Focus Group Views on Prêt à Voter 1.0

Steve Schneider* Morgan Llewellyn† Chris Culnane* James Heather* Sriramkrishnan Srinivasan * Zhe Xia*
*University of Surrey, UK
†IMT Lucca, Italy

***Abstract*—This paper discusses the findings of a series of four focus group sessions carried out on a variant of the original Prêt à Voter prototype implementation [2]. The aim of these sessions was to investigate users' ability to use the system, to discover any inadequacies of the system, and to gauge the participants' understanding of its security mechanisms. The groups also discussed general issues around security in election systems.**

***Keywords*-Prêt à Voter, trustworthy voting systems, requirements, focus groups**

I. Introduction

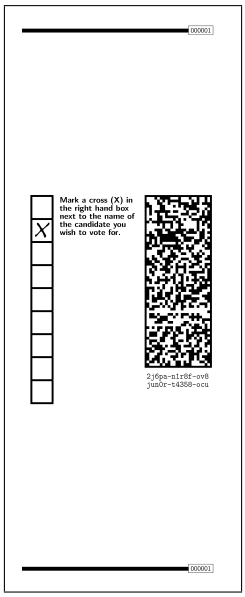
This paper reports on a series of four focus group sessions carried out on a variant of the original Prêt à Voter prototype implementation [2]. The aim of carrying out these focus groups was to gain an understanding of the various issues that voters might have with an implementation of Prêt à Voter, including, but not limited to, their ability to use the system correctly; their understanding of the system, in particular its security features; their trust in the system; and their attitudes to the system. We were particularly interested in identifying issues at an early stage that will require addressing in the next implementation of Prêt à Voter. These issues might range from straightforward usability issues which are easy to address, through the identification of security mechanisms that users are unwilling or unable to use in practice.

The version of Prêt à Voter used for these focus groups was based on the existing prototype previously developed at the University of Surrey [2], based on the design in [4]. The Single Transferable Vote election method used in the original implementation was replaced for the focus groups by the First Past The Post method. The ballot form contained only one race, with nine (fictitious) candidates, rather than several races as had been used previously. This simplified the casting of a vote to the marking of a single 'X' against the selected candidate on the ballot form, as occurs in UK general elections, providing a voting experience as familiar as possible to the participants.

II. Background: Prêt à Voter

Prêt à Voter [7] is proposed as an end-to-end verifiable voting system. It is designed to enable an audit trail from the voters casting their votes through to the final tally. It achieves this in several stages: the voters are able to verify that their vote has been included in the processing of the votes; the processing of the votes (which involves anonymising and decrypting the votes) can be verified by independent auditors who are able to confirm that the votes output correspond to the votes input; and the tallying of the decrypted votes, which can be verified independently, since the decrypted votes are public. There are several variations on the technical details of how this is done, as discussed in [7]. The version used in the focus groups was based on the decryption mixnet scheme of [4] whose implementation is described in [2]. However, the voter experience is similar across the various designs, so the findings from the focus groups, which are concerned with the voter experience, understanding, and responses, are applicable across the Prêt à Voter family.

To provide the intended security, Prêt à Voter requires voters to follow particular procedures: to cast their vote, to participate in ballot audits, and to check later that their vote has been included. Ballot forms each contain a list of candidates in a randomised order, and a voter is asked to mark a box against their preferred candidate (see Appendix A). The form is then divided down the middle, to separate the list of candidate list from the marked box, and the list of candidates is destroyed. The remaining half contains the marked box consisting of the vote, and also the order of candidates in an encrypted form as a barcode (for the system to later reconstruct the vote), as in the following example:



The marked box could have been against any candidate, so this half does not give away who the vote was cast for, thus providing vote secrecy. It is scanned for submission to the system for processing, and the voter retains a record of what has been scanned, for later checking that it was included. The barcode is not decrypted at this stage.

In Prêt à Voter, voters are also offered the opportunity to audit ballot forms. The integrity of the election relies on the integrity of the ballot forms: that the encrypted candidate order used to reconstruct the vote matches the order printed on the ballot form. One of the proposed ways of ensuring the integrity of the ballot forms is to ask voters to carry out checks and in some cases ask for an audit of a ballot form they have been given. Audit of a ballot form involves decrypting the encrypted candidate order and checking that the result matches the printed list. Not all voters are required to do this, but we assume that sufficiently many will choose to audit, to provide the random sampling necessary to detect any attack on integrity with sufficiently high probability.

