ISAS Working Paper

No. 115 – 12 October 2010

469A Bukit Timah Road
#07-01, Tower Block, Singapore 259770
Tel: 6516 6179 / 6516 4239
Fax: 6776 7505 / 6314 5447
Email: isassec@nus.edu.sg
Website: www.isas.nus.edu.sg

The Threat of the Geeky *Goonda*: India's Electronic Voting Machines

Robin Jeffrey[1]

Executive Summary

The paper examines the controversy over the reliability of India's Electronic Voting Machines (EVMs). Since the national elections of 2009, there have been allegations that the 1.4 million small stand-alone EVMs can be – and according to some protagonists, have been – doctored or rigged to allow election results to be falsified. The paper outlines the charges and describes the formal procedures under which the EVMs have operated for more than 10 years. It concludes that there is no convincing evidence that the machines have been rigged in India. It points out that any comparison with the networked, centralised electronic voting systems of the United States (US) and Europe, which have fallen into disfavour, are inappropriate. However, it is clear that if technically skilled people were to have ready and widespread access to EVMs, they could introduce external components that would enable the machines to be manipulated. Such manipulation would require large numbers of trained and reasonably adept conspirators who would have to escape the notice of or suborn both election officials and agents of rival parties. This is an improbable scenario. The Election Commission of India (ECI) has not however, met the allegations as ably and openly as it might. The Commission should not only be constantly testing, monitoring and improving existing EVMs, but also researching and costing methods that could add a paper trail to the current paperless process that could be used to verify election results.

[1] Professor Robin Jeffrey is a Visiting Research Professor at the Institute of South Asian Studies, an autonomous research institute at the National University of Singapore. He can be reached at isasrbj@nus.edu.sg. The views reflected in this paper are those of the author and not of the institute.

Once upon a time, when the world was a simpler place, rigging an Indian election could be seen as an exercise in job creation for unskilled labour. An unscrupulous candidate or political party would mobilise muscular retainers – *goondas* – to take over polling stations, shoo away voters, intimidate election staff and get down to the serious work of marking ballots and stuffing ballot boxes. When the polls closed, beautifully sealed and signed ballot boxes would be returned to the constituency headquarters where their carefully prepared contents would be counted and contribute to the victory of their paymaster-candidate.

There were, of course, other ways to fix elections. Sheer intimidation of the poor and vulnerable was one. Marching landless labourers to the polling booth under armed escort and telling them how to vote was once a method favoured by some rural power-holders. Or you could reward voters individually with bribes and convince them that if they took the money and voted the wrong way, the paymaster would find out. Or you could use your *goondas* to ensure that only your supporters voted at particular polling stations. All these methods required muscle power and quite a lot of it.

From 1999, the ECI began to introduce the EVMs: small, simple computer units, which recorded votes without paper. The machines are self-contained, and one (or more) is allocated for every polling station where an election is being held. An average constituency for a national election has upwards of 1,500 polling stations, and in 2009 the Election Commission used about 1.4 million EVMs to conduct the national elections.

When the polls close, the EVMs in each constituency are brought to constituency headquarters, where they are stored until counting day. On counting day, the total on each machine is calculated by the push of a button on each machine in the presence of the candidates' scrutineers and election officials. The tally on each machine is noted down, the total is added up – all this is done physically with candidates' agents signing off on the totals on each machine – and the result declared.

India runs the biggest democratic system in the world, and the Election Commission and the EVMs have been matters of pride. There were 714 million eligible voters for the national elections in 2009, and an average state election – say, the one approaching in 2011 in Kerala – will have more voters than there are people in Australia. Indian elections, in spite of *goonda* deployment in the past, have been remarkably honest (although there have been a few disastrous exceptions).[2]

[2] Kashmir elections prior to 1977 and again in 1987 were among the exceptions.

Indeed, in the past 20 years, the election process has become – most observers agree – more efficient, fair and strictly administered. Veteran returning officers speak of three changes that have improved the working of the voting system. First, from the tenure of T. N. Seshan, Chief Election Commissioner from 1990-6, the Commission acquired greater authority to enforce its powers. It can prevent governments from transferring officials and order the deployment of police. Rules of conduct for elections have been strictly enforced, and candidates are disqualified if the rules are broken. One longtime polling station official writes:

> ‘There is a rule stating that no placards or hoardings or signs should be put within 100 metres of a polling station. In the 1980s this was common. The rule was often violated and sometimes, if the offending candidate had a lot of local support (meaning in Kerala, muscle, or, more often, vocal-cord power) presiding officers found it difficult to enforce the rule. No longer. Partymen themselves now take care that these rules are not violated.’[3]

In the 2009 elections, journalists lamented the absence of colour and noise that resulted from Election Commission bans on giant hoardings, painted walls and noisy processions.

