to be compatible with the principle of official nature of the implementation of the election for the state election authorities to relinquish control over the entire course of events, including the technical details. Democracy and the rule of law were said rather to demand that the entire election events, ranging into the ramifications of the technical details, could be traced both by state bodies and by the people. The design of the election procedure, the monitoring and the parliamentary and judicial examinability of the election results, were said to be subject to the state's reserve as core state tasks. 70

The technical and constructional security faults in the voting machines were said to violate the principles of electoral law as to the freedom, equality and secrecy of the elections. If votes were diverted, electronically "caught" and "spied on", the freedom of the elections was said to be placed at risk. Equality was also said to be affected if it was not sure whether the vote that had been cast had been counted at all, and if so whether it was counted correctly. What is more, it was said that the secrecy of elections could suffer damage were manipulations to occur. It was said to be sufficient for a violation of the principles of electoral law that a situation had been created by the deployment of electronic voting machines in which the errors described were possible. 71

The restrictions of the principles of electoral law were said not to be justified by contrary constitutional provisions. Nedap's company secrecy interests that are protected by fundamental rights had to be subordinated to the interest of the public in information and to the public monitoring which was fundamental to democracy. The gain in democracy (rapidity of ascertaining the election results and increased level of security of the election procedure), linked with the deployment of computer-controlled voting machines, was also said to be unable to justify the impairment of public elections. 72

The election errors were said to be relevant to mandates. Major alterations were said to be possible in the mandate structure because of the major part of the votes affected by the election errors. The complainant re 1. was said not to bear the burden of proof for the elections having led to a different result without voting machines than had in fact been the case in the constituencies in which voting machines had been deployed. For the election errors which had been complained of, in particular the violation of the principle of the public nature of elections, were said to have eliminated the actual possibility to demonstrate a manipulation in concrete terms. 73

bb) The complainant re 2. is essentially moving to rescind the rejection of his objection by the German *Bundestag* and to repeat the elections in the constituencies designated in the written objection of 15 October 2005, as well as basically to establish the unconstitutionality of § 35 of the Federal Electoral Act and the Federal Voting Machine Ordinance. 74

The complainant re 2. challenges both the constitutionality of the legal basis for the 75

deployment of computer-controlled voting machines (§ 35 of the Federal Electoral Act and the Federal Voting Machine Ordinance), and the concrete deployment of the Nedap voting machines in the elections to the 16th German *Bundestag*. The electronic voting machines used were said to violate as to their construction and functioning the principles of electoral law of the public and official nature of elections and Article 38.1 sentence 1 of the Basic Law, as well as the Federal Voting Machine Ordinance. The procedures for the approval of the voting machines by the *Physikalisch-Technische Bundesanstalt* and the Federal Ministry of the Interior which were the subject of complaint were also said not to comply with the principles of democracy and the rule of law, as well as with the principles of electoral law of the public nature of elections and the sovereign implementation of elections.

As grounds, the complainant re 2. repeats the arguments that he already submitted in the objection procedure before the German *Bundestag*. He additionally alleges that the equality of elections had been violated by differing treatment of voting slip voters and voting machine voters since the principles of democracy and the rule of law, as well as of the public and official nature of the elections, were said to apply to the same degree to voting slip voters and to voting machine voters, and that the legislature had not provided legal provisions for the deployment of the electronic voting machines which were identical and equivalent to those in the Federal Electoral Code for voting slip elections. Insofar as it was not possible to rule out that because of the technical shortcomings of the voting machines there might be discrepancies between the ballot intended by voters and the ballot registered by the voting machine, the principle of equality between "successful" and "unsuccessful" voters was said to have been violated. 76

He also objects to the proceedings before the German *Bundestag*. The length of the proceedings was said not to be acceptable. The German *Bundestag* was said to have taken its decision on the basis of an insufficiently verified set of facts. The impugned resolution of the German *Bundestag* was said to have not come into being effectively for a lack of a quorum since 40 Members at most had attended the ballot. The deliberations of the Committee for the Scrutiny of Elections were said to have taken place in camera. The Rules of Procedure of the German Bundestag (*Geschäftsordnung des Deutschen Bundestages – GO-BT*) were said to be unconstitutional because they had not provided for the hearings, deliberations and rulings of the committee in the election scrutiny procedure to be held in public. Despite an explicit motion, no date had been set for an oral hearing. 77

2. The complaints requesting the scrutiny of an election were served on the German *Bundestag*, the *Bundesrat*, the Federal Government, all *Länder* Governments, the federal associations of the parties represented in the German *Bundestag* (CDU, SPD, The Greens, FDP, Linkspartei, CSU) and the federal returning officer. The *Physikalisch-Technische Bundesanstalt* and the Federal Office for Information Security were afforded the opportunity according to § 27a of the Federal Constitutional Court Act (*Bundesverfassungsgerichtsgesetz – BVerfGG*) to make a statement on 78

the technical questions that had been put forward.

a) The federal returning officer considers the deployment of the electronic voting machines to be lawful. 79

b) The Federal Ministry of the Interior has extended and supplemented its statements from the objection procedure before the German *Bundestag* on the use of the voting machines allegedly having been constitutional and lawful. 80

The public nature of elections was said to be overstretched if it were to be demanded that anyone should be able to verify the entire election events, including the preparations for the election, right down into the ramifications of the technical details and the entire state activity in an election, including the type approval of the voting machines, and that the other preparatory work of the election bodies and other institutions were subject to public monitoring. 81

The local organisation was said to be one of the most important means to prevent manipulations in the use of voting machines. Since the local authorities decided on their own responsibility on the acquisition of the voting machines and were said to be responsible for the proper storage of the voting machines, and for their examination prior to deployment, manipulation of the voting machines was said to require, in addition to the appropriate technical skills, a knowledge of the manner in which each individual local authority stored the voting machines and how the security measures could be overcome. The local organisation was said to also include the ascertainment of the results in the respective polling station. This meant that it was not possible to manipulate the voting machine during transportation. Impacts of any irregularities were hence restricted to the election result in the respective constituency. 82

c) The *Physikalisch-Technische Bundesanstalt* explained the examination concept on which the type sample check was based, and stated that the security requirements should be judged in the context of the implantation of the voting machines into the proven processes in traditional elections. The arguments of the complainant were said not to take this into account. 83