Thus there are three processes involving the voter in Prêt à Voter:

- Voting: the primary purpose;
- Ballot auditing: to ensure integrity of the ballot forms;
- Checking inclusion of the vote: to ensure their vote will be counted as cast.

There are other checks and security measures involved in the stages of processing the votes, but these do not involve the voter and so we are not concerned with them in this paper.

III. Focus Group Setup

Four focus group sessions were run in total: two in Crawley, Sussex, UK (24 February 2010), and two in Birmingham, UK (1 March 2010). In each location the groups were separated by age, using the age ranges 'over 35' and '18–35', referred to in this document as Group 1 and Group 2 respectively. There were approximately eight participants in each group, and they were screened to have voted 'in a recent election' when invited to participate.

Focus groups have previously been successful in eliciting voter attitudes [9]. They provide a good way of identifying a range of reactions and viewpoints at an early stage of development, while high level design decisions are still under discussion. The intention in our case was to use an initial prototype to obtain reactions, concerns and aspects of voter understanding, which would inform our development of the next version of Prêt à Voter.

The discussions were held at custom viewing facilities, and in each case were chaired by a professional facilitator: one for Crawley and one for Birmingham. Although the facilitators were different in the two locations, they both used the same discussion guide, which had been prepared before any of the discussions took place. The research team did not come into direct contact with any of the participants, but were able to watch the discussions from behind a one-way mirror. The participants were made aware that the research was being conducted by Surrey University, and that some of research team were behind the mirror. The discussions were recorded by video and later transcribed.

Each session lasted around 90 minutes. The sessions began with a general discussion about voting and brought in security issues. The Prêt à Voter prototype system was explained and discussed, and then the participants were asked to carry out several tasks on the system: voting, auditing, and checking their vote. They discussed their experience, and their understanding of the various aspects of the system design was explored. The full discussion guide used for the sessions is reproduced in Appendix B.

The transcripts of the focus group discussions were analysed by the facilitators, who each extracted the key points from the discussions and provided a written report on the sessions. The research team took notes of significant points during the sessions, and also reviewed the transcripts to identify issues.

IV. Findings for Prêt à Voter

Once the system had been introduced, participants were asked to carry out various tasks using the system. Our interest lay in observing how easily they could carry out the voting task, how well they understood the security mechanisms underneath the processes, and their attitudes to the various elements of Prêt à Voter.

A. Casting a vote

The first task they were asked to carry out was to cast a vote. Participants were provided with the instruction sheet 'Voting with the Prêt à Voter voting system' (reproduced in Appendix C) and asked to perform the following tasks: select a candidate, mark an 'X' by their chosen name, separate the list of names on the left-hand side from the marked right-hand side, feed the left-hand side through the shredder, and then have their ballot form scanned and receive the receipt. When participants had completed these tasks, they were then asked to check that the printed receipt matched what had been scanned, and to retain it.

In general, most participants were able to cast votes to their satisfaction, and to check that the receipt matched the vote that had been cast in terms of the position of the 'X'. However, upon review of the voting process and participant comments several minor and major deviations from the instructions were identified that indicate either an improper design or a lack of participant understanding.

Two design issues brought up during the voting process related to how the ballot sheet was formed and read. One point of slight confusion encountered by one of the Crawley groups was which way the ballot should be inserted into the machine. Another participant asked how the scanning

and audit technology would operate in the event of over- or under-voting.

A more significant issue was that, in one of the groups, the voters forgot to shred the list of names, and simply formed a queue at the scanner. Hence even with a facilitator who had a reasonable understanding of the system, and a discussion with the group about how the destruction of the left-hand side ensured secrecy of the vote, the group collectively forgot to shred their left-hand sides as required by step 3 of the instruction sheet. When asked about their failure to shred the left hand half they said it did not matter to them.

Facilitator: *None of you have taken off your list of names and shredded it, why is that?*

Respondent: *Actually I've got to be honest we all think, we all did just follow the person in front of us, so who's to blame?*

Facilitator: *Does it matter, do you wish you had?*

Respondent: *No, not really, I suppose you get another bit of paper in your hand but other than that...*

Birmingham Group 2

The participants appeared to understand the reason for the random order of names when it was explained to them, and could see that this ensured that the marked vote (and the receipt) did not indicate the selected candidate, but only a position on a random list. They did not express any particular usability concern about the names appearing in a random order.