Second, today close to 90 per cent of eligible voters have voter identification cards with photographs. These began to be issued in the 1990s. The ID cards eliminated disputes at polling stations. Election agents also have a voters’ list with photographs. A person attends the polling station where he or she is eligible to vote, shows the ID card to the satisfaction of the election official and the party agents and is permitted to vote. Previously, challenges about identity were ‘a presiding officer’s nightmare. Now that the ID cards are compulsory there is never any challenge.’[4] Voters must vote at the polling station where they are enrolled.

EVMs have been the third element in making the system more efficient. As well as eliminating the need for huge printing contracts, for tons of paper to be transported around a vast country and for millions of ballot papers to be secured and accounted for, the EVMs have made voting easier and reduced the capacity for errors. And while it is still possible to capture a polling booth and have faithful retainers push the right buttons over and over again to give the required result, an honest presiding officer can, on first apprehension of an assault, push a button that freezes the EVM thereby stopping polling at that station. Election officials would then order a repoll at a later date and ensure adequate security. ‘I am very enthusiastic about the EVM,’ the Kerala presiding officer wrote.

[3] A teacher in a college in Thiruvananthapuram writing to Robin Jeffrey about his experience as a presiding officer at a polling booth during the 2004 national elections.

[4] Ibid.

> ‘Earlier … the most important items were the ballot papers and the ballot boxes. The papers were a headache. They were stitched in bundles of 50 each. We would count each one, ballot paper by ballot paper, making sure that they were in the correct serial number and were not damaged or defective. We even had to check that the counterfoil and the ballot paper had identical numbers. There were often defects and these had to be recorded on two different sets of documents … If by mistake a polling officer issued two ballot papers to a voter and the voter slyly made off with both, our accounts wouldn’t be correct and the election agents would raise hell.’[5]

The EVM removed much of this capacity for human error.

> ‘All you need to do is learn to use the voting machine properly. It’s a marvel: sturdy, easy to use, most reliable and about as foolproof as a machine can be. … Only the most gadget-challenged of people will have problems operating it.’[6]

The problem thrust forward in the last 12 months lies, however, in the words ‘as a machine can be.’

Since the national general elections in May 2009 a few disappointed politicians and computer specialists have been arguing that the EVMs are deeply flawed and can be manipulated. The critics have not demonstrated that the machines have in fact been tampered with or have produced false results. But they have attempted to show how machines could be manipulated if geeky *goondas* could get access to them at particular stages and replace components or insert small pieces of hardware to make the machines respond to unseen outside commands.

In August 2010, one of the critics, Hari Prasad, managing direct of an electronics firm in Hyderabad, was arrested by the Mumbai police and transported to Mumbai on the charge of stealing an EVM in order to show how it could be rigged to give false results.[7] Opposition members of India’s parliament have called for ‘an all-party meeting where different technical opinions can be presented … so that this doubt and question mark … can be answered once and for all …’[8]

[5] Ibid.

[6] Ibid.

[7] *The Hindu* (22 August 2010), www.thehindu.com/todays-paper/article587079.ece?css=print, accessed on 24 August 2010. He got bail on 26 August 2010.

[8] Arun Jaitley (Bharatiya Janata Party), Leader of the Opposition in the Rajya Sabha (upper house), 25 August 2010, Rajya Sabha Debates, http://164.100.47.5/newdebate/220/25082010/fullday.pdf, accessed on 30 August 2010. *The Hindu* (26 August 2010), www.thehindu.com/news/national/article594388.ece?css=print, accessed on 26 August 2010.

Accusations after the May 2009 national elections asserted that EVMs had been rigged. ‘Many candidates of BJD [the winning party in the Orissa state elections],’ wrote Biswabhusan Harichandan in the *Organiser*, the English weekly of the Rashtriya Swayamsevak Sangh,

> ‘who had never dreamt of winning … won the election with unbelievable margins of 25,000 to 60,000 votes. Some have now admitted that it is due to the appropriate programming of EVM, they have won the election with such high margin [sic].’[9]

Harichandan drew on technical critiques of EVMs prepared by Hari Prasad and publicised by a one-time member of the national executive of the Bharatiya Janata Party (BJP), G. V. L. Narasimha Rao.[10] They generated further credibility when they linked up with European and the US opponents of electronic voting and with an assistant professor of electrical engineering and computer science at the University of Michigan (with a PhD from Princeton) and some Indian doctoral candidates in the same field.