3. a) The Chaos Computer Club e.V. refers in its statement to an examination of the security and manipulability of Nedap election computers which was implemented in 2006 in cooperation with the Dutch initiative "We do not trust voting computers" ("*Wij vertrouwen stemcomputers niet*"). The software and the hardware of the Dutch ES3B type, which in the view of the study's authors differed only slightly from the ESD 1 and ESD 2 types used in Germany, was said to have been susceptible to manipulation with relatively little effort. The test indicates that the processes and programming methods analysed by reconstructing the source code of the voting machine were trivial and only constituted the state-of-the-art of the early nineteen-nineties. 84

The voting machines could be manipulated by the votes cast for an electoral proposal being altered prior to their storage, so that they would be stored on the vote storage module as votes cast for another party. This was said not to require any knowledge of 85

the list place of the party or of the candidate. A further manipulation variant was said to consist in already providing for a preset percentage final result for a specific electoral proposal prior to commencement of the elections without this coming to light in a test election. It was said to be possible in practice to exchange the software without encountering difficulties. The storage media could be removed from the voting machine, read out, deleted and re-programmed using widely available tools. A person with a modicum of technical knowledge could exchange a storage medium within less than five minutes after brief training; someone with experience could have effected a swap in about one minute. Manipulations to the hardware were also simple without this being identifiable by any testing procedure used or proposed by Nedap or by the *Physikalisch-Technische Bundesanstalt*.

All in all, the tests had shown that the Nedap voting machines did not meet the requirements of the Federal Voting Machine Ordinance. The dynamics of the development in the potential for attack and manipulation were said to constitute one of the main risk factors of computer-aided election procedures. In contradistinction to established procedures, it was possible at any time for attack methods to be developed which were as yet unknown and the consequences of which were not foreseeable which remained unrecognised and made it possible to falsify an election. None of the fundamental difficulties in the use of computer-controlled voting machines was said to be solvable by technical means with sufficient reliability since greater technical security measures would of necessity lead to more complex systems which could be examined by even fewer people. 86

b) The Federal Ministry of the Interior takes the view that the statement of the Chaos Computer Club showed all in all an over-evaluation of technical security requirements as to the voting machines. There was said to be no way to guarantee absolute security against falsification in elections. Ballot box election and postal voting was said to be theoretically susceptible to manipulation in a similar way to elections with voting machines. Any technical security measure could be circumvented with the corresponding effort. 87

The criticised manipulation possibilities still in existence despite a protected environment were said not to differ from the risks also existing in classical elections. The existing regulations were said to be adequate. 88

4. In the oral hearing, the Senate furthermore heard Dr. Jörn Müller-Quade, European Institute for Systems Security (*Europäisches Institut für Systemsicherheit*) in Karlsruhe, and Melanie Volkamer, Institute of IT-Security and Security Law (*Institut für IT-Sicherheit und Sicherheitsrecht*) of the University of Passau, as experts. Dr. Müller-Quade particularly made a statement on the question of whether and to what degree manipulation to the hardware or software could be discovered by subsequent examinations of the voting machines. Ms Volkamer explained how the concurrence of the software with the samples installed in the individual voting machines could be examined prior to the elections. 89

B.

Insofar as the complainant re 2. objects to the proceedings before the German *Bundestag*, his complaint requesting the scrutiny of an election is unsuccessful. 91

The complaints requesting the scrutiny of an election are well-founded insofar as they complain about the Federal Voting Machines Ordinance permitting the use of computer-controlled voting machines without ensuring effective monitoring of the election act and effective subsequent monitoring of the ascertainment of the result. In this respect, there is a violation of the principle of the public nature of elections under Article 38 of the Basic Law in conjunction with Article 20.1 and 20.2 of the Basic Law. The use of Nedap's computer-controlled voting machines was also not compatible with the principle of the public nature of elections. Both election errors however do not lead to the elections being declared invalid in the constituencies designated by the complainant. 92

It can remain open whether the constructive characteristics of the voting machines, and hence also the type approvals and the use authorisation, were compatible with the requirements contained in the Federal Voting Machine Ordinance, and in particular in the Guidelines for the Construction of Voting Machines, and with the principles of electoral law under Article 38.1 sentence 1 of the Basic Law. The same applies as to the complaints that the voting machines used had not been subject to adequate official monitoring, that the examination of the samples by the *Physikalisch-Technische Bundesanstalt* and that the type approval procedure had not taken place in public, as well as that the examination reports and documents of the *Physikalisch-Technische Bundesanstalt*, and the source code of the voting machine software, had not been made available to the public. 93

I.

The complaint requesting the scrutiny of an election of the complainant re 2. is unsuccessful insofar as the complainant complains of the length of the proceedings before the German *Bundestag* and that the Committee for the Scrutiny of Elections had not deliberated in public and wrongly had not set an oral hearing. The complaint that the German *Bundestag* had not been quorate on accepting the resolution recommendation of the Committee for the Scrutiny of Elections is also not well-founded. 94

In the context of the complaint proceedings, the Federal Constitutional Court reviews the impugned resolution of the German *Bundestag* in formal and substantive terms. Faults in the proceedings of the German *Bundestag*, as they are claimed by the complainant, can only be relevant to the complaint if they are material and deprive it of the basis for its decision (see Decisions of the Federal Constitutional Court (*Entscheidungen des Bundesverfassungsgerichts* – BVerfGE 89, 243 (249); 89, 291 (299)). No such procedural violations are recognisable here. 95

1. Even if the proceedings took more than one year between the submission of the objection to the election and the decision of the German *Bundestag*, this does not yet 96

constitute a grievous procedural error. The length of the proceedings by itself does not remove the basis for the decision (see Federal Constitutional Court (*Bundesverfassungsgericht* – BVerfG, judgment of the Second Senate of 3 July 2008 – 2 BvC 1/07, 7/07 –, *Neue Zeitschrift für Verwaltungsrecht – NVwZ* 2008, p. 991 (992)).

