Outsourcing Democracy in the Netherlands: The Risk of Contracting Out E-Voting to the Private Sector

Anne-Marie Oostveen

Oxford Internet Institute
University of Oxford
1 St. Giles, Oxford, OX1 3JS, UK
anne-marie.oostveen@oii.ox.ac.uk

ABSTRACT

Contracting out IT services is a common practice for many governments. This case-study shows that outsourcing is not without risk, especially where elections are concerned. Studying electronic voting in the Netherlands through documents obtained with Freedom of Information requests, we see that government agencies at both local and national level lacked the necessary knowledge and capability to identify appropriate voting technology, to develop and enforce proper security requirements and to monitor performance. Furthermore, the public sector became so dependent on the private sector that a situation evolved where Dutch government lost ownership and control over both the e-voting system and the election process.

KEYWORDS

Public sector outsourcing, e-voting, public-private relationship, Freedom of Information Act (FOIA)

1. INTRODUCTION

In the past decade governments have undergone a revolutionary transformation by moving many of their activities online. The concept of e-government stands for a large class of socio-technical changes in the public sector, deploying a broad set of ICT-based innovations (e.g. Snellen & van de Donk, 2000; Schmid et al., 2001; Anttiroiko & Mälkiä, 2006). Electronic government promises fast and accurate transactions and delivery of information and services. Secondly, governments want to actively engage their citizens, thus establishing greater consultation and citizen participation. New technologies offer possibilities for citizens to interact with their local or national governments on a level that have not been possible before. People can use these e-democracy technologies to register an opinion, participate in a survey or vote in a referendum or election. In this paper we focus on the e-democracy tool of electronic voting for national and local elections. E-voting refers to casting a ballot via a broad range of electronic telecommunications technology including the internet, (mobile) telephones, cable and satellite television, and computers at polling stations without internet connections (Gibson, 2002).

The use of (remote) e-voting systems is relatively new and researchers have only recently started to pay attention to the consequences of this technology. Proponents of e-voting argue that electronic voting systems provide a convenient and user-friendly voting process which will increase voter participation and reduce election costs, therefore making it usable in many decision-making situations (Dictson & Ray, 2000; Mohen & Glidden, 2001). Moreover, direct-recording electronic (DRE) voting computers report votes more quickly, prevent voters from unintentionally voting for more than one candidate, and can help the visually impaired through the use of earphones and large screens (Moynihan, 2004). Critics of e-voting express concerns about security, transparency, verifiability, the impossibility of a recount, and the lack of equal access (Phillips & von Spakovsky, 2001; Alvarez & Nagler, 2000). Furthermore, serious doubts have been raised with respect to increased voter turnout as a result of the introduction of electronic voting (e.g. Norris, 2005; Trechsel, 2007; Wilks-Heeg, 2008; Oostveen, 2007).

Despite heated political and public debate in recent years about the use of e-voting systems, little attention has been paid to the consequences of contracting out e-voting systems to the private sector, a practice very common in most countries. Bradwell and Gallagher (2007: 40) point at the dangers of merging public and private sector roles: 'This developed through the contracting out of public service delivery to the private sector in the 1980s, and has progressively blurred the distinction between the two as their functions intertwine. This has served to exacerbate the questions of power, responsibility and coercion in both'. It is therefore timely and appropriate to critically examine these outsourcing developments. Based on action-oriented research this paper will focus on the experiences of the use of DRE voting systems in the Netherlands, a country which has been an early pioneer in the field. The aim of the paper is to offer a case-study of the actual problems of outsourcing elections experienced by the Dutch government, in order to acquire knowledge and draw conclusions which should be taken into account by future adaptors of both DRE and remote e-voting systems.

