4

Privacy and security concerns

Introduction

4.1 Over the course of the inquiry three concerns have been raised on matters of privacy and security:

- first, electronic petitions could be compromised by the fraudulent addition of electronic signatures, by hand or more particularly by way of an automated process, resulting in petitions that were not representative of actual opinion;[1]
- second, petitioners signing electronic petitions could have their personal details disseminated, resulting in both a loss of privacy and deterring would-be petitioners;[2] and
- third, electronic petitions could be disrupted through unauthorised access to electronic support systems, and this could result either in fraudulent signatures, or denial-of-service: that is, in the electronic petitions system being unavailable for a period of time.[3]

4.2 The Clerk noted that in a UK Procedure Committee report on e-petitions it was

[1] The Hon Wilson Tuckey MP, Submission no.1; Mr G Harris, Submission no.11.

[2] GetUP, Submission no.7, p.4.

[3] PPC, Submission no.2.1, p.2; see also House of Commons Procedure Committee 2008, *E-Petitions, First Report from the Procedure Committee*, Session 2007-08, HC 136, House of Commons, viewed 15 July 2009, <http://www.publications.parliament.uk/pa/cm200708/cmselect/cmproced/136/136.pdf>, p.45.

> proposed that once the e-Petition had been submitted, the principal petitioner would receive an email asking him or her to confirm that he or she had sent the petition, thereby checking that the email address was genuine. A similar procedure would be followed for e-signatories and the names of e-signatories would not be added to e-petitions until signatories had confirmed signature of petitions. The system would identify duplicate names and addresses and would prevent someone signing a petition more than once.[4]

4.3 This approach was currently in use, the Clerk told the Committee, by the 10 Downing Street electronic petitions website.[5]

4.4 In relation to the second concern, the Clerk advised that a future model for electronic petitions in the House 'will need to provide and convey security to its users to ensure that people felt comfortable using the system and providing their personal details'.[6]

4.5 In relation to the third concern, the Clerk informed the Committee that any future electronic petitions system 'will need to meet stringent IT security standards' and that it was 'essential for the system to be secure, robust and reliable'.[7] Statements by the Scottish Public Petitions Committee (PPC), cited below, also highlight the importance of this.

Preventing fraudulent signatures

4.6 The Committee considered the methods used to prevent fraudulent signatures in Queensland and Scotland.

Queensland

4.7 A number of measures are taken by the Queensland Parliament to provide checking of signatures to electronic petitions. First, the Clerk of the Legislative Assembly told the Committee, the electronic petitions web-site protects against 'auto scripting', so that:

> each and every time somebody goes to sign up on a petition a page comes up that makes them copy down a number—and

[4] Clerk of the House of Representatives, Submission no.13, p.7.

[5] Clerk of the House of Representatives, Submission no.13, p.7.

[6] Clerk of the House of Representatives, Submission no.13, p.8.

[7] Clerk of the House of Representatives, Submission no.13, p.8.

> authentication number, if you like. [This] … essentially … stops people from running auto script databases. So somebody cannot actually have a database of names and addresses and automatically download that onto our system. The auto script procedure makes it a requirement that each and every time somebody enters an e-petition they are given an authentic, individual number and that number has to be put on the system.[8]

4.8 Second, while the system 'cannot stop people individually entering fraudulent names onto it, we can see ISP addresses':

> Say one computer has entered 500 addresses overnight. We can tell if it comes from the same IP address, so that would give us an indication to tell us whether or not there is fraud involved or whether or not it is just people where a petition has been popular.[9]

4.9 The Clerk told the Committee that this ability to check signatures against IP addresses was one of the advantages of parliaments hosting their own system, in contrast to arrangements at the Scottish Parliament where the system is hosted by a third party: 'We felt that, if we were going to have an e-petitions process, it should be administered by the parliament itself, which reduced the risk of any sort of fraud'.[10]

4.10 However the Clerk suggested that there was no absolute method to verify all signatures: 'when you are dealing in the electronic world, there are limitations to authentication'.

4.11 Comparisons between hard-copy and electronic petitions provided a useful perspective:

> I think we have to take a relatively pragmatic view towards authentication. My view is this: for hundreds of years paper petitions have circulated in the community and members have placed their names on and signed petitions. The reality is that we have never conducted audits to make sure that those paper petitions are all the time authentic. We have only ever investigated fraud when allegations have been made and there has been some evidence of fraud submitted. So for hundreds of years we have accepted paper petitions and have taken at face value that there is

[8] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, pp.4-5.

[9] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.5.

[10] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.2.