2. The fact that the Committee for the Scrutiny of Elections refrained from holding an oral hearing on the complainant's objection to the election, and also deliberated in camera in other respects, also does not constitute a grievous error removing the basis for the decision of the German *Bundestag*. 97

a) According to § 6.1a no. 3 of the Law on the Scrutiny of Elections in the version of 24 August 1965 (Federal Law Gazette I p. 977 (Law on the Scrutiny of Elections, *Wahlprüfungsgesetz – WahlPrG*, old version)), which applied at the time of the decision on the complainant's objection, the committee was able to refrain from holding an oral hearing if the preliminary review revealed that the objection was manifestly unfounded. Since the amendment of § 6.1 of the Law on the Scrutiny of Elections by the Act Amending the Law on the Scrutiny of Elections of 6 June 2008 (Federal Law Gazette I p. 994), a date for an oral hearing is only to be set if the preliminary examination reveals that this can be expected to further promote the proceedings. 98

An objection is manifestly unfounded if no aspect is recognisable at the time of the decision which may help it to succeed (see BVerfGE 89, 243 (250); 89, 291 (300)). The evaluation is not conditional on the unfoundedness of the appeal being evident; it may also be the result of a prior thorough examination (see BVerfGE 82, 316 (319-320) on the regulation of § 24 of the Federal Constitutional Court Act with identical content). 99

Even if there may be reasons according to the submission of the complaint suggesting that the objection was not manifestly unfounded, in particular with regard to compliance with the Guidelines for the Construction of Voting Machines, refraining from holding an oral hearing is certainly not so grievous that the decision of the German *Bundestag* would be deprived of its basis by these means. It based its decision primarily on the deployment of computer-controlled voting machines not violating the principle of the public nature of elections and the concrete non-constitutional provisions contained in electoral law. In this respect, the German *Bundestag* has addressed the complainants' arguments in detail and made a detailed statement on the questions raised. Where it deals with the question of the approval of the Nedap voting machines used in the *Bundestag* election, it takes as a basis the statement of the Federal Ministry of the Interior, according to which manipulations are theoretically possible but, because of the bundle of technical and organisational security measures, are ruled out to the same degree as in classical voting slip elections. 100

b) In contradistinction to the view taken by the complainant re 2., the Committee for the Scrutiny of Elections was not obliged to deliberate in an open hearing. 101

The Law on the Scrutiny of Elections regulates in the provisions on oral hearings 102

(§§ 6 et seq. of the Law on the Scrutiny of Elections) the preconditions under which the proceedings of the Committee for the Scrutiny of Elections are held in public. If an oral hearing is not waived, the hearing takes place in public. According to § 10.1 of the Law on the Scrutiny of Elections, the Committee for the Scrutiny of Elections deliberates in secret on the result of the oral hearing. According to the system of the Act, this applies in the same way if an oral hearing is waived. No constitutional aspects are evident which might oblige the legislature to enact any different regulation when legislating on the scrutiny of elections (Article 41.3 of the Basic Law).

3. The complaint of the complainant re 2. that the resolution of the German *Bundestag* of 14 December 2006 had allegedly not effectively come into being for a lack of a quorum is also unsuccessful. The German *Bundestag* decides with a simple majority on the recommendation for a resolution of the Committee for the Scrutiny of Elections (§ 13.1 sentence 1 of the Law on the Scrutiny of Elections). According to § 45.1 of the Rules of Procedure of the German Bundestag, the *Bundestag* is quorate if more than half of its members are present in the plenary. The *Bundestag* is regarded as being quorate regardless of the number of its members present until it is found to not be quorate in the proceedings prescribed in § 45.2 of the Rules of Procedure of the German Bundestag. This provision does not come up against any constitutional reservations (see BVerfGE 44, 308 (314 et seq.) on the provisions of § 49.2 of the Rules of Procedure of the German Bundestag, old version, the content of which is largely identical). 103

As is shown by the record of the session, the German *Bundestag* unanimously accepted the resolution recommendation of the Committee for the Scrutiny of Elections on 14 December 2006 (see Minutes of plenary proceedings 16/73, Stenographic Record p. 7259 B). It cannot be derived from the minutes how many delegates were present in the house when the ballot was held. There is no record that it had been doubted, or indeed ascertained, whether the German *Bundestag* was quorate. There is hence no indication that the Bundestag was not quorate. 104

II.

1. In the context of a complaint requesting the scrutiny of an election according to § 13 no. 3 and § 48 of the Federal Constitutional Court Act, the Federal Constitutional Court has not only to guarantee compliance by the competent election bodies and the German *Bundestag* with the provisions of federal election law, but also to review whether the provisions of the Federal Electoral Act comply with the requirements of the constitution (see BVerfGE 16, 130 (135-136); BVerfG, judgment of the Second Senate of 3 July 2008 – 2 BvC 1/07, 7/07 –, *Neue Zeitschrift für Verwaltungsrecht* 2008, p. 991 (992)). This examination also covers the validity of legal ordinances. 105

2. The deployment of computer-controlled voting machines is in particular to be reviewed against the standard of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law). 106

The public nature of elections is a fundamental precondition for democratic political will-formation. It ensures the correctness and verifiability of the election events, and hence creates a major precondition for the well-founded trust of the citizen in the correct operation of the elections. The state form of parliamentary democracy, in which the rule of the people is mediated by elections, in other words is not directly exercised, demands that the act of transferring state responsibility to parliamentarians is subject to special public monitoring. The fundamentally required public nature of the election procedure covers the electoral proposal procedure, the election act (broken regarding the ballot by the secret nature of elections) and the ascertainment of the election result (see BVerfG, judgment of the Second Senate of 3 July 2008 – 2 BvC 1/07, 7/07 –, *Neue Zeitschrift für Verwaltungsrecht* 2008, p. 991 (992) with further references). 107

a) The basis for public elections is formed by the fundamental constitutional options for democracy, the republic and the rule of law (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law). 108

aa) In a representative democracy, the elections of the people's representation constitute the fundamental act of legitimisation. The ballot in the elections to the German *Bundestag* forms the major element of the process of will-forming from the people to the state bodies, and hence at the same time constitutes the basis for political integration. Compliance with the election principles applicable to this, and confidence in compliance with them, hence constitute preconditions for a viable democracy. Only by the possibility of monitoring whether the elections comply with the constitutional election principles is it possible to ensure that the delegation of state power to the people's representation, which forms the first and most important part of the uninterrupted legitimisation chain of the people to the bodies and office-holders entrusted with state tasks, does not suffer from a shortcoming. The democratic legitimacy of the elections demands that the election events be controllable so that manipulation can be ruled out or corrected and unjustified suspicion can be refuted. This is the only way to facilitate the well-founded trust of the sovereign in the correct formation of the representative body. The obligation incumbent on the legislature and on the executive to ensure that the election procedure is designed constitutionally and is implemented properly is not sufficient by itself to impart the necessary legitimacy. Only if the electorate can reliably convince itself of the lawfulness of the transfer act, if the elections are therefore implemented "before the eyes of the public" (see Schreiber, *Handbuch des Wahlrechts zum Deutschen Bundestag*, 7th ed. 2002, § 31 marginal no. 2) is it possible to guarantee the trust of the sovereign in Parliament being composed in a manner corresponding to the will of the voters that is necessary for the functioning of democracy and the democratic legitimacy of state decisions (see North Rhine/Westphalia Constitutional Court (*Verfassungsgerichtshof Nordrhein-Westfalen* – NRW VerfGH), judgment of 19 March 1991 – VerfGH 10/90 –, *Neue Zeitschrift für Verwaltungsrecht* 1991, p. 1175 (1179); Hanßmann, *Möglichkeiten und Grenzen von Internetwahlen*, 2004, p. 184). 109