2. OUTSOURCING SERVICES TO THE PRIVATE SECTOR

According to Gauld and Goldfinch (2006) there are different reasons why governments are keen on large and complex investments in new IT solutions. First of all, they point to *technological infatuation* where public servants and politicians believe that IT can transform the business of government. The public sector must now compete with the private in terms of its adoption of new technologies or face being seen as behind the times and resistant to change (Gauld & Goldfinch, 2006). Moynihan notes that: 'the adoption of technology communicates to the public that government is modern and innovative, valuing technology and its benefits' (2004: 520). The belief in ICT and technology as the ultimate solution to existing problems (progress ideology), has led many governments to embrace it and make it a top priority for modernization. This shows that the instigators of e-government have a utopian deterministic view. Secondly, *technophilia* of developers plays an important role. This 'myth of the technological fix' believes that better technology and more of it will solve any practical problem. Technology development becomes an end in itself. Finally, public officials have to deal with *lomanism*, described by the authors as 'the enthusiasm, feigned or genuine, that sales representatives and other employees develop for their companies' products and skills' (Gauld & Goldfinch, 2006: 18).

Although the above mentioned reasons are drivers for government to embrace large-scale e-government and e-democracy services, these initiatives face several challenges. A shortage of IT skills

and financial resources are two main barriers to e-government efforts (Moynihan, 2004; Chen & Grant, 2001). Lower pay in general in the public sector makes it difficult to attract and retain experienced and skilled staff (Cordella & Willcocks, 2010). Due to these financial and staffing pressures, governments have sought solutions through partnerships with private sector IT service providers. Through IT outsourcing, governments gain access to skilled staff in a particular IT service area with the added benefit of economies of scale (Chen & Perry, 2003). Another incentive to opt for IT outsourcing is the compelling pull of convenience and the political belief that private sector companies tend to be more efficient (Cordella & Willcocks, 2010).

However, contracting out is not always the right way forward. This applies in particular to elections. Most, if not all e-voting systems are outsourced to private companies rather than developed in-house, but as Xenakis and Macintosh (2005: 196) express: 'The e-electoral process, due to its democratic nature, cannot be fully outsourced to commercial suppliers'. Elections need to be open, transparent and democratic, nevertheless in the remainder of this paper we shall see that this transparency and openness can get compromised when elections are contracted-out to the private sector. Furthermore, Moynihan (2004) points out that the benefits and risks are markedly different for e-government and e-voting. While failure in e-government service cause inconveniences for individual citizens; it does not pose fundamental risks for the government. The author explains: 'the failure of e-voting technology has profound consequences for the reliability of, and public confidence in, our electoral system. The consequences of a failed election are much greater, and the adoption of e-voting has increased the risk that such failure will occur' (ibid.: 515).

3. THE CASE: E-VOTING IN THE NETHERLANDS

Electronic voting computers were in use in the Netherlands for 20 years with almost the entire voting population using two DRE voting systems to cast their ballots. The introduction of this technology in the late 1980s was not preceded by any public debate. By 2006, ninety percent of all the votes in the Netherlands were cast on the Nedap/Groenendaal ES3B voting computer. The hardware of the voting computers was built by Nedap, while the small company of Groenendaal wrote the software. Municipalities would buy the voting computers for €5000 per machine, but would have annually recurring expenses and be responsible for maintaining, storing, and transporting the machines and preparing them for each election (Election Process Advisory Commission, 2007). The second system 'NewVote' developed by the SDU company had a different business model from Nedap/Groenendaal in the sense that it didn't sell their machines, but provided a complete turn-key service. Municipalities contracted-out their elections for six, eight, or ten years. This cost them about €1200 per voting computer, per election in return for full service (storage, delivery, support, and maintenance).