The Election Commission of India (ECI), which has an enviable reputation for rectitude and efficiency, did not respond as well as it could to challenges to the EVMs. Members of the Election Commission made the unwise claim, for example, that they were ‘1000 [sic] per cent sure that no one can manipulate’ the EVMs.[11]

Computer engineers, on the other hand, are unanimous in opining that *if* geeky *goondas* can get their hands on such simple computer hardware as that contained in the EVMs, they can substitute or add parts that will allow properly equipped assailants to make the machine do what they wish. ‘Funnily enough,’ wrote a senior professor of computer science, ‘computer scientists are most suspicious of these technologies since we know how easy they are to hack (Trojan Horse code etc.).’[12] The trust placed in India’s EVMs has to be based on more than a belief that computers can be made immune to manipulation.

But no one has yet presented convincing evidence that any Indian election has been rigged as a result of manipulating EVMs. There have, to be sure, been allegations, including one by the Congress politician Ghulam Nabi Azad, currently Minister of Health and Family Welfare in the national government, that ‘EVMs were manipulated during the [Orissa state] poll which resulted

[9] *Organiser* (12 July 2009), p. 9.

[10] G. V. L. Narasimha Rao, *Democracy at Risk! Can We Trust Our Electronic Voting Machines?* (New Delhi: Citizens for Verifiability, Transparency and Accountability, 2010). For Narasimha Rao’s political affiliation, *Hindustan Times* (18 February 2009), quoted on ‘Friends of BJP,’ http://friendsofbjp.org/2009/02/18/lks-the-man-gvl-narasimha-rao/, accessed on 11 August 2010. He was not listed on the BJP website in August 2010.

[11] S. Y. Quaraishi in *The Hindu* (14 December 2009), http://beta.thehindu.com/news/national/article64660.ece?css=print, accessed on 14 December 2009.

[12] Email from professor of computer science at the University of British Columbia, Vancouver, 17 August 2010.

in defeat of many Congress candidates.'[13] Azad had been responsible for Congress organisation in Orissa, where it had fared badly.

The claims are that EVMs are vulnerable in two simple ways. First, an attacker 'could alter election results by replacing parts of the machines with malicious look-alike components.' The fake components could then be made, using wireless technology, to deliver the results required. 'Election results could be compromised by inserting a dishonest display into an EVM control unit at any point before votes are publically counted, perhaps years before the election.[14]

A second method of manipulating the machines once voting has taken place would involve a *goonda* attaching a small device to an EVM that would allow the totals recorded in the machine to be altered.[15] This requires 'the temporary application of new hardware.'

The critics of the EVM make valid points, which the Election Commission could treat as constructive. Some of the critiques, however, have a whiff of political losers looking for conspiracies to explain defeats or of technical specialists seeking notoriety for theoretical cleverness.

First, it is true that the current EVM system leaves no paper trail. If EVMs were corrupted or broken, there would be no way of back-tracking to discover the true intentions of voters. In the US, a majority of the 50 states requires a Voter Verified Paper Audit Trail (VVPAT).[16] This usually involves voters voting electronically and then receiving a print-out record of their vote which they deposit in a ballot box. If necessary, the paper records can be counted to confirm the electronically recorded result. The disadvantages – particularly apposite for India – of such a system are that they introduce an additional element of technology and paper: printers in working order would have to be at every polling booth. In India, it would be necessary to build printers as robust as the EVMs and ensure that the batteries that power the EVMs in many localities were powerful enough to drive printers too. Nevertheless, such a system would still eliminate the mountains of pre-election printing that were required to prepare ballots for elections in the days before EVMs. Such a system could be made to work, but it would involve heavy cost, careful development and rigorous testing.

[13] IANS, 18 June 2009, www.thaindian.com/newsportal/politics/voting-machines-manipulated-in-orissa-polls-claims-azad_100206516.html , accessed on 25 August 2010. Azad does not seem to have repeated the remark, made at a press conference in Bhubaneswar.

[14] Hari K. Prasad, J. Alex Halderman, Rop Gonggrijp, *et al.*, 'Security Analysis of India's Electronic Voting Machines,' p.10., 29 April 2010, http://IndiaEVM.org, accessed on 18 August 2010.

[15] Ibid., pp.1-2.