> no fraud involved with them, unless an allegation is made to that extent.[11]

4.12 As a result, Mr Laurie told the Committee:

> I think we have to be as pragmatic when it comes to electronic petitions. We have to take at face value that the people who are signing are actually the people who are putting their name to it, if you can understand what I mean, until or unless somebody takes the contrary view.[12]

4.13 However, the methods employed by the Queensland Parliament provided a measure of control over the veracity of signatures, and applied a filter for more obvious instances of fraud:

> There is no way that we can guarantee, or anyone can guarantee, authentication of people online unless there is a process for authentication such as that which the banks have with PINs or identification numbers. We have no way of being able to do that. However, the fact that it is done in-house here does allow us to notice suspicious activity. For example, if there is a lot of activity on a petition overnight, if the numbers go up by a thousand or something, it may cause us to have a look at the database to see whether there has been anything suspicious about that activity. But, as I say, there are no guarantees in this business. I do not think that the fears about authentication, however, should dissuade us from having processes like this.[13]

Scotland

4.14 The PPC told the Committee that in the Scottish Parliament several layers of checking were applied to e-petitions. First, both the electronic petitions website and the discussion forum were monitored by parliamentary staff. Second, the e-petitions system performed routine checking for duplications of signatories' e-mail address, and for 'rogue signatures', such as 'Mickey Mouse or Donald Duck'.[14]

4.15 These practices provide a level of scrutiny, but could not be expected to completely prevent false signatures, the PPC told the Committee. Parallels were drawn with hard-copy petitions, where manual checking could be

[11] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.4.

[12] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.4.

[13] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.4.

[14] Mr F Cochrane, *Transcript of Evidence*, 26 November 2008, p.2.

anticipated to control for gross inaccuracies, but not at the other end of the scale. Consequently, 'to a certain extent' the Public Petitions Committee relies 'on trust quite a lot' for both hard-copy and electronic petitions.[15]

4.16 The PPC told the Committee that under this regime, to date, there has been 'fairly little abuse of the system':

> Offensive comments, spam and rogue signatures are quickly removed (the monitoring of the site is undertaken by our clerks). This helps maintain the system's integrity.[16]

Privacy

4.17 The protection of personal information entered by signatories to petitions was considered a significant issue by contributors to the inquiry.

4.18 GetUP informed the Committee that it had 'most serious concerns' regarding privacy and online petitions hosted by Parliament. In particular GetUP suggested that an electronic petitions process should not 'allow the collection of data on petitioners - their opinions, their whereabouts, their Internet use, personal details and other information'.[17] In no way should electronic petitions provide an opportunity 'store or collect unnecessary information about' petitioners. To prevent this, 'there would need to be strong guarantees and procedures that guaranteed' their privacy.[18]

4.19 The Committee regarded this aspect of electronic petitioning as important. Particular concern was voiced at the prospect that the personal details of petitioners, harvested from electronic petitions, could be used to create email lists which in turn would be used by those with a political interest to contact voters.[19]

4.20 The Speaker of the Legislative Assembly advised the Committee that specific processes have been framed to protect the privacy of signatories to electronic petitions in the Queensland Parliament:

> The names and addresses of signatories are not available on the website. However printed copies of the tabled e-petition are

[15] Mr F Cochrane, *Transcript of Evidence*, 26 November 2008, p.2.

[16] PPC, Submission no.2, p.4.

[17] GetUP, Submission no.7, p.4.

[18] GetUP, Submission no.7, p.4.

[19] *Transcript of Evidence*, 12 November 2008, p.12.

> available upon request to the public as is the case with paper petitions.[20]

4.21 In addition:

> Petitioners' details are deleted from electronic storage in accordance with the data retention policy at a maximum of 6 months after the tabling date.[21]

4.22 The PPC did not comment directly on privacy in electronic petitioning. However the electronic petitions website of that committee makes the following statement:

> Only your name and country will appear on the website. The other details you give us are needed by the [PPC] to validate your signature. This is the same information required for a paper petition. Your details will only be used by the PPC and the International Teledemocracy Centre (ITC) who host the e-Petitions System, unless you have given permission for your details to be passed on to the principal petitioner. Your details will not be used for any purposes other than e-Petitioner, unless you have expressly given permission otherwise.[22]

System integrity

4.23 For an electronic petitions website two important aspects of system integrity are the ability to protect against unauthorised access and the ability to manage variations in demand from internet users. Representatives of the Queensland and Scottish parliaments did not report any instances of unauthorised access to electronic petitions systems.

4.24 With respect to levels of demand, Mr Laurie told the Committee that the Queensland Parliament electronic petitions system had received ‘55,000 or 60,000 signatures in a week’, for a petition on daylight saving, but there had not been ‘any problem with the system operating with that sort of capacity’.[23]

[20] The Honourable Mike Reynolds MP, Submission no.12, p.2.

[21] The Honourable Mike Reynolds MP, Submission no.12, p.2.

[22] *Public Petitions Committee: e-Petitions*, viewed 5 August 2009, <http://epetitions.scottish.parliament.uk/#privacy>.

[23] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.5.

4.25 However, the PPC was concerned about the currency and resilience of the electronic system that supports electronic petitions in the Scottish Parliament. This was important due to high volumes of traffic on the electronic petitions website which, the PPC informed the Committee regularly received 'over 1 million hits per month, some months have approach[ed] 1.8 million hits'. As a result, the PPC suggested that such systems should have a capacity 'to cope with usage beyond expectations'.[24]

4.26 These concerns were borne out early in 2008 when for 'a period' the discussion forum part of the electronic petitions website was 'down due to hardware problems'. This was 'extremely regrettable and inconvenient to us and petitioners'.[25]

Committee comment

4.27 In the Committee's view, these three requirements—reasonable measures to control for fraudulent signatures; adequate privacy provisions; and sufficient redundancy and resilience in information technology arrangements—are achievable in the House of Representatives environment.