bb) In a republic, elections are a matter for the entire people and a joint concern of all citizens. Consequently, the monitoring of the election procedure must also be a matter for and a task of the citizen. Each citizen must be able to comprehend and verify the central steps in the elections reliably and without any special prior technical knowledge. 110

cc) The public nature of the elections is also anchored in the principle of the rule of law. The public nature of the state's exercise of power, which is based on the rule of law, serves its transparency and controllability. It is contingent on the citizen being able to perceive acts of the state bodies. This also applies as to the activities of the election bodies. 111

b) The principle of the public nature of elections requires that all essential steps in the elections are subject to public examinability unless other constitutional interests justify an exception. Particular significance attaches here to the monitoring of the election act and to the ascertainment of the election result. 112

An election procedure in which the voter cannot reliably comprehend whether his or her vote is unfalsifiably recorded and included in the ascertainment of the election result, and how the total votes cast are assigned and counted, excludes central elements of the election procedure from public monitoring, and hence does not comply with the constitutional requirements. 113

c) Despite the considerable value attaching to the constitutional principle of the public nature of elections, it does not ensue from this principle that all acts in connection with the ascertainment of the election result must take place with the involvement of the public so that a well-founded trust in the correctness of the elections can be created. For instance, activities of the district returning officer with which according to § 76.1 of the Federal Electoral Code the – public – ascertainment of the election result is prepared by the district election committee are not constitutionally obliged to be subject to the principle of the direct public nature of elections (see BVerfG, judgment of the Second Senate of 3 July 2008 – 2 BvC 1/07, 7/07 –, *Neue Zeitschrift für Verwaltungsrecht* 2008, p. 991 (992)). 114

d) The requirements as to the examinability of the election events apply to the implementation of parliamentary elections regardless of the responsibility of the state bodies which have a constitutional structure (see BVerfGE 20, 56 (113); 41, 399 (414); Seifert, *Bundeswahlrecht*, 3rd ed. 1976, p. 130). 115

It is primarily a matter for the legislature to regulate how the retraceability of the essential steps in the election procedure is ensured. Article 38.3 of the Basic Law empowers and obliges the legislature to determine the details of the structure of electoral law (in particular the election system and the election procedure) and compliance with the principles of electoral law (see Magiera, in: Sachs, *GG*, 5th ed. 2009, *Art. 38*, marginal nos. 106 et seq. and 113 et seq.). The design of the technical aspects of the election events also falls within the regulatory mandate under Article 38.3 of the Basic 116

Law (see Morlok, in: Dreier, *GG*, Vol. 2, 2nd ed. 2006, *Art. 38*, marginal no. 127), and hence the decision on deployment of voting machines and the determination of the more detailed preconditions for their deployment. Details may be regulated by means of a legal ordinance on the basis of a statutory authorisation (see Magiera, in: Sachs, *GG*, 5th ed. 2009, *Art. 38*, marginal no. 114).

The legislature is entitled to broad latitude when lending concrete shape to the principles of electoral law within which it must decide whether and to what degree deviations from individual principles of electoral law are justified in the interest of the uniformity of the entire election system and to ensure the state policy goals which they pursue (see BVerfGE 3, 19 (24-25); 59, 119 (124); 95, 335 (349)). The Federal Constitutional Court only reviews whether the legislature has remained within the boundaries of the latitude granted to it by the Basic Law, or whether it has violated a valid constitutional election principle by overstepping these boundaries. It is not a matter for the Court to find whether the legislature has found solutions which are expedient or desired in terms of legal policy within the latitude to which it is entitled (see BVerfGE 59, 119 (125)). 117

3. The deployment of voting machines which record the voters' votes in electronic form and ascertain the result of the election electronically is hence only compatible with the Basic Law subject to strict preconditions. 118

a) When electronic voting machines are deployed, it must be possible to check the essential steps in the election act and in the ascertainment of the results reliably and without special expert knowledge. 119

The necessity of such monitoring emerges not lastly from the susceptibility to manipulation of electronic voting machines and their amenability to error. In these, the acceptance of the voters' votes and the calculation of the election result is based on a calculation act which cannot be examined from outside or by persons without special computer knowledge. Errors in the voting machine software are hence difficult to recognise. Over and above this, such errors can affect not only one individual election computer, but all the devices used. Whilst manipulations or election falsifications are virtually impossible in classical elections with voting slips under the conditions of the valid provisions, including the provisions on the public nature of elections – or at least are only possible with considerable effort and with a very high risk of discovery which has a preventive impact – a major impact may in principle be achieved with relatively little effort by encroachments on electronically controlled voting machines. Manipulations of individual voting machines can already influence not only individual voters' votes, but all votes cast with the aid of this device. The scope of the election errors which are caused by alterations and malfunctions of a single software program affecting multiple devices is even wider. The major scope of the effect of possible errors in the voting machines or targeted election falsifications requires special precautions to be taken in order to comply with the principle of the public nature of elections. 120

aa) The voter himself or herself must be able to verify – also without a more detailed 121

knowledge of computers – whether his or her vote as cast is recorded truthfully as a basis for counting or – if the votes are initially counted with technical support – at least as a basis for a subsequent re-count. It is not sufficient if he or she must rely on the functionality of the system without the possibility of personal inspection. It is hence inadequate if he or she is exclusively informed by an electronic display that his or her ballot has been registered. This does not facilitate sufficient monitoring by the voter. Equal viability must also apply to the election bodies and to interested citizens.