Although a number of citizens, scholars and politicians posed critical questions about the security, transparency and verifiability of the two e-voting systems, government always brushed these concerns aside. This changed in 2006 when concerned citizens organized themselves and started a grassroots campaign named *Wij vertrouwen stemcomputers niet* (We do not trust voting computers). Within weeks the activists had put the security and verification problems of e-elections firmly on the political agenda, resulting in a complete shift in the way people thought about the election system in the Netherlands. After the campaign had shown many security flaws by hacking a Nedap machine (Gonggrijp & Hengeveld, 2006) the government finally took the problems serious. This was reflected in

setting up two committees which were to look into the electoral process. In September 2007 the Election Process Advisory Commission issued its critical 'Voting with confidence' report. As a result the State Secretary for the Interior announced that the 'Regulation for approval of voting machines 1997' would be withdrawn, which came into effect the next month. On October 1, 2007 the District Court of Amsterdam decertified all Nedap voting computers. The court order was a result of an administrative law procedure started by *Wij vertrouwen stemcomputers niet* in March 2007. In May 2008 the Dutch government decided that elections in the Netherlands would from then on be held using paper ballots and red pencil only. A proposal to develop a new generation of voting computers was rejected.

4. RESEARCH METHODOLOGY

Not only was the Netherlands one of the first countries to use voting computers, it was also the 8th country in the world to adopt the Freedom of Information Act (FOIA) in 1980 [1]. The Dutch Government Information (Public Access) Act (WOB, Wet Openbaarheid Bestuur) contains regulations governing public access to government information. The Act states that any person can demand information related to an administrative matter if it is contained in documents[2] held by public authorities or companies carrying out work for a public authority. The requests for government-held information can either be written (letter or email) or oral. In comparison to other countries, the volume of FOIA requests is not high in the Netherlands (Vleugels, 2009). Where in the United States the number of requests per year is 492 per 100.000 inhabitants, the Netherlands only has 7 requests per 100.000 inhabitants, lacking well behind other European countries like the United Kingdom (64) or Ireland (75). However, according to FOIA specialist Vleugels the number of requests filed at national bodies and lower government bodies is on the rise, with the share of requests filed by journalists (who are still the main users) slightly declining and the share of requests by NGOs increasing. Vleugels points out that FOIAs have on average a substantial disclosure, in 25% of all cases in the first decision. This figure rises to 45% after an administrative complaint; to 65% after a court appeal and to 75% after a high court appeal.

This paper relies on an analysis of documents received by the *Wij vertrouwen stemcomputers niet* campaign as a result of 26 separate FOIA requests. The activists sent out their FOIA requests to local government agencies, several Ministries, and the Electoral Council over a period of 3 years. Thousands of pages of reports, letters, emails, contracts, and instructions were disclosed by the authorities [3]. Although the authorities are obliged to provide the requested information within 28 days, in practice it often took them several months to send all the relevant documents. This however was not unique to the requests sent by the campaign; according to Vleugels only 10 percent of Dutch requests get a timely response (de Jong, 2009). Since October 2009 a law on penalties is in power for time delay, hopefully speeding up procedures. Once the FOIA documents were received they were scanned and published on the campaign's website to provide the information directly to the public[4].

[1] Sweden was the first country to implement the FOIA in 1766, while the United Kingdom (2005), Germany (2006) and Switzerland (2006) are among the latest countries in which the FOIA came into power (Vleugels, 2006).
[2] A document has any content whatever its medium (on paper or as a sound, visual or audiovisual recording). Documents for which third parties hold intellectual property rights and documents held by public service broadcasters are not covered.
[3] See http://wijvertrouwenstemcomputersniet.nl/Wob-verzoeken for a list of all the FOIA requests and received documents.
[4] All the PDFs were scanned with OCR (Optical Character Recognition) software so that search engines like Google can index them.

The research in this paper is part of a larger study looking at the *Wij vertrouwen stemcomputers niet* single-issue grassroots campaign against unverifiable electronic voting in the Netherlands. The study falls under the 'action-oriented' research method where the researcher was not only an observer but also a participant of the activist group studied. The author is one of the four founders and board member of the foundation and was from the start actively involved in many parts of the work undertaken by the campaign.