Verification

4.28 In the future new electronic tools may come into being which support higher levels of checking for electronic petitions. At present, the Committee agrees with the proposition of the PPC that balancing the twin imperatives of maintaining security and accessibility requires careful judgement.

4.29 As the PPC suggested, the challenge is to maintain 'an open system, which allows the robust exchanges of views', while 'preventing abuse'. [26] Essentially, this entails tolerating minor degrees of error (for example in signature counts) in order to protect accessibility. While it is important that the majority of signatures are genuine and valid, too high a level of vigilance may effectively close-down access, defeating the purpose of a petitions system.

[24] PPC, Submission no.2.1, p.2.

[25] PPC, Submission no.2.1, p.2.

[26] PPC, Submission no.2, p.4.

Privacy

4.30 Similarly, the Committee also heard persuasive evidence that the privacy of petitioners was a key aspect of their willingness to participate in a petitions process. It appears unequivocal that petitioners are wary of surrendering personal details in a petition and then having those details shared with other entities, or used for other purposes.

4.31 Queensland Parliament has adopted a clear policy on the confidentiality of petitioners' details. While petitioner's names are published electronically, other details, such as postal and email address are held in confidence in the back-end of the system. Electronic records of these details are deleted six months after the petition has closed, although they are retained in the record of the business of the chamber by virtue of the petition being printed prior to its presentation to Parliament.[27]

4.32 Here too balance is important. It is a standing arrangement that hard-copy petitions in the House can be viewed, at any time after presentation, on request. This is integral to principles of transparency: once presented, petitions are public documents, open to inspection by anyone who so asks.

4.33 Such a process is consistent with the idea, indicated above, that when a petitioner signs a petition, the surrender of personal details is the democratic 'price' of expressing a view. The information lends weight to the signature by providing a basis for verification.

4.34 In the House of Representatives requests may be made to view petitions, but are infrequent. It is important to consider whether the advent of electronic petitions in the House would make it necessary to change these arrangements.

4.35 In the Committee's view, present anxieties over the sharing and transmission of personal details stem chiefly from the ease of sharing electronic information. Electronic contact lists have commercial and political value, and may be misused in a variety of ways.

4.36 These are good arguments for maintaining high levels of security and confidentiality when holding personal details in trust. Clear policies on how long such records are kept, and when they are deleted, are likely to help keep faith between Parliament and any future petitioners in the electronic domain.

4.37 In the Committee's view, however, management of such details is less problematic in relation to paper printouts of petitions. Since they can only

[27] Mr N Laurie, *Transcript of Evidence*, 24 June 2009, p.5.

be viewed in the Table Office at Parliament House, and cannot be copied, access to petitions is unlikely to represent a significant threat to confidentiality for multiple signatories attached to a petition. There is value in the transparency provided by having these physical copies available, which should be held in balance with issues of confidentiality.

4.38 Another question which relates to privacy is: should petitioners' details be used for email communications from the Committee? Does this breach confidentiality? The Scottish Parliament employs an 'opt-in' approach, whether petitioners have to actively nominate to be contacted by the PPC via email. Many petitioners appear to do this: the PPC advised that subsequent to the introduction of electronic petitions, the majority of its correspondence took place via email.[28] This is an approach which could be followed by the House.

System integrity

4.39 The Committee notes the evidence of the PPC regarding sufficient IT capacity to allow for variations in demand. It also notes the Clerk of the House's reference to system failure as a source of risk (resulting in loss of reputation) under an electronic petitions system.[29] This is important in view of the volumes of traffic quoted for the PPC's electronic petitioning website.

4.40 The Committee notes the importance of an ability to add further elements to the system to respond to such volumes and variations in internet traffic (known as 'scaleability').

4.41 The Committee also notes the importance of monitoring technical developments, including those relevant to validation and verification. This is an area of technology undergoing significant and rapid change. If the House adopts electronic petitioning, electronic petitions facilities should be maintained and developed so they remain current.

4.42 Above all, the Committee wishes to emphasise the importance of getting the balance right between different imperatives involved in, and highlighted by, electronic petitioning to parliaments. The matters considered in this chapter show a strong nexus between reliability, accessibility, engagement, privacy and credibility, in order for electronic petitions to gain traction and the House keep faith with petitioners.

[28] PPC, Submission no.2.1, p.3.

[29] Clerk of the House of Representatives, Submission no.13, p.4.

4.43 Together, these constitute a minimum requirement. Breaches in any of these areas would alienate potential petitioners. On a more positive note, if well-managed in this regard, an electronic petitioning system could make possible substantive gains in the realm of engagement—even without the use of the social networking facilities employed elsewhere—simply by providing a safe, secure, widely-accessible system through which petitioners can express their views.