The consequence of this is that the votes may not be stored exclusively on an electronic storage medium after the ballot. The voter may not be required to trust solely in the technical integrity of the system after the electronic ballot. If the election result is ascertained by computer-controlled processing of the votes stored in an electronic storage medium, it is not sufficient if only the result of the calculation process as implemented in the voting machine can be taken note of using a summary paper printout or an electronic display. By these means, voters and election bodies can only examine whether the voting machine has processed as many votes as voters have been admitted to operate the voting machine in the elections. It is not easily recognisable in such cases whether there have been programming errors in the software or targeted election falsifications through manipulation of the software or of the voting machines. 122

bb) The legislature is not prevented from using electronic voting machines in the elections if the constitutionally required possibility of a reliable correctness check is ensured. In particular, voting machines are conceivable in which the votes are recorded elsewhere in addition to electronic storage. This is for instance possible with electronic voting machines which print out a visible paper report of the vote cast for the respective voter, in addition to electronic recording of the vote, which can be checked prior to the final ballot and is then collected to facilitate subsequent checking. Monitoring that is independent of the electronic vote record also remains possible when systems are deployed in which the voter marks a voting slip and the election decision is recorded simultaneously (for instance with a "digital election pen", see on this Schiedermair, *Juristenzeitung* 2007, p. 162 (170)), or subsequently (e.g. by a voting slip scanner; see on this Schönau, *Elektronische Demokratie*, 2007, pp. 51-52; Khorrami, *Bundestagswahlen per Internet*, 2006, p. 30) by electronic means in order to evaluate these by electronic means at the end of the election day. 123

It is certainly ensured in these cases that the voters are in charge of their ballot and that the result of the election can be reliably checked by the election authorities or by interested citizens without any special prior technical knowledge. Whether there are still other technical possibilities which create trust on the part of the electorate in the correctness of the proceedings in ascertaining the election result based on verifiability, and which hence comply with the principle of the public nature of elections, need not be decided here. 124

b) Restrictions on possibilities for citizens to monitor the election events cannot be 125

compensated for by sample devices in the context of the type approval procedure or in the selection of the voting machines specifically used in the elections prior to their deployment being subjected to verification by an official institution as to their compliance with certain security requirements and their proper technical performance. The monitoring of the essential steps in the election promotes well-founded trust in the correctness of the election certainly in the necessary manner that the citizen himself or herself can reliably verify the election event.

For this reason, a comprehensive bundle of other technical and organisational security measures (e.g. monitoring and safekeeping of the voting machines, comparability of the devices used with an officially checked sample at any time, criminal liability in respect of election falsifications and local organisation of the elections) is also not suited by itself to compensate for a lack of controllability of the essential steps in the election procedure by the citizen. 126

Accordingly, neither participation by the interested public in procedures of the examination or approval of voting machines, nor a publication of examination reports or construction characteristics (including the source code of the software with computer-controlled voting machines) makes a major contribution towards ensuring the constitutionally required level of controllability and verifiability of the election events. Technical examinations and official approval procedures, which in any case can only be expertly evaluated by interested specialists, relate to a stage in the proceedings which is far in advance of the ballot. The participation of the public in order to achieve the required reliable monitoring of the election events is hence likely to require other additional precautions. 127

c) The legislature can permit exceptions to the principle of the public nature of elections to a restricted degree in order to bring other constitutional interests to fruition, in particular the written principles of electoral law from Article 38.1 sentence 1 of the Basic Law. For instance, restrictions of public monitoring of the ballot with postal voting (§ 36 of the Federal Electoral Act) can be justified with the aim of achieving as comprehensive participation in the elections as possible, thereby complying with the principle of generality of elections (see BVerfGE 21, 200 (205); 59, 119 (125)). When deploying computer-controlled voting machines, however, no contrary constitutional principles are recognisable which are able to justify a broad restriction of the public nature of elections and hence the controllability of the election act and the ascertainment of the results. 128

aa) Where the deployment of computer-controlled voting machines aims to rule out inadvertent incorrect markings on voting slips, unwanted invalid ballots, unintentional counting errors or incorrect interpretations of the voters' intention when votes are counted (see Schreiber, *Handbuch des Wahlrechts zum Deutschen Bundestag*, 7th ed. 2002, *§ 35*, marginal no. 2) which repeatedly occur in classical elections with voting slips, this serves the interest of the implementation of the equality of elections under Article 38.1 sentence 1 of the Basic Law. What weight attaches to this purpose 129

can however be left open. It certainly does not justify by itself forgoing any type of verifiability of the election act. Unintentional counting errors or incorrect interpretations of the voters' intention can also be ruled out by voting machines if supplementary monitoring by the voter, the election bodies or the public is made possible in addition to electronic recording and counting of the votes. Corresponding monitoring is for instance possible with electronic voting machines which record the votes not only in electronic form in the voting machine, but at the same time in a form which is independent of this (see II. 3. a) bb above). Apart from this, user errors – such as pushing the "invalid" key presuming that this made it possible to correct an erroneous entry – cannot be ruled out in the voting machines approved for the elections to the 16th German *Bundestag*.

bb) The principle of the secrecy of elections certainly does not constitute a counter constitutional principle which can be used as a basis for a broad restriction of the controllability of the election act and of the ascertainment of the results. There is no "conflict of interest" between the principle of secret elections and the principle of the public nature of elections which might justify such restrictions (*Bundestag* document 16/3600, Annex 1, p. 20). 130

The principle of secret elections guarantees that the voter alone is aware of the content of his or her election decision, and obliges the legislature to take the necessary steps to protect the election secret (see H.H. Klein, in: Maunz/Dürig, *GG*, *Art. 38*, marginal no. 110 [March 2007]; Pieroth, *Juristische Schulung – JuS* 1991, p. 89 (91)). The secrecy of elections constitutes the most important institutional protection of the freedom of elections (see BVerfGE 99, 1 (13)). In historic terms, secret elections may have been a caesura in the public nature of the election procedure because they renounced the open ballot in order to protect the freedom of election (see Breidenbach/Blankenagel, *Rechtliche Probleme von Internetwahlen*, Berlin 2000, pp. 34-35). Under the regime of the Basic Law, which explicitly prescribes elections as secret in order to protect their freedom, however, the principle of the public nature of elections from the outset does not apply to the act of the ballot. If the public nature of the elections is not ruled out in order to enable the ballot to be cast unobserved, the election procedure is subject to the principle of the public nature of elections (see H.H. Klein, in: Maunz/Dürig, *GG*, *Art. 38*, marginal no. 113 [March 2007]; Seifert, *Bundeswahlrecht*, 3rd ed. 1976, *Art. 38*, marginal no. 35). Accordingly, the impact of the principle of secrecy of elections is not to restrict the principle of the public nature of elections for the ballot act. It also does not justify a restriction of public monitoring in the casting of the – previously secretly marked – vote carrier or in the ascertainment of the results. This already follows from the fact that it does not oppose additional precautions enabling the voter to monitor whether his or her vote is recorded in an unfalsified manner as a basis for a subsequent re-count. 131

cc) Finally, the goal of being able to form a viable people's representation in a short period does not constitute a restriction of the principle of the public nature of elections in the deployment of computer-controlled voting machines. The clarification of the 132

correct composition of the people's representation within a suitable period is one aspect which can be taken into account when shaping the election procedure and the election scrutiny procedure (see BVerfGE 85, 148 (159)). The matter of the assembly of a new *Bundestag* in good time (see Article 39.2 of the Basic Law) is however not endangered by sufficient precautions being taken to ensure public elections. There is no constitutional requirement for the election result to be available shortly after closing the polling stations. What is more, the past *Bundestag* elections have shown that the preliminary official final result of the elections can as a rule be submitted in a matter of hours, even without the deployment of voting machines. The interest in rapidly clarifying the composition of the German *Bundestag* is therefore not a constitutional interest that is suited to impose restrictions on the public nature of the election event.