5. FINDINGS

5.1 Lack of Expertise

Public sectors often 'do not have the capacity, resources, and personnel to adequately develop and monitor outsourced projects, particularly as during the privatization drives of the 1980s and 1990s government-owned computer and information technology agencies were often sold off' (Gauld & Goldfinch, 2004:23). High levels of outsourcing can impede the development of state capacity which can lead to an uneven relationship between powerful IT and consultancy companies and comparatively less powerful and less competent governments. In the case of e-voting in the Netherlands it became clear that the government did not have sufficient expertise about electronic voting to lay down appropriate legal requirements, and as a consequence adopted a highly laissez-faire model. Although investigations found that the used voting computers were insufficiently secure, the Nedap machines *did* comply with all Dutch regulatory requirements. Gonggrijp and Hengeveld (2006: 21) note that: 'These requirements, although very detailed on topics that deal with availability, say absolutely nothing about security against any kind of attack.' The Election Process Advisory Commission came to the same conclusion (2007: 8-9): 'The Commission looked in depth at the way in which duties and responsibilities for the election process are allocated. This is generally satisfactory, but there are two areas that have not been adequately provided for, if at all: the laying-down of requirements for equipment used in ballots, the enforcement of these requirements and the security and management of the equipment are not properly regulated. This responsibility should rest overall with central government, specifically the Minister of the Interior and Kingdom Relations, and should be enshrined in the law and regulations.'

The lack of IT expertise also resulted in the Dutch government not taking a lead role in the testing of the voting computers to make sure they passed certification. Instead, TNO a security evaluations company in the Netherlands had been approved by the Dutch government to certify the voting computers using specific technical criteria in Dutch law. If the voting computers passed certification they could be used during elections. This did not mean that the voting computers were secure and could not be manipulated; as we already explained the criteria in Dutch law did not cover any of these issues. Remarkably TNO did not work for the government when testing voting computers; its customers were the makers of voting computers in the Netherlands: Nedap/Groenendaal and SDU. Furthermore, TNO did not send the complete test reports to the Dutch government; the ministry would only receive a single sheet of paper stating that the device had passed the certification.

When the *Wij vertrouwen stemcomputers niet* activists filed a FOIA request in which they wanted to have access to the full test reports, the director of TNO objected to publication of the documents in a letter to the Ministry of the Interior: 'They [the documents] contain personnel confidential information,

among other things the names of our employees and company secrets (about our practices, intellectual property, etc.)', furthermore: 'Also in our contracts with Nedap it has been explicitly indicated that no publication will take place. The TNO reports have not been written, each in itself at any time, to inform any person.'[5] The fact that the ministry only had a small fraction of the reports from the TNO certification institute is an indication that government no longer viewed elections as 'core business'. Even understanding how the elections worked was completely in the hands of the private sector.

5.2 Loss of Ownership Election System

Voting computers need new software whenever something changes with regard to elections. Without support the voting computers quickly become unusable. Almost all municipalities had voting computers from the 1980's, so the dependence on the vendor was enormous. Groenendaal's company wrote the software that tabulates the election results on both the local and the national level. The Dutch government depended on Groenendaal's company to the extent that it could not hold elections without his help. On April the 15th, 2005 the Dutch Electoral Council sent a letter[6] to minister Pechtold bringing up this issue of dependency. The electoral council seemed to regret that the software was not Open Source: 'The manufacturers supply updates to the software before each election [...]. So for elections to proceed the municipalities depend on these manufacturers. The Electoral Council would like to point out that neither the source code to the software inside the voting computers nor the source code to the software that adds up the totals is in the public domain.' These concerns can not be underestimated. The source code of electronic voting systems is often kept secret for two reasons.

First of all there are the commercial interests of the vendors. The software that runs on the voting computers is private property of the corporations that built the machines; hence, it cannot be examined by independent experts to see if intentional of unintentional glitches are skewing the vote count. When the Electoral Council informed the vendor that it would like to put a copy of the source code of his software at a so-called "escrow organization" for safe keeping, the vendor demanded a 100 Million Euro guarantee from the Electoral Council in case something would happen to the source code for which the escrow organization could not be held responsible.