However, later comments on the receipt showed this understanding to be superficial in some cases. Some participants expressed an expectation that the receipt should say who the vote was for (perhaps this expectation was raised by the word 'receipt').

> *I think that actually seeing a name is the thing that puts your mind at ease, rather than matching up your cross there.*
>
> Crawley Group 2

> *I do think if you could, say you do want to just go home and confirm it's more reassuring when you know that you have actually put the cross in the right place. Because you could have voted for Bill and not Ben by accident. It is just confirming.*
>
> Crawley Group 2

This indicates that they had not fully understood the purpose of randomising the list of names, which is precisely to ensure that the evidence provided does not indicate who the vote was for.

There was some discomfort that the vote casting process does not provide direct feedback of who the vote is for. In the casting of the vote, participants would like to see the name of the candidate they have voted for on a small screen to confirm that their vote has been entered.

> *Yes, I'd agree that if it came up with a name just on a small screen and so you know you fed your vote in and it came up with a name, you could walk away confident that it has read that bit of encryption and it has come up with that name and so you can walk away happily. Then if you wanted to dispute it at a later stage, if you want to dispute the system then each individual is responsible for not only casting their vote, but reading the name on the screen.*
>
> Crawley Group 2

They had no concerns regarding possible secrecy issues in this respect. They indicated that they would rather risk someone else seeing their vote than any uncertainty that their correct vote has been registered.

> *I would rather the chance that somebody might look over my shoulder and glance at who I voted for, and know that my vote has gone to the correct person, than perhaps have doubts in this system, having not been told by e-mail or on a little screen that my vote for Daniel has actually gone through.*
>
> Crawley Group 2

B. Auditing a ballot form

Participants were able to carry out the instructions from the instruction sheet 'Checking ballot forms in the Prêt à Voter voting system', and the actual process of auditing was quite straightforward for participants.

However, there was less understanding of the purpose of auditing ballot forms, or at least offering that possibility to the voters themselves. One group (Birmingham Group 1) were not interested in auditing ballot forms and had to be cajoled into it, and of that group one participant doing an audit did not compare the lists of names.

Some considered that an audit would not provide certainty because it did not relate to their actual ballot paper, and that there might still be room for error with other papers.

Some participants who had concerns felt that these would not be allayed by checking the occasional ballot paper.

> *If it's just like a percentage, then I guess it's how much is it going to be audited really.*
>
> Crawley Group 2

> *You can't tell that just checking the odd one here and there.*

Furthermore, there was a feeling that if a ballot paper did not audit then trust would be gone for ever.

> *Even if you'd voted like that for fifteen years and you'd got it right and you check it and it gets it wrong just once you'd think for the last fifteen years everything's gone wrong.*
>
> Birmingham Group 2

> *It would be an instant loss of faith and I think a lot of people would lose it if something came up wrong.*
>
> Birmingham Group 1

Hence there is an understanding that audits have the potential to expose problems with the system.

However, this understanding did not translate into a desire to carry out audits. Participants were not in the mindset of wanting to check that the system was indeed behaving correctly. In some cases they felt uncomfortable even with the discussion that the system might not be trustworthy.

> *I think obviously England would be shocked if there was some conspiracy in the voting system because we kind of demand and agree in ourselves that it is trustworthy, so you know I'm not sure. Is this telling us that there is something not right? Is it a corrupt system?*
>
> Birmingham Group 1

In some cases they felt it was inappropriate to be asked to check a system they could be asked to vote with.

> Facilitator: *But you're saying that if the system were proven to be inaccurate then the whole system would fail, but you don't want proof that it is accurate?*
>
> Respondent: *We trust.*
>
> Respondent: *We trust.*
>
> Respondent: *You have got to trust.*
>
> Respondent: *You've got trust in the current system haven't you.*
>
> Birmingham Group 1

Some expressed an expectation that the system should be validated and approved fit for purpose prior to their involvement with it.

> *If there are any doubts about the process, the system, then people wouldn't go. A lot of people wouldn't go, if they had those doubts, they wouldn't bother. So the certainty has to be before the system is started up.*

C. Checking inclusion of the vote

Participants were able to carry out the instructions from the instruction sheet 'Checking your vote has been included in the count in the Prêt à Voter voting system', and the actual process of checking the receipt on the website was quite straightforward for participants.