[16] http://.en.wikipedia.org/wiki/Voter_Verified_Paper_Audit_Trail, accessed on 26 August 2010.

The *second* potential flaw lies in the nature of the EVMs themselves: they are simple, self-contained and abundant – there are 1.4 million of them. It would be foolish to dispute the claim that if *goondas*, supported by moderately talented technicians, have access and time, they can insert illicit hardware that will allow an EVM to be manipulated. But the process sounds laborious and even more labour-intensive than booth capturing in the old days. 'To use the [clip-on] device,' to gain control of an EVM, write Hari Prasad and his associates,

> 'the attacker connects a jumper wire to the control unit CPU to hold it in reset. Next, he clips the device to one of the EEPROMs on the control unit board. … To steal votes, the attacker indicates his favored candidate using the rotary switch [installed by the attacker], shown in Figure 8. … When the switch is set …, the chip on the clip-on-device executes a vote-stealing program ...'[17]

Such interference on one EVM could result in manipulation of no more than the 2,000 votes that might be cast at a single polling station. Even to rig a single constituency in this fashion would take a lot of eager, moderately trained fingers and a great many sealed lips to prevent the conspiracy being revealed. Access to stored EVMs is no doubt possible. They are stored, in theory, under guard in a locked strong room at district election headquarters; but India has more than 600 districts and standards of maintenance and probity vary. Illegal access in some places would no doubt be possible. The fact that an EVM in Mumbai was stolen for a few days to allow Hari Prasad to work on it – the reason why he was arrested in August 2010 – illustrates vulnerability.

But would attackers seek to doctor every EVM in a Lok Sabha constituency – more than 1,500 machines? If at an early stage they had got inside a great many EVMs and inserted clip-on devices, they would still need to get access to the machines to twist 'the rotary switch' to indicate the chosen candidate's place on the list of candidates on the ballot. That listing is, of course, only determined once nominations close. Critics of the EVMs seem united that 'to hack an EVM and manipulate its functioning, one has to open the machine and alter the source code (program) in the EVM.'[18] Something physical has first to be done to each EVM to make it susceptible to manipulation. An 'honest' EVM, untampered with, cannot be manipulated simply by pointing a cleverly programmed wireless device at it.

A *third* vulnerability lies in the possibility of the chips, on which the simple software that operates the machines is burned, being replaced at the factory or while EVMs are in storage by illicit chips (easily designed and manufactured, critics says).[19] The illicit chips could be

[17] Ibid., p.14.

[18] Ibid., p.98.

[19] Narasimha Rao, *Democracy*, pp.26, 148.

controlled from outside. On counting day *goonda* geeks in key tally rooms would manipulate the results using wireless technology directed from cell phones.[20]

It would be foolish to deny that such attacks are *possible*. But no evidence has been produced that such attacks have happened. The allegations are characterised by unconvincing assertions such as:

1. 'According to the grapevine, some of these private players engaged by the EVM manufacturers [to check and troubleshoot the EVMs] are close associates and relatives of political leaders.'[21]
2. 'There were no apparent reasons as to why a nationally resurgent Congress party should suffer losses in a state where the party had been out of power for a decade.'[22]
3. 'Is there something esoteric [sic] and mysterious in the fact that the only two parliamentary elections in India's parliamentary history, where the pollsters in general have gone horribly wrong, were totally electronic elections in which electronic voting machines (EVMs) were used all over the country?'[23]
4. 'Many such instances of election fixers [offering to rig EVMs] have been narrated to me …'[24]
5. 'From various problems cited in this chapter, it is evident that hackers already appear to have done so [i.e., 'manipulated' EVMs].[25]

Chapter 2 of *Democracy at Risk!* begins with a paragraph on Hitler, *Mein Kampf* and the 'Big Lie' technique' and accuses the Election Commission of having 'applied the Big Lie technique to perfection' in seeking to whitewash the EVM.[26] Such exaggeration and gossip are unconvincing.