A second reason to keep the source code a secret is the idea of 'Security by Obscurity': you protect the system by keeping the design or operation secret. As Groenendaal (2006) explains: 'Open Source or publishing the source code provides opportunities for mala fide characters and unfortunately election and election fraud are both as old as democracy itself. The fact that only a limited group of people has this knowledge can also be interpreted in a positive light'. However, according to the current computer security community the principle of security by obscurity is outdated and not suitable as a primary security mechanism. 'We would argue that in the case of voting systems, the only meaningful security against insiders is to have a voting mechanism of which all the details are published, and that a substantial portion of the general population is capable of comprehending in-depth. We pose that any other solution creates a situation in which the population depends in essence on reassuring statements that cannot be verified independently' (Gonggrijp & Hengeveld, 2007:19-20). Not only

[5] Letter of TNO (as an appendix in a decision from the ministry of the Interior, 5 September 2006, Dutch) http://www.wijvertrouwenstemcomputersniet.nl/images/6/64/Wob-3_buit.pdf

[6] http://wijvertrouwenstemcomputersniet.nl/images/1/19/20050415_kr2bz_kiesraad_maakt_zich_zorgen_om_continuiteit_bij_Nedap-Groenendaal.pdf

Nedap/Groenendaal's software was secret. When the activists sent an open letter to the mayor of Amsterdam to request access to investigate the SDU NewVote machines, the answer was that the local government did not own the e-voting systems and therefore could not grant permission[7].

Besides having no ownership over, or insight into, the software running on the e-voting computers, (local) governments also lacked understanding and control over other aspects of the elections. Looking at the FOIA documents about the SDU NewVote system we see that the elections had truly been outsourced. The local council did not control anything between the voting computer and the election results: not only the computers were supplied by SDU, but the entire process was managed by SDU. Plans for the future revealed that all programs that count and total the votes would run on computers at SDU premises and election officials would only receive the results at the end of the day.

5.3 Loss of Control over the Election Process

As already explained, around ninety percent of the votes in the Netherlands were cast on Nedap machines. In the aforementioned letter to minister Pechtold, the chairman of the Electoral Council underlined how dependent on one company Dutch democracy had become: 'We can conclude that the market for voting computers [...] in the Netherlands is very vulnerable. Only two players operate on this market. The largest part of the market is in the hands of Nedap/Groenendaal [...] it is safe to say that Nedap/Groenendaal has a near-monopoly.'

Electronic voting computers are a small fraction of Nedap's business. However, developing and supplying e-voting software is the sole business of Groenendaal which employs only a handful of people. It is precisely this small size of the company and the director's imminent retirement that started to worry the Dutch Electoral Council in 2005:

> 'It has been known for some time that Mr. J Groenendaal will end his activities in the foreseeable future. The effects of this on his enterprise are currently unclear. Also: the Dutch market for voting computers is nearly saturated. For this reason the Council assumes that there is little incentive for others to support the municipalities that use the Nedap/Groenendaal computers and software. For this reason the Council advises, in keeping with your general responsibility with regard to proper management of elections, that you initiate contact with representatives of Nedap/Groenendaal on short notice. After all, continuing support for the voting computers currently on the market as well as for the software used to calculate the results is essential in order to ensure the continuity of elections'.

Besides being concerned about retirement of key players, governments should also be concerned about the possibility of the vendor firm perhaps being taken over, or going bankrupt (Cordella & Willcocks, 2010).