Some wanted to see how they had voted. For some participants, confirming simply that their encrypted vote on the bulletin board corresponded to their receipt did not provide a sufficient guarantee for them. They wanted to see who they had voted for, and complained that:

> *You can't tell, or be reassured that your vote has been registered for who you voted for.*
>
> Birmingham Group 2

For most participants, having a receipt did not appear to add anything in terms of their trust in the system. They noted that they do not have a receipt with the current system used in the UK, and have no need for one.

> *You don't have one now, why do you need another one?*
>
> Crawley Group 1

> *What is the advantage, the bonus of doing that? Why would you want to go and do that, because you know you've voted and I've got a receipt? I mean why would I want to go and do that process?*
>
> Birmingham Group 1

However, some recognised that the receipt gave more confirmation than is available with the current system.

> *To be honest it's more confirmation than what we get now because at the minute we just have somebody sitting there that says thanks, I will count that later but we don't even, they might just think oh forget it and just screw it up and chucks them in the bin.*
>
> Birmingham Group 2

The majority of participants said they would not bother to check their receipt, but were happy that others were doing it.

> *I can't see me going back home to check it.*
>
> Birmingham Group 1

> *You'd have the small minority that would want to check but most people would walk out and as far as they've walked out, they've voted, it's finished with until they hear the result and then they just*

get on with it.

Birmingham Group 1

I think if you were happy to use this system, I don't think I would personally require a receipt, so you could maybe have it as an option if somebody wanted a receipt

Crawley Group 1

This was also seen in the context of auditing:

It might not be something that we would bother for ourselves but it's got to be in place hasn't it, it's still got to be in place.

Birmingham Group 1

Others could not see the point of checking the receipt online.

I know what I voted for and that's it and it's electronic then it's gone.

Birmingham Group 1

Well that receipt clearly shows where I put my 'X' in, so why would I need to check it online?

Birmingham Group 2

V. More general findings

Some more general attitudes and views also emerged during the course of the focus groups.

A. Time and Convenience

Firstly, it is clear that time and convenience is important. There were concerns that the voting process takes longer and that there are more steps.

The thing is now you go in, you take your card and you get a ticket, you go to the booth, you cross it and you walk out again.. This you've got to tear it, shred it, go over to the thing, get a receipt, it's more time. If it's a computer screen you walk in, bang, bang, bang, it just seems a lot of waste of paper and very time-consuming.

Birmingham Group 1

You just expect to just go in, vote and then come out.

Birmingham Group 2

One voter (Crawley Group 1) had a vote that was not correctly read by the system first time. He did not wish to try again despite being offered the opportunity. It appeared that he felt he had done as much as he was prepared to do, and did not want to engage when it did not succeed first time. The desire for speed and convenience was also evident in the suggestions for other ways of voting, either through a touchscreen, or remotely:

So why are they bothering with the paper? Why are they not just giving you a screen where you just push a button and walk away?

Birmingham Group 1

But if you could do it on the internet then you wouldn't have to leave the pub would you.

Birmingham Group 2

Anybody got an iPhone, I want to vote, it would be great.

Birmingham Group 2

Text messages, things like that.

Crawley Group 1

Even through the telly you can, can't you?

Crawley Group 1

I'd rather be able to sit at home and do it online, surely it must be easier for them to count all the votes and things like that.

Birmingham Group 2

However, there was a recognition that such approaches might be less secure.

Oh voting, I'm always a bit dodgy with voting online because anybody can get in. You've only got to accidentally leave a password lying round or someone can have a lucky guess, so I wouldn't really go online and do it.

Birmingham Group 2

B. Vote privacy

The majority of the participants said they personally were not concerned with others knowing how they voted, though there was a general recognition that vote secrecy was important and that other voters might want to keep their vote secret.

However, some also seemed to accept without concern that 'they' might know how you voted, and almost saw how they voted in the same way as other 'consumer information' that might be retained about them:

Tesco know, Tesco's know what you shop for, it's the same and pet insurance and stuff like that, so they can sift out anything can't they

Birmingham Group 1

Yes of course it can [learn how you have voted and retain that for future reference] because if

you go to Amazon, if you are buying books it knows whether you like history, horror you know, it's nothing for it to pick up on what you are going to vote in the future as such.