Much too has been made of the fact that European countries and the US have moved away from electronic voting or have combined it with a back-up paper ballot.[27] Narasimha Rao, for example, reproduces a headline from *Newsweek* magazine in the US: 'We do not trust machines: people reject electronic voting.'[28] These European and the US systems, however, involved networked computers aggregating votes polled at many polling stations over a wide geographical area. If you can attack the software of such systems, you can rig large aggregations of votes. A

[20] Ibid., pp.176-7, has a table of eight ways to rig the voting.
[21] Ibid., pp.156-7.
[22] Ibid., p.85. The reason might be that such a party had totally lost an effective presence after 10 years in the wilderness
[23] Ibid., p.78.
[24] Ibid., p.61.
[25] Ibid., p.54.
[26] Ibid., p.19.
[27] Ibid., pp.197-214. See also http://verifiedvotingfoundation.org/, a website, founded by Professor David Dill of Stanford University, focused on the flaws of computerised voting in the US.
[28] Ibid., p.203, citing *Newsweek* (1 June 2009).

virtue of the Indian system is that one rigged EVM can deliver no more than a couple of thousand votes, and it is possible to identify where, for example, an overwhelming and suspicious vote for a particular candidate was cast. Comparison with the US and European systems appears erroneous and misleading.

The latter quality, however, also represents a negative feature of the EVMs. It is possible, if one can get at the records after an election, to discover how individuals have voted. Some veteran election officials see this as a graver defect than the possibility of electronic vote rigging.[29]

The Election Commission has not been adroit in responding to recent criticisms. In its Press Note of 8 August 2009 after critics of the EVM system had failed to demonstrate flaws in the machine during an appointment with the Commission, the latter 'once again completely reaffirm[ed] its faith in the infallibility of the EVMs. These are fully tamper-proof, as ever.'[30] Faith and infallibility belong in religion, not politics.

According to the critics, another meeting between themselves and the Election Commission on 3 September 2009 ended abruptly. According to this version, the Election Commission opened a few EVMs to allow the critics to show how they could be tampered with. The critical group'note[d] down the details of card and circuit level checks on plain paper.'[31] The engineers working for the Election Commission 'suddenly became jittery and rushed… to stall the inspection process lest they be exposed.' The critics claimed that the Election Commission was 'in a totally panicked state' and stopped the inspection of the EVMs.[32] There have been no further inspection sessions.

What conclusions can an observer draw about EVMs?

First, there is no convincing evidence that EVMs have been manipulated to affect the result in any Indian election so far.

Second, *if* corrupt people were able to get inside EVMs, they could install components that would allow those EVMs to be manipulated. This, however, would involve a vast, very carefully orchestrated conspiracy, first to install the hardware and then to make it perform as required in the right places at the time of the poll.

[29] Email from senior official on 27 August 2010. See also Prasad *et al.*, 'Security,' p.14.

[30] Press Note, Electronic Voting Machines – regarding, PN/ECI/41/2009, 8 August 2009.

[31] Narasimha Rao, *Democracy*, p.105.

[32] Ibid., pp.105-06.

The obstacles to such a conspiracy are substantial. First, there are the claims that security is high in the government-owned companies that make the EVMs. Those who work in India know, however, that breaching such security would be possible; but having installed false hardware in new machines, the election-fixers would have no way of knowing where the machines were going to be deployed. They are distributed around the country, and there are various generations of machines in use.[33] Machines are sent to polling stations randomly, like shuffling cards for a card game, and candidates' agents are invited to observe the random-distribution process.

There is no doubt that if technicians can get inside an EVM, it can be made to perform in unintended ways. One of the responses is to point out that a national election in India uses 1.4 million EVMs. Would criminals be able to corrupt them all? The reply is that

> 'one doesn't have to tamper with all the EVMs to win elections. Elections are won by small margins and even if a few EVMs are managed … in one's favour, it can … turn a loser into the winner …'[34]

A corrupt party would aim to tamper with elections in only a few dozen key seats.

Let us assume, however, that a single corrupted batch replaced every EVM in a particular Lok Sabha constituency – somewhere between 1,500 and 2,000 machines. Two ways to manipulate the election then seem possible. On polling day, an eligible voter in each polling station would go to vote, having been instructed what to do. The corrupt voter would somehow, either without the returning officer's knowledge or with the officer's connivance, quickly tamper with the EVM to trigger a 'trojan' in the chip that had been illegally inserted earlier. The EVM would then follow instructions communicated through the 'trojan' to record votes to favour the cheating candidate.

A second method would be that on the day the vote is tallied – often a few weeks from the day of voting – a corrupt agent would be in the tally room. That person would use a wireless method, perhaps through a cell phone, to communicate with the tainted hardware, installed previously, to instruct some of the 1,500 machines to change their totals to favour the desired candidate.

The scale of this sort of fraud would be vast, even if only a few score machines in a few dozen constituencies were to be rigged. And other methods of doctoring results – e.g., inserting clip-on memory manipulators – are equally labour intensive and fiddly; they require knowledgeable

[33] Ibid., p.130. A criticism of the older machines is that they are so simple in design that they are especially vulnerable.