Not long after the debate about the security and transparency of e-voting computers in the Netherlands started, it turned out that the fears of being too dependent on a private supplier of election software were not unfounded. Once the e-voting vendor started to feel that his business was in jeopardy he wrote to election officials in the lead up to the national elections in November 2006, threatening to cease 'cooperation' if the government did not accede to his requests. This correspondence became public after another FOIA request by the *Wij vertrouwen stemcomputers niet*

[7] http://wijvertrouwenstemcomputersniet.nl/images/f/f6/Open-brief-Cohen.pdf

campaign. The letters show that the vendor was more or less blackmailing the Dutch government. On November 10th 2006, an email was sent by the e-voting supplier warning the ministry that they would stop all activity if one of the leading figures (and computer expert) of the campaign would become a member of the independent committee that was to investigate the future of the electoral process. This committee was set up after earlier exposés by the campaign. The vendor writes:

> 'On hearing the word 'commission', my hair stands on end. […] It is not a secret that the moment hacker G. would be admitted to such a commission, we will instantly suspend all our activities and seek publicity. Apart from that, we have asked our Legal Adviser to examine the possibilities to start criminal proceedings against this criminal, based on a so-called section X procedure, for situations where the government has failed to fulfil its law enforcement duty. After all, his activities are disrupting society and thereby comparable to acts of terrorism. Detention pending trial and a preliminary investigation hearing would have been completely justified here'[8].

The vendor, sensing that the committee's report was likely to negatively impact the value of his company, offered in the same email a very straightforward business proposal: 'The ministry buys the shares of our company at a reasonable price, [...] and we will still cooperate during the next election [e.g. the provincial elections to be held only 4 months later]'.

On November 22nd 2006, the day of the national elections, the vendor wrote a letter to minister Nicolaï, in which he indicates his need to sell quickly because of his immediate retirement[9]. But when that letter fails to elicit a fast response, he writes an email to the Electoral Council saying: 'We are heading towards a very dangerous situation'. Right in the heat of election preparations, he writes: 'I have ordered my employees to halt all activity until we have received an answer that is acceptable to us', and asks the secretary-director of the Electoral Council to intervene on his behalf. As the campaigner accused of terrorism by the e-voting vendor explained: 'These e-mails shed new light on the relationship between Nedap/Groenendaal and the state, and thus also on the entire chain of events regarding voting computers. We too had the opportunity to wreak havoc regarding the election organization. But that has never been our intention; we are merely here to campaign for elections with a verifiable outcome. Had we emailed the minister in this tone, we would be at the police station now'. In reaction to the revealing FOIA documents the *Wij vertrouwen stemcomputers niet* campaign sent an open letter to the new responsible minister Ter Horst calling on her to 'take the necessary measures needed to restore confidence in the electoral process and in the notion that our government cannot be blackmailed'[10].

The FOIA documents show that the vendor was well aware of its powerful and near monopolistic position. Outsourcing e-voting services requires a good monitoring system by the public sector to keep control over the election process, something which was completely absent in the Netherlands. Even the vendor pointed at the lack of government involvement, first by noting how the Ministry of Interior Affairs was 'shining for decades along the sidelines with grave blunders' then by stating that:

[8] http://wijvertrouwenstemcomputersniet.nl/images/7/7e/20061110_groenendaal2bzk_koop_mijn_bedrijf_of_ik_kap_er_nu_mee.pdf
[9] http://wijvertrouwenstemcomputersniet.nl/images/e/e6/Letter-nicolai-translation.pdf
[10] http://wijvertrouwenstemcomputersniet.nl/images/d/d9/Open_letter_Bijleveld.pdf

> 'One must realize without exaggeration that the organization of the election process in the Netherlands is by far the best in the world! Without false modesty we dare to state that our involvement played a big role. So, you have to appreciate that our motivation, which pushed us for more than 20 years to bring the election process, despite little cooperation of respective ministries and policy civil servants, in the Netherlands and later also in other countries, to an undeniable high quality level, at present has decreased to far below zero'(see footnote 7).