Birmingham Group 1

C. Trust in computer systems

Attitudes to trust in computer systems generally will naturally be a factor in voters' trust in an electronic voting system. There was a perception that some trust needed to be invested in the system, and that explanations of its security need to be available.

You're putting a lot of trust into this encryption code that it's actually voting for the right candidate.

Crawley Group 2

I'm not certain. I'm not. I'd have to be convinced that it was a secure system, as I see it. I know what you're saying about the post on one hand, that my figures, do you know what I mean? I'd like to know what the controls are on it.

Crawley Group 1

There was also a general awareness of the kind of things that can go wrong with computer systems, accidentally or maliciously, and some well known failures in the UK were mentioned.

If it's a computer, it might be more liable to be tampered with

Crawley Group 1

What if there a server failure or something like that; it just loses all the votes. It's not like the tickets get mixed up and you can do a recount of that box. Once it's clicked and it's gone, do you really know that it's voted.

Crawley Group 1

I think with all this data going missing, in the NHS, people's records, personal records and things like that, all this so called 'secure' data, you know these people have no doubt gone to the best people to do the job and yet it's still going missing. So I think the concern is that this could happen again you know.

Crawley Group 1

VI. Summary of issues raised

The purpose of the focus groups was to elicit issues to be considered in the development of the next prototype of Prêt à Voter for use in wider ranging user trials. Some suggestions can be incorporated, but others (e.g. receipts showing how you voted) are not appropriate owing to the very nature of the system. Some of the issues raised will require further research.

A. Considerations for enhancing Prêt à Voter

In functional terms, participants were generally able to cast votes with Prêt à Voter without difficulty, and to follow the instructions for auditing and for checking their receipt.

However, their understanding of some of the security aspects was not so strong. This can have an impact on security, since it may affect whether voters carry out the procedures which are necessary to provide the security assurances, such as shredding the left-hand side, auditing ballots, and checking receipts.

These observations concur with those reported on trials with Scantegrity II [3, 8], and with a range of prototype vote verification systems [5, Chapter 6]. In those cases voters were on the whole able to cast a vote without significant additional difficulty, but their behaviour or their responses to questionnaires indicated a weaker understanding of or interest in the security mechanisms. For example, it was observed in the Scantegrity Mock Takoma Park voting trial [8] that

> "Some Mock1 voters were enthusiastic about the security features of Scantegrity, but most seemed not to care much about security, focusing primarily on the physical process of receiving a ballot, marking the ballot, and scanning the ballot."

Given voters' primary focus on casting their vote, with the security mechanisms secondary in some cases, we should perhaps consider other ways of carrying out the security procedures. Further, in view of the participants' emphasis on time and convenience, the design of the system should aim to minimise the expectations on the voter who wishes simply to cast their vote with the least possible overhead in processes or need to understand. In any case, the key point is that the system must not be able to tell reliably which voters are carrying out the security checks, so that the security-conscious voters are a random sample unknown to the system.

Strong procedures will need to be in place to ensure that the left-hand side of the ballot is indeed destroyed when a vote is cast. Our experience suggests that it is not enough to rely on officials or poll workers to remind voters and to enforce this, and not enough to rely on voters who also may not understand the reasoning, or who may not themselves have privacy concerns.

With regards to audits and to checking receipts, it may be appropriate to involve some authority in either or both of these tasks, either to augment voters' participation or else to take it over. This approach was taken to auditing ballots in the use of Scantegrity II in the Takoma Park municipal

election [3], where an official carried out audits of ballot forms throughout election day; checking receipts was left to the voters.

Participants' desire for a speedy process also highlights that it is important that the scanning of votes and printing of receipts must be fast and reliable, and that the hardware in the next prototype should be as fast as reasonably practicable. The danger if queues could form is that voters may decide not to wait, or that poll workers are put under pressure, or that voters are themselves put under pressure if there is a problem with their vote that requires some corrective action which holds up the queue.

B. Privacy vs convenience

The Prêt à Voter system is designed to provide the highest levels of vote privacy: that a voter cannot be linked directly to their vote. It provides privacy both from other people (in that the receipt does not indicate the vote), and from the components of the election system itself, by distributing trust.

However, additional elements can be added to Prêt à Voter which make voting easier or more convenient, or increase voters' confidence in the system, but with some compromise of privacy. For example, the use of touchscreens, or remote voting, can be considered.