[34] Ibid., p.104.

people to push the right buttons at the right moments. It may all be possible, but the chances of being found out or of a conspirator spilling the electronic beans would be very high.[35]

What needs to be reiterated is the decentralised nature of the Indian EVMs. Critics of the EVM are disingenuously fond of comparing them to discredited European or North American systems; but the latter have been vast, networked operations in which the corruption of a software program can cast doubt over tens of thousands of votes. Each EVM in India is a discreet unit; it is not networked. Each accounts for no more than a few thousand votes. The final tabulation is done with pencil and paper. Each machine in a constituency is produced in the tally room, its security seals inspected and removed in the presence of election officials and representatives of the parties. Each machine then has a button pressed to reveal the votes recorded for each candidate. Party representatives examine the totals and these are written down. When every machine – close to 2,000 in some constituencies – has been examined, the written totals are added up, the sums signed off by party and election officials and the result of the election declared.

As cynics experienced in Indian elections say, the easiest way to rig a constituency is at this stage: you bribe everyone in the tally room to sign off on false totals and a false winner. The complications and conspirators are far fewer than would be required to rig EVMs effectively. The sums of money available in Indian elections today are huge – large enough to make even the most upright official pause for a moment.[36] Shady media organisations in the 2009 elections, for example, appear to have had a 'poll-period take … estimated to be in hundreds of millions of rupees' by selling favourable news coverage to candidates – or offering to forestall bad coverage.[37]

Attacks on the credibility of the EVMs will undermine confidence in them.[38] The danger is that such attacks will also undermine confidence in the electoral system and the office of the Election Commissioner, which has been one of India's most admirable institutions. Allowing critics to be arrested and remanded in custody on charges of stealing one EVM for experimental purposes is bad public relations at the very least.

To maintain its high reputation and credibility, the Election Commission needs to take various steps:

[35] An Australian politician, now dead, had a credo that when faced with the choice between a conspiracy and a stuff-up as an explanation for an event, choose the stuff-up every time.

[36] Conversations with a senior civil servant and emails with a longtime presiding officer.

[37] P. Sainath in *The Hindu* (26 October 2009), www.beta.thehindu.com/opinion/lead/article38482.ece?css=print, accessed on 30 August 2010.

[38] This is happening with both constructive criticism and ill-informed commentary. *DNA*, Mumbai (7 September 2010), p.10. *Sunday Express* (5 September 2010), p.13.

1. set up an authentication unit of specialist computer engineers under the Election Commission as was proposed in 2006-07, whose job would be to anticipate potential technical failings that critics have suggested are possible[39]
2. replace the first-generation EVMs with improved later-generation models to incorporate safeguards suggested by critics and thus minimise both the possibility of tampering and of mechanical failure as the machines age
3. institute constant random checks on the storage facilities of EVMs around the country to demonstrate high standards of security between elections[40]

In the longer term, the Commission needs to explore the requirements and costs of a voting system that leaves a paper trail. This would complicate the EVM system and add to the costs. Such a system would involve a printer being attached to each EVM. A voter would vote electronically and receive a printout with the symbol of the candidate for whom the vote was cast. The voter would deposit that slip of paper in a ballot box. In the event of dispute over the electronic returns, the paper returns could be called on. Such a method introduces the complications of security of paper and effectiveness of printers, but given that criticism of EVMs will continue, it is sensible to anticipate the demand for a paper trail.[41]

In conclusion, convincing evidence has not been presented that an Indian election has been won through electronic rigging; but the threat from the geeky *goonda* remains a possibility. The task of the Election Commission is to anticipate and prevent such possibilities and demonstrate constantly and publically the ways in which the EVM system is made secure and honest.

. . . . .

[39] Narasimha Rao, *Democracy*, pp.26-7.

[40] The Election Commissioner announced additional checking and random dispersal of EVMs for the Bihar state elections in October 2010. *The Hindu* (7 September 2010), www.thehindu.com/news/national/article617920/ece?css=print, accessed on 7 September 2010.

[41] India's critics of the EVMs make much of the fact that European countries have been abandoning electronic voting and that most US states require a paper verification. 'The EVM is like a black box in which you cast your vote. You do not know what happens to it. It does not generate any physical record of voting' (Narasimha Rao, *Democracy*, p.49). The difference, however, is that the European and the US systems involve networked computers that accumulate large totals electronically. The decentralised nature of India's EVMs minimises some of the risks and maximises the difficulties for those who would rig elections through the EVMs.