4. The normative level on which the questions related to the deployment of voting machines are to be regulated is determined in line with the requirements of the parliamentary reservation and the requirements which are placed on the authorisation to issue legal ordinances (Article 80.1 sentence 2 of the Basic Law). 133

a) The parliamentary reservation rooted in the principle of the rule of law and in the principle of democracy requires that the major decisions are to be taken by the legislature in fundamental normative areas, especially in the area of the exercise of fundamental rights, insofar as this is amenable to state regulation (see BVerfGE 49, 89 (126-127); 61, 260 (275); 80, 124 (132); 101, 1 (34)). The obligation to legislate relates here not only to the question of whether a certain article must be regulated by law at all, but also to how far these individual regulations have to go (see BVerfGE 101, 1 (34)). 134

According to Article 80.1 sentence 2 of the Basic Law, the content, purpose and scope of the authorisation to issue legal ordinances must be laid down in the statute concerned. The legislature itself must decide which questions are to be regulated by the legal ordinance, within what limits and with what goal (see BVerfGE 2, 307 (334); 5, 71 (76-77); 23, 62 (72)). The wording of the authorisation need not be formulated as precisely as possible; it must constitutionally only be sufficiently determined (see BVerfGE 55, 207 (226); 58, 257 (277); 62, 203 (209-210). It is sufficient if the limits of the authorisation are determinable by interpretation using the interpretation principles that are generally recognised; the goals of the statute, the context together with other provisions and the genesis of the statute are significant here (see BVerfGE 8, 274 (307); 23, 62 (73); 55, 207 (226-227); 80, 1 (20-21)). In detail, the requirements as to the level of determinedness depend on the particularities of the respective object of regulation and on the intensity of the measure (see BVerfGE 58, 257 (277-278); 62, 203 (210); 76, 130 (143)). Whilst less stringent requirements are to be made with circumstances that are highly varied and subject to rapid change, more stringent requirements apply to the degree of determinedness of the authorisation with those regulations which are linked to more intensive encroachments on legal positions which are protected by fundamental rights (see BVerfGE 58, 257 (278); 62, 203 (210)). 135

b) Because of their particularities, regulations relating to the deployment of voting machines are reserved for parliamentary decision insofar as they relate to the major requirements for the deployment of such devices. This includes the decisions on the permissibility of the deployment of voting machines and the fundamental prerequisites for their deployment. These decisions cannot be left to the institution adopting the ordinance. 136

The more detailed preconditions for the approval of voting machines and the procedures to be complied with here, the details of the use of the voting machines in the elections and the guarantee of the principles of electoral law in the concrete deployment of voting machines, by contrast, do not require any detailed parliamentary regulation, but can be regulated by the institution adopting the ordinance. The respective requirements of the voting machines depend heavily on the nature of the respective voting machine, and hence do not already have to be legislated in detail at the level of the parliamentary statute. Thus, for instance, the requirements for the deployment of electronically operated voting machines differ from those for the deployment of exclusively mechanical voting machines. Because voting machines are subject to ongoing technical development, a rapid adjustment of the law is better guaranteed if the detailed regulations are transferred to the institution adopting the ordinance. 137

III.

According to these standards, the authorisation to hand down ordinances contained in § 35 of the Federal Electoral Act does not give rise to any profound constitutional objections. 138

1. The parliamentary legislature was not obliged over and above the regulation contained in § 35 of the Federal Electoral Act to regulate the deployment of computer-controlled voting machines since the major questions in connection with the deployment of computer-controlled voting machines are determined in § 35 of the Federal Electoral Act. Where § 35 of the Federal Electoral Act authorises the adoption of the Federal Voting Machine Ordinance, the content, purpose and scope of the authorisation that has been issued is adequately regulated (Article 80.1 sentence 2 of the Basic Law). 139

The parliamentary legislature made the fundamental decision in § 35.1 of the Federal Electoral Act for the deployment of voting machines. By restricting the deployment of the voting machines to facilitating the casting and counting of votes, the legislature clearly determined the goal of the authorisation to issue ordinances. It made it clear by deleting the words "with separate counting devices" in 1999 that § 35 of the Federal Electoral Act also covers the deployment of computer-controlled voting machines. 140

The fundamental prerequisites for the deployment of the voting machines are named in § 35.2 sentences 2 to 5 and 35.3 of the Federal Electoral Act, in particular the official type approval and the official authorisation of the use of the voting machines. Of the constitutionally guaranteed election principles, only the secrecy of the 141

ballot and the keeping of the secrecy of elections are explicitly spoken of in § 35.2 sentence 1 of the Federal Electoral Act. The other principles of electoral law are regulated in § 1.1 sentence 2 of the Federal Electoral Act. They therefore certainly also apply to the deployment of voting machines in the elections to the German *Bundestag*. Finally, the legislature provided in § 35.3 sentence 1 no. 6 of the Federal Electoral Act that the Federal Ministry of the Interior may regulate the particularities in connection with the elections brought about by the use of voting machines. This provision forms not only a sufficient normative basis in order to account for the constitutional particularities of the deployment of computer-controlled voting machines. It also makes it recognisable for citizens that an election with voting machines may entail modifications in comparison with the classical ballot box election. It is not constitutionally required that all details of the content of a legal ordinance can be derived from the respective basis for the authorisation. The latitude which can be granted to the institution adopting the ordinance in this respect is also to be measured accounting for the complexity of the material and the dynamics of development processes in voting machines. The parliamentary legislature is hence certainly not constitutionally obliged to make detailed regulations for the deployment of electronic voting machines.