In considering possible additions to Prêt à Voter it is important to understand the tradeoff of privacy against convenience. There were a variety of views expressed on their importance for participants, which give rise to questions concerning the extent to which privacy can be weakened. For example

- Can a voting device be permitted to know (transiently) your vote?
- Equipment is intended to ensure certain properties (e.g. that it is not retaining information about your vote). What safeguards and assurances are acceptable?

Participants were aware that some approaches gave weaker guarantees, for example that internet voting was more vulnerable, but did not seem uncomfortable with that.

Expectations on a new system

Thus introducing a new technology might raise new expectations derived from experiences that appear similar, such as use of Electronic Point of Sale systems. The understanding of 'receipts' is one example: receipts seemed to introduce an expectation of what should be on them. However, this may be due to the terminology used; the word 'receipt' may have connotations that some other name (e.g. 'confirmation slip') does not.

One area for further research would be to elicit the expectations on voting systems; and if the current system changes in particular ways, to identify how the expectations change. A related research question would be the extent to which expectations depend on the terminology used.

VII. Voters' understanding of Prêt à Voter security

Participants' understanding of the various security mechanisms of Prêt à Voter were varied, and it was difficult to elicit in the focus group setting how strong their understanding was. More systematic experiments with Prêt à Voter would be required to gain a better understanding of how well users can understand the elements of Prêt à Voter, and this would be an aspect worth exploring in greater depth, to inform the best way of presenting and running Prêt à Voter in the field.

A related question is the extent to which voters need to understand the security mechanisms in order to participate in voting. It seems likely that an understanding of the reason, e.g. for checking the receipt, is more likely to encourage voters to follow the processes, and conversely a lack of understanding will lead to these processes being ignored. It may be appropriate to revise or replace processes whose motivation is not so well understood.

A. Terminology

Analogy and metaphor are strong tools for explanation, but the examples must be carefully chosen to be properly effective. We need to take care that we relate the voting process to something voters already know. However, accurate analogies familiar to voters are not so easy to find. Adida [1] discusses why assurance in voting systems is *not* analagous to assurance in banking systems, or in flight control software, but it is difficult to find common examples of systems that are similar. One example is 'gift receipts', which give the idea of a receipt with only partial information (the price is omitted).

We also find that the use of particular words raises expectations and associations for the participants. We saw this with reference to 'receipt' and to the 'audit' process.

The word 'receipt' has connotations of evidence of a transaction, and some participants thus expected the receipt to indicate who they had voted for. Being more explicit about what the receipt contains, perhaps calling it a 'vote inclusion record', might help in managing voters' expectations.

The word 'audit' may have negative connotations, since it is concerned with evaluation and checking of systems or processes, and we saw some discomfort around the idea that the systems might not be trustworthy. A more positive word such as 'verification' or 'confirmation' may be a more user-friendly name for what the Prêt à Voter literature has termed 'ballot audit'.

VIII. Conclusion

The focus groups have provided some initial information into the ability of voters to use the Prêt à Voter system, and their understanding of it. It has also raised more general issues that we will also need to take into consideration in our design of the next version of Prêt à Voter.

Broadly speaking, we have seen that voters are able to cast a vote and to carry out the tasks of auditing a ballot and checking their receipt. However, they can make mistakes that have security implications, as we saw one entire group forget to shred the left-hand half of their ballot, compromising privacy.

Their understanding of the various security mechanisms, and the levels of assurance that the system provides, was more varied. It seems that it will not be possible to rely on voters' understanding of the system as motivation for carrying out ballot audit and receipt checking, and so our approach to these aspects of the system should be revisited.

The groups provided only a snapshot of public attitudes to voting, but it raises some intriguing questions and will also inform our approach to public presentation and explanation of the system. Time and convenience are very important to voters, in some cases more than the privacy of their vote. The view was expressed by some participants that they want to trust their voting system, and expect it to be validated in advance — they did not fully grasp the idea of auditing ballots during the election.

Trust in computer systems generally is also an issue. Although participants were often generally trusting of technology, they were also aware of high profile failures and some had questions about the security. This particular issue is in fact expressly addressed by Prêt à Voter, which is designed specifically to avoid the need to trust the computer system: one of the design principles is 'software independence' [6]: that the information generated by the system can be checked independently. However, presenting this argument in an accessible way remains a challenge.