6. CONCLUSION

In retrospect, it is probably fair to state that in the Netherlands the dependency on the private sector for the running of elections got out of hand. By examining the Freedom of Information documents disclosed to the *Wij vertrouwen stemcomputers niet* campaign, it becomes clear that the government had an inadequate understanding of the technology used for the elections. The government had failed to retain enough in-house capability to be able to make informed decisions about the outsourced systems, and to lay-down and enforce proper technical requirements. By not having any insight into the election software and by being dependent on a near-monopolist vendor, the government had given away their core competence of running an open and transparent election to the market; all in the name of progress, efficiency, and convenience.

In this paper we have seen that in the Dutch elections the counting of the votes was no longer the responsibility of election officials but instead of the private companies which built and maintained the electronic voting machines. In other words, the most sacred process in any democracy, counting the votes, had been completely outsourced. This means there was no system of checks and balances anymore and the election results were based on blind trust in commercial companies. This is not in compliance with the idea of transparent, open, and democratic elections. Because of the controversy surrounding e-voting and the resulting committee reports (Hermans & van Twist, 2007; Korthals Altes et al., 2007) the Dutch government acknowledged that they had to take more responsibility:

> 'The organization and execution of the elections is a government task. Within it there is only a subordinate place for the market, namely as supplier of the means that the government wants to use for the elections. The Ministry of Interior Affairs must take care that it has sufficient expertise to make its own (including technical) assessments and choices and is able to review the possible threats and risks.' (Bijleveld-Schouten, 2007: 5).

To make electronic voting more transparent for both election officials, politicians and citizens the Dutch government should move from market contracts back to in-house delivery, use open source software, involve independent experts to determine requirements and test the hard and software, set clear criteria for evaluating performance, and promote public engagement in the service delivery process.

Worldwide, both DRE and remote e-voting projects often seem to be driven by technological possibilities and bureaucratic convenience, rather than by democratic debated social utility. When efficiency dominates – as is the case with outsourcing important aspects of public sector roles – it clashes with accountability and undermines democratic values (Verkuil, 2007). This can have a negative consequence on the confidence of citizens in the election process and government in general. Therefore governments need to retain control, competency and full responsibility over such a fundamental public service as elections by retaining the main IT activities in-house.

REFERENCES

Alvarez, M and Nagler, J., 2000. *The Likely Consequences of Internet Voting for Political Representation*. The Internet Voting and Democracy Symposium. Loyola Law School, October 26, 2000, LA, California.

Anttiroiko, A-V. and Mälkiä, M., 2006. *Encyclopedia of Digital Government*. Hershey: Idea Group.

Bijleveld-Schouten, A., 2007. Inrichting verkiezingsprocess. Letter from the Ministry of Internal Affairs in reaction to the Hermans, M. and van Twist, L., 2007. Online: http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/90850/reactiekabinetadviesinrichtingverkiezingsproces.pd

Bradwell, P. and Gallagher, N., 2007. *The New Politics of Personal Information*. Demos report. London: Julie Pickard.

Chen, Y-C. and Perry,J., 2003. Outsourcing for E-government: Managing for Success. *Public Performance & Management Review*, Vol. 26, No. 4, pp. 404-421.

Cordella, A. and Willcocks,L., 2010. Outsourcing, bureaucracy and public value: Reappraising the notion of the "contract state". Government Information Quarterly, Vol. 27, pp. 82-88.

De Lange, M., 2009. *De Wob. Wet openbaarheid van bestuur of Wet obstructive door bestuur?* Journalism bachelor dissertation, Dutch University College Ede. Online: http://www.wobsite.be/uploads/documentenbank/ace152f6e8124dbb44ede5b4f7a72f84.pdf

Dictson, D. and Ray, D., 2000. *The Modern Democratic Revolution: An Objective Survey of Internet-Based Elections*. SecurePoll.com, White Paper, January 2000.