2. § 35 of the Federal Electoral Act is compatible with the principle of the public nature of elections. 142

a) It is not constitutionally objectionable that § 35.1 of the Federal Electoral Act permits voting machines "in place of voting slips and ballot boxes". For § 35.1 of the Federal Electoral Act does not rule out with this wording the approval and use of voting machines with control devices which record the votes in addition to (electronic) recording in the voting machine in a manner controlled by the voter. According to the systematic status of § 35.1 of the Federal Electoral Act, the words "in place of voting slips and ballot boxes" refer to the classical election procedure set out in § 34 of the Federal Electoral Act in which exclusively official voting slips and ballot boxes are used. § 35.1 of the Federal Electoral Act, by contrast, does not rule out the adoption of provisions which provide for devices for a verifiability of the election result that is independent of the electronic recording and evaluation of votes. 143

b) It is unobjectionable for the principle of the public nature of elections contained in § 35 of the Federal Electoral Act to not be explicitly listed once more as a precondition for the authorisation and use of computer-controlled voting machines. These requirements emerge directly from the constitution, and hence are also binding on the institution adopting the ordinance in lending concrete form to § 35 of the Federal Electoral Act. Independently of this, it also emerges from other provisions of the Federal Electoral Act that the use of voting machines is only permissible if the principle of the public nature of elections is adhered to. § 31 of the Federal Electoral Act determines that the election act is public. § 35.3 sentence 1 no. 4 of the Federal Electoral Act permits regulations to be made on the open testing of a voting machine prior to its use. 144

IV.

The Federal Voting Device Ordinance is unconstitutional on grounds of a violation of the principle of the public nature of elections from Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law. It does not already encounter legal reservations because the expansion of the area of application of the Federal Voting Device Ordinance to cover computer-controlled voting machines effected by the Ordinance Amending the Federal Voting Device Ordinance of 20 April 1999 (Federal Law Gazette I p. 749) had exceeded the framework of the provision on authorisation of § 35 of the Federal Electoral Act. The Federal Voting Machine Ordinance does not however contain any provisions ensuring that only those voting machines are approved and used which comply with the constitutional preconditions of the principle of the public nature of elections. 145

1. Insofar as the Ordinance Amending the Federal Voting Machine Ordinance of 20 April 1999 (Federal Law Gazette I p. 749) with effect from 24 April 1999 regulates the preconditions for the deployment of computer-controlled voting machines, it remains within the authorisation contained in the version of § 35 of the Federal Electoral Act still applicable on 24 April 1999. The latter permitted the use of voting machines "with separate counting devices" (§ 35.1 of the Federal Electoral Act). The subsequent deletion of the words "with separate counting devices" was considered necessary "in order to adjust the Federal Voting Device Ordinance to technical developments in voting machines" (*Bundestag* document 14/401, p. 5). This exception from the legislative procedure to amend § 35.1 of the Federal Electoral Act cannot however exert a decisive influence on the interpretation of the provision in the version which it had prior to the amendment. The expansion of the area of application of the Federal Voting Machine Ordinance to cover computer-aided voting machines was compatible with the wording of this earlier version. The term "counting device" only requires that item numbers, flow volumes or other values are calculated and shown automatically (see Duden, *Das große Wörterbuch der deutschen Sprache*, 3rd ed. 1999). According to the wording, this therefore also covers electronic or software-controlled counting devices in computer-controlled voting machines. The characteristic "separate counting devices" is intended in the view of the institution adopting the ordinance to refer merely to the requirement of "independent counting of first and second votes"; such independent counting of first and second votes is also possible with computer-controlled voting machines using an electronic counting device. Even if the legislature was not yet able to consider deployment of microprocessor-controlled voting machines in the original version of § 35.1 of the Federal Electoral Act (see Breidenbach/Blankenagel, *Rechtliche Probleme von Internetwahlen*, Berlin 2000, p. 7), neither the wording nor the purpose of § 35 of the Federal Electoral Act in the version applicable on entry into force of the Ordinance Amending the Federal Voting Machine Ordinance on 24 April 1999 suggest that these voting machines were intended to be ruled out from the legislative authorisation of the institution adopting the ordinance. 146

2. The Federal Voting Machine Ordinance violates the principle of the public nature 147

of elections under Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law because in the use of computer-controlled voting machines it guarantees neither effective monitoring of the election act nor the reliable verifiability of the election result. This shortcoming cannot be remedied by means of an interpretation in conformity with the constitution.

a) The public nature of elections requires in the deployment of computer-controlled voting machines that the essential steps in the election act and the ascertainment of the results can be reviewed reliably and without special expert knowledge. Such provisions are not contained in the Federal Voting Machine Ordinance. 148

It particularly does not emerge from the Federal Voting Machine Ordinance that only voting machines may be deployed which enable the voter in casting his or her vote to ensure reliable monitoring of whether his or her vote is recorded in an unfalsified manner. The ordinance also does not make any concrete content and procedural requirements as to reliable subsequent monitoring of the ascertainment of the results. 149

The obligation to seal computer-controlled voting machines and the containers in which the vote storage media are located after ascertaining the election result (§ 15.3 of the Federal Voting Machine Ordinance), as well as to ensure that the vote storage media are not accessible to unauthorised parties (§ 16.2 of the Federal Voting Machine Ordinance), is not sufficient in this respect. Even if the vote storage media can be read out once again at any time after the election day with the aid of a voting machine, the object of such a re-count is only the electronically stored votes, with regard to which neither voters nor the returning committee can examine whether they were recorded without falsification. The citizen cannot examine the essential steps in the ascertainment of the results if the re-count again takes place inside a voting machine. 150

In addition, the counting of the ballot records entered in the list of voters and of the election slips which have been accepted, as well as the comparison with the numbers for the total first and second votes at the voting machine shown (see § 13 of the Federal Voting Machine Ordinance) only facilitates monitoring as to whether the voting machine has processed as many votes as voters have been admitted for the operation of the voting machine. This does not guarantee the public monitoring of the essential steps in the election act and the ascertainment of the results. 151

b) The Federal Voting Machine Ordinance cannot be interpreted in conformity with the constitution such that only voting machines may be deployed which comply with the principle of the public nature of elections. 152

An application of the Federal Voting Machine Ordinance in conformity with the constitution such that type approval and use authorisation may only be issued by the Federal Ministry of the Interior if effective monitoring of election acts and ascertainment of the results is guaranteed (see Schiedermair, *Juristenzeitung – JZ* 2007, p. 162 (170)) would overstep the boundaries of an interpretation in conformity with the constitution. In principle, the institution handing down the ordinance has various pos- 153

sibilities at its disposal to ensure that the central steps in ballot and vote counting can be checked. Since the Federal Voting Machine Ordinance in its current version does not make it possible to recognise what such monitoring should look like, there is no constitutionally required provision, and hence there are no adequate indications which an interpretation in conformity with the constitution could take as its starting point.