Acknowledgements

This research was funded by EPSRC under grant EP/G025797/1. The analysis was conducted while the fourth-named author was a Royal Academy of Engineering/Leverhulme Trust Senior Research Fellow. The focus groups were run by Surrey Social and Market Research, and we are grateful to them for their comments on the discussion guide. We are also grateful to Jeremy Clark and to Richard Carback for useful discussions on issues around this work.

References

[1] B. Adida. *Advances in Cryptographic Voting Systems*. PhD thesis, M.I.T., 2006.

[2] D. Bismark, J. Heather, R. M. A. Peel, P. Y. A. Ryan, S. Schneider, and Z. Xia. Experiences gained from the first Prêt à Voter implementation. In *First International Workshop on Requirements Engineering for E-voting Systems*, 2009.

[3] R. Carback, D. Chaum, J. Clark, J. Conway, A. Essex, P.S. Herrnson, T. Mayberry, S. Popoveniuc, R.L. Rivest, E. Shen, A.T. Sherman, and P.L. Vora. Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy. In *Proceedings of the 19th USENIX Security Symposium*, 2010.

[4] D. Chaum, P. Y. A. Ryan, and S. Schneider. A practical voter-verifiable election scheme. In *ESORICS*, pages 118–139, 2005.

[5] P. J. Herrnson, R. G. Nieme, M. J. Hanmer, B. B. Bederson, F. C. Conrad, and M. W. Traugott. *Voting Technology*. Brookings Institution Press, 2008.

[6] R.L. Rivest. On the notion of 'software independence' in voting systems. In *Phil. Trans. Royal Society A*, volume 366, pages 3759–3767, 2008.

[7] Peter Y. A. Ryan, David Bismark, James Heather, Steve Schneider, and Zhe Xia. Prêt à Voter: a voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security*, 4(4):662–673, 2009.

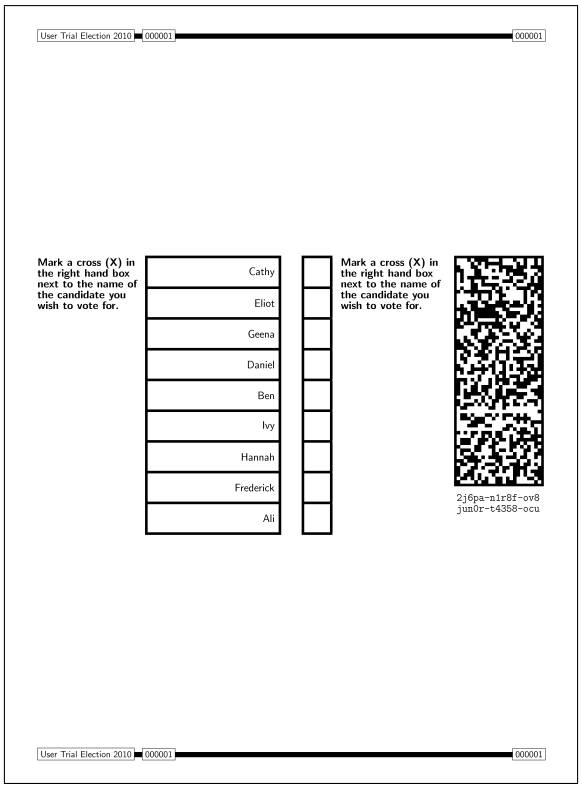
[8] A.T. Sherman, D. Chaum, J. Clark, A. Essex, P.S. Herrnson, T. Mayberry, S. Popoveniuc, R.L. Rivest, E. Shen, B. Sinha, and P.L. Vora. Scantegrity mock election at Takoma Park. In *Proceedings of the 4th International Conference on Electronic Voting (EVOTE)*, 2010.

[9] T. Storer, L. Little, and I. Duncan. An exploratory study of voter attitudes towards a pollsterless remote voting system. In D. Chaum, R. Rivest, and P. Ryan, editors, *IaVoSS Workshop on Trustworthy Elections (WOTE 06) Pre-Proceedings*, pages 77–86, 2006.

APPENDIX

A. Ballot form

The ballot form is printed on an A4 piece of paper with a perforation down the middle. Different forms provide the left-hand list of names in different orders, and the encrypted information regarding the order of the names is contained in the 2D bar code on the right hand side.



B. Focus group discussion guide

The focus groups in Crawley and in Birmingham all used the following discussion guide, developed in advance of the first focus group.