Election Process Advisory Commission, 2007. Voting with Confidence report. The Hague: Ministry of the Interior and Kingdom Relations. Online: http://wijvertrouwenstemcomputersniet.nl/images/0/0c/Votingwithconfidence.pdf

Gauld, R. and S. Goldfinch (2006) *Dangerous Enthusiasms: E-government, ComputerFailure and Information System Development*. Dunedin: Otago University Press.

Gibson, R. (2002) Elections online: Assessing Internet Voting in Light of the Arizona Democratic Primary. *Political Science Quarterly*, Vol.116, No 4, pp. 561-583.

Gonggrijp, R. and Hengeveld, W., 2007. *Studying the Nedap/Groenendaal ES3B voting computer: a computer security perspective*. Proceedings of the Usenix/Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop (Boston, MA). USENIX Association, Berkeley, CA, USA.

Groenendaal, J., 2006. WIJVERTROUWENSTEMCOMPUTERSNIET. Nedap/Groenendaal Bureau voor Verkiezingen. Online: http://www.election.nl/bizx_html/ISS/documents/WIJVERTROUWENSTEMCOMPUTERSNIET.pdf

Hermans, M. and van Twist, L., 2007. *Stemmachines, een verweesd dossier*. Rapport van de Commissie Besluitvorming Stemmachines. Online: http://www.minbzk.nl/actueel/publicaties?ActItmIdt=105148

Korthals Altes, F. et al., 2007. *Voting with Confidence*. Report by the Election Process Advisory Commission, September 27, 2007. The Hague: Ministry of the Interior and Kingdom Relations.

Mohen, J. and Glidden, J., 2001. The Case for Internet Voting. *Communications of the ACM*, 44, 1 (January), pp. 72-85.

Moynihan, D.P., 2004. Building Secure Elections: E-Voting, Security, and Systems Theory. *Public Administrative Review*, Vol. 64, No. 5, pp. 515-528.

Norris, P., 2005. E-voting as the magic ballot for European Parliamentary Elections? Evaluating e-voting in the light of experiments in UK local elections. In A. Trechsel & F. Mendez (Eds.) *The European Union and e-voting: Addressing the European Parliament's Internet voting challenge*. London: Routledge.

Oostveen, A., 2007. *Context Matters. A Social Informatics Perspective on the Design and Implications of Large-Scale e-Government Systems*. Ph.D. Thesis. University of Amsterdam.

Phillips, D. and von Spakovsky, H., 2001. Gauging the risks of internet elections. *Com. of the ACM*, 44, 1, pp. 73-85.

Schmid, B. et al., 2001. *Towards the E-Society: E-Business, E-Commerce, and E-Government*. Dordrecht: Kluwer Academic Publishers.

Snellen, I. Th. M. and van de Donk, W., 1998. *Public Administration in an Information Age*. Amsterdam: IOS Press.

Trechsel, A.H., 2007. E-voting and electoral participation, pp. 159 – 182. In: C. de Vreese (ed) D*ynamics of referendum campaign – An international perspective*. Palgrave, London.

Verkuil, P., 2007. *Outsourcing Sovereignty: Why Privatization of Government Functions Threatens Democracy and What We Can Do About It*. Cambridge: Cambridge University Press.

Vleugels, R., 2009. Overview of all 90 FOIA Countries and Territories. *Fringe Special,* September 9, 2009.

Vleugels, R., 2006. Overview of FOIA Countries Worldwide – February 1, 2006. Online: http://www.statewatch.org/news/2006/feb/foia-feb-2006.pdf

Wilks-Heeg, S., 2008. *Purity of Elections in the UK. Causes for Concern*. Report by the Joseph Rowntree Reform Trust Ltd.

Xenakis, A. and Macintosh, A., 2005. E-electoral administration: organizational lessons learned from the deployment of e-voting in the UK. In *Proceedings of the 2005 National Conference on Digital Government Research* (Atlanta, Georgia, May 15 - 18, 2005). dg.o, vol. 89. Digital Government Society of North America, 191-197.