It must also be taken into consideration here that the Federal Ministry of the Interior, as the institution handing down the ordinance, as it has also clearly confirmed in its statements in the proceedings at hand, considers the possibilities for monitoring which are constitutionally necessary for effective monitoring of election acts and ascertainment of the results to be neither legally required nor expedient. 154

V.

The computer-controlled voting machines used in the elections to the 16th German *Bundestag* also did not meet the requirements made by the constitution as to the use of electronic voting machines. 155

The use of the Nedap electronic voting machines of Type ESD1 hardware versions 01.02, 01.03 and 01.04, as well as of Type ESD2 hardware version 01.01, violates the principle of the public nature of elections (Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law) because these voting machines did not facilitate effective monitoring of the election act or the reliable verifiability of the election result. 156

The votes were exclusively recorded on an electronic storage medium after the ballot. Neither the voter nor the returning committees, nor the citizens present in the polling station, were able to check whether the votes cast were recorded by the voting machines without falsification. Using the display on the control unit, the returning committees could only recognise whether the voting machines registered a ballot, but not whether the votes were recorded by the voting machines without changing the content in any way. The voting machines did not provide a possibility to record the votes independently of the electronic record on the vote storage module enabling the respective voter to check his or her ballot. 157

The essential steps in the ascertainment of the results by the voting machines also could not be verified by the public. Since the ascertainment of the results exclusively formed the object of a data processing procedure running inside the voting machines, it was possible for neither the election bodies nor the citizens participating in the ascertainment of the results to verify whether the valid votes cast were correctly allotted to the electoral proposals and the votes accounted for by the individual electoral proposals in total were correctly ascertained. It was not sufficient that the result of the computing process implemented in the voting machine could be taken note of using a summary paper printout or an electronic display. A public examination by means of which the citizen could have reliably verified the ascertainment of the election result himself or herself without prior special technical knowledge was hence ruled out. 158

VI.

159 It may remain open whether the further complaints are well-founded. The complainants complain amongst other things that the characteristics of the voting machines and of the software used do not meet the requirements of the Federal Voting Machine Ordinance, in particular the Guidelines for the Construction of Voting Machines (Annex 1 to § 2 of the Federal Voting Machine Ordinance). The voting machines used were also said not to have been subject to sufficient official monitoring and examination of the samples by the *Physikalisch-Technische Bundesanstalt*, and that the type approval procedure should have been designed differently. The complainants hence ultimately object to the deployment of the computer-controlled voting machines used in the elections to the 16th German *Bundestag*. Even if these complaints were well-founded, in addition to the finding of the violation of the principle of the public nature of elections from Article 38 in conjunction with Article 20.1 and 20.2 of the Basic Law, these election errors would not take on any particular weight.

VII.

160 The election errors that were ascertained do not lead to the complaints requesting the scrutiny of an election being permitted or to the repetition of the elections in the constituencies designated.

161 1. The election error emerging from the fact that the type approvals for Nedap computer-controlled voting machines were granted, that the use of these voting machines in the elections to the 16th German *Bundestag* was approved and that the voting machines were indeed deployed in the elections without an effective legal basis, has no relevance to mandates. Approval and use of voting machines despite inadequate design of the legal basis do not lead as such to an influence on the election result.

162 2. The election error emerging from the fact that computer-controlled voting machines were approved and deployed the characteristics of which were not compatible with the requirements of effective verifiability of the election events, even if its relevance to mandates were to be assumed, does not lead to a partial declaration of invalidity of the elections to the 16th German *Bundestag*.

163 a) In the cases in which an election error may have had an impact on the distribution of mandates in the *Bundestag*, the election scrutiny decision of the Federal Constitutional Court is subject to the principle of the least incisive encroachment. The decision may only go so far as is demanded by the election error that has been ascertained. In principle, the requirement of the protection of the status quo of an elected people's representation (see BVerfGE 89, 243 (253)), which finds its legal basis in the principle of democracy, must be weighed up with the impact of the election error that has been ascertained. Simple influences on the election carrying no weight whatever do not therefore lead to the invalidity of an election. The encroachment on the composition of an elected people's representation by a decision under the law that regulates the

scrutiny of elections must be justified in light of the interest in conserving the elected people's representation (see BVerfG, judgment of the Second Senate of 3 July 2008 – 2 BvC 1/07, 7/07 –, *Neue Zeitschrift für Verwaltungsrecht* 2008, p. 991 (997) with further references). Even where an election error that is relevant to mandates can be restricted to certain mandates, in other words where the whole election did not have to be declared invalid, a weighing up is to be undertaken which may come out in favour of the interest in protecting the status quo.

b) The interest in the protection of the status quo of the people's representation composed in trust in the constitutionality of the Federal Voting Machine Ordinance outweighs the election errors that have been ascertained. Given that there are no indications that voting machines worked incorrectly or might have been manipulated, and hence that the election result would have been different in the constituencies concerned without the deployment of the computer-controlled voting machines, its possible impact on the composition of the 16th German *Bundestag* can be regarded as marginal at most. Such uncertain impacts do not justify the partial declaration of the invalidity of the elections to the 16th German *Bundestag* applied for. It should also be taken into account here that the violation of the constitution that was ascertained did not take place with intent, but when the legal situation was still unclear. Under these circumstances, after the above there is no election error making the continuation of the elected people's representation appear untenable. 164

B.

With regard to the fact that the complainants rightly complain of the unconstitutionality of the use of computer-controlled voting machines, the necessary expenses which they have incurred are to be refunded to them according to §§ 18 and 19 of the Law on the Scrutiny of Elections in conjunction with § 34a.3 of the Federal Constitutional Court Act in this respect. Accordingly, the complainant re 1. is to be refunded the necessary expenses in full, and the complainant re 2., whose complaints are partly unfounded, is to be refunded three-quarters of the necessary expenditure. 166

Judges: Voßkuhle, Broß, Osterloh, Di Fabio, Mellinghoff, Lübbe-Wolff, Gerhardt, Landau

Bundesverfassungsgericht, Urteil des Zweiten Senats vom 3. März 2009 - 2 BvC 3/07

Zitiervorschlag BVerfG, Urteil des Zweiten Senats vom 3. März 2009 - 2 BvC 3/07 - Rn. (1 - 166), http://www.bverfg.de/e/cs20090303_2bvc000307en.html

ECLI ECLI:DE:BVerfG:2009:cs20090303.2bvc000307

Prashant Bhushan

(TRUE COPY)