Introduction

- Introduce self — independent professional market researcher from SSMR (based at University of Surrey)
- Explain purpose of group — to help develop a possible computer-based voting system
- Introduce recording — reassure re confidentiality — reporting only in general terms (but will have agreed to DVD recording)
- Explain presence of University of Surrey personnel (in next room)

Personal introductions

- First name, occupation, when last voted (if can remember)

Background on voting (Aim for overall view, not too much detail on any point)

- What do you think about the current voting system in the UK (the actual process, not issues of representation etc.)?
- Do you have any concerns about the way we vote?
- What about voting in other countries?
- PROMPT as necessary if not mentioned:
  - Secrecy of ballot (Does this matter to you? Do you feel voting in the UK is secret?)
  - Coercion
  - Votes not being counted correctly
  - Votes not being included (e.g. Iran)
  - Votes not being registered (e.g. hanging chads)
  - Vote stuffing (e.g. Afghanistan)
  - People casting wrong vote/spoiling ballot by mistake (e.g. Scotland)

Introduce new system by explanation plus provision of information sheet for reference

- Note:
  - Random order of questions
  - Encrypted information in righthand block shows which answers are to which questions
  - Serial number identifies voter
  - Tear paper in half
  - Feed half into system
  - Take this half away with them (other half shredded)
  - Receipt is printed out

Tasks

- EXPLAIN TASKS (make sure each is clearly understood)
  1) Vote for a particular candidate (allow respondents to compare ballot papers)
  2) Check a receipt (visually)
  3) Audit a ballot form i.e. feed a blank receipt into the machine, audit will reconstruct lefthand side so can check (can't then use for voting)
  4) Check the vote on the bulletin board (via website on another laptop — type in serial number from receipt, will then show physical position of markers, confirms vote has gone into the system)
- All carry out one task, then ask for their reactions to that task — run through tasks one at a time (OBSERVE any difficulties)
  1) How easy did you find it to cast your vote? Would anything have made it any easier? Do you like voting on paper and feeding it in?

Why/why not? Or would you prefer a fully electronic interface?
2) Would you prefer to have the original as a receipt or one printed out to check? Or both? Does this matter to you?
3) How easy was it to audit a ballot paper? Would anything have made it any easier?
4) Does using the bulletin board make sense? Do you know what you are looking for? Do you think you would actually do this? Does this increase trust in the system?

Overall:

- Do you feel that using this system would make you feel reassured that your vote has been included? Is this important to you?
- How do you feel this system compares with the current paper ballot:
  - ease of use?
  - trust in the system?
  - security?
- What would help you to trust this system more? (e.g. endorsement by media — which?)

Understanding

- Do you understand each of the following:
  - Why the names are in a different order on different forms?
  - Why the names are in random order?
  - Why the ballot paper is split in half?
  - The reason for auditing a ballot paper?
  - What it would mean if a ballot paper didn't audit?
  - What it would mean if the receipt came out wrong?

Finally:

Going back to some of the things you said about voting at the beginning (PROMPT AS REQUIRED), to what extent do you think this system addresses your concerns?

Check with client whether any further issues; feed in as required

Is there anything else you'd like to say about the system?

Thanks and Close

C. Information sheets

Three information sheets were provided to the focus group participants during the sessions, as follows:

- Voting with the Prêt à Voter voting system
- Checking ballot forms in the Prêt à Voter voting system
- Checking your vote has been included in the count in the Prêt à Voter voting system

These are reproduced below:

Voting with the Prêt à Voter voting system

1) Mark an 'X' against your preferred candidate
2) Fold and tear the ballot form in half along the perforation
3) Shred the left-hand half
4) Scan the right-hand half
5) Check the receipt matches the right-hand half
6) Retain the receipt for later checking

[The order of candidates is different on different ballot forms, so the receipt does not give away how you voted]

Checking ballot forms in the Prêt à Voter voting system

1) Do not mark the ballot form
2) Tell the officials you want to check your ballot form
3) Tear the ballot form in half along the perforation
4) Scan the right-hand half
5) The barcode will be decrypted to reveal the candidate list
6) Check the candidate list matches the left-hand half of the ballot form

[voters can check that ballot form barcodes are correct]

Checking your vote has been included in the count in the Prêt à Voter voting system

1) Go to the election website
2) Enter the number of your receipt
3) Check that your receipt matches the vote recorded on the website