PSO

Policy & Internet

www.psocommons.org/policyandinternet

Vol. 2: Iss. 4, Article 8 (2010)

Outsourcing Democracy: Losing Control of E-Voting in the Netherlands

Anne-Marie Oostveen, ***University of Oxford***

Abstract

Outsourcing IT services is a common practice for many governments. This case study shows that outsourcing of elections is not without risk. 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, over the 20 years that e-voting was used in the Netherlands, 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)

Author Notes: I gratefully acknowledge support for this research from the Marie Curie Intra-European Fellowship Programme, contract number MEIF-CT-2006-041676.

Recommended Citation:
Oostveen, Anne-Marie (2010) "Outsourcing Democracy: Losing Control of E-Voting in the Netherlands," *Policy & Internet*: Vol. 2: Iss. 4, Article 8.
DOI: 10.2202/1944-2866.1065
Available at: http://www.psocommons.org/policyandinternet/vol2/iss4/art8

Introduction

Over 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 and van de Donk 1998; Schmid et al. 2001; Anttiroiko and Mälkiä 2006), and 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 has not hitherto been possible. 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 technologies, 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 and Ray 2000; Mohen and Glidden 2001). Moreover, direct-recording electronic (DRE) voting computers at polling stations 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, however, express concerns about security, transparency, verifiability, the impossibility of a recount, and the lack of equal access (Phillips and von Spakovsky 2001; Alvarez and Nagler 2000). Furthermore, serious doubts have been raised with respect to the expected increase in 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 about the use of e-voting systems[1] and several independent security evaluations in recent years

[1] The first critical questions about e-voting were posed in the Dutch Parliament as early as 1989.

(Feldman, Halderman, and Felten 2007; Gonggrijp and Hengeveld 2007; Wolchok et al. 2010), 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 out 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 e-voting outsourcing developments. Based on action-oriented research—a research approach concerned with informing practice, policy, and social change—this paper focuses on the experiences of the use of DRE voting systems in the Netherlands, an early pioneer in the field. The aim of the paper is to offer a case study of the problems experienced by the Dutch government in outsourcing elections, in order to acquire knowledge and draw conclusions that should be taken into account by future adaptors of both DRE and remote e-voting systems.

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 sector in terms of its adoption of new technologies, or face being seen as behind the times and resistant to change (Gauld and 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 has led many governments to embrace it and make it a top priority for modernization (progress ideology). This shows that the instigators of e-government often have a utopian deterministic view. Secondly, the *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

http://wijvertrouwenstemcomputersniet.nl/images/2/23/19890831_kamervragen_problemen_stemmachines.pdf [FOIA #8].

Gauld and Goldfinch as "the enthusiasm, feigned or genuine, that sales representatives and other employees develop for their companies' products and skills" (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 important barriers to e-government efforts (Moynihan 2004; Chen and Grant 2001). Lower pay, in general, in the public sector makes it difficult to attract and retain experienced and skilled staff (Cordella and Willcocks 2010). Due to these financial and staffing pressures, governments have sought solutions through partnerships with private sector IT service providers. Contracting (also "privatizing" or "outsourcing") for system implementation is often viewed as an appealing alternative, or supplement, to in-house development. However, public managers must strike the proper balance between outsourcing and building capacity internally to support IT system adoption (Brown and Brudney 1998). Through IT outsourcing, governments gain access to skilled staff in a particular IT service area, with the added benefit of economies of scale (Chen and 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 and Willcocks 2010).

However, contracting out is not always the right way forward when applied to elections. Most e-voting systems are outsourced to private companies rather than developed in-house. For example, the 2007 Parliamentary Elections in Estonia, with 30,275 votes cast by remote e-voting, were contracted out to Cybernetica; three municipal elections in Finland saw a total of 12,234 votes cast on DRE software provided by Scytl in 2008; the same company also provided the software for the French Abroad Assembly Election in 2009, with 330,000 remote voters. In the United States the supply is more varied, with the major electronic voting manufacturers being Diebold (now known as Premier Election Solutions), ES&S, and Sequoia Voting Systems.[2] 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 become compromised when elections are contracted out to the private sector. Furthermore, Moynihan (2004) points out that the benefits and risks are markedly

[2] Source: E-voting database of the Competence Center for Electronic Voting and Participation http://db.e-voting.cc/.

different for e-government and e-voting. While failure in e-government service causes 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).

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 one of two available 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, 90 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 owned by Groenendaal (three employees) wrote the software. Municipalities bought the voting computers for €5,000 per machine, but incurred further annual expenses, and were also 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 10 years. This cost them about €1,200 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, the government always brushed these concerns aside. This changed in 2006 when concerned citizens organized themselves into a grassroots campaign called *Wij vertrouwen stemcomputers niet* ("We do not trust voting computers"). Within weeks these 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. The government finally took the problems seriously after the campaign managed to demonstrate the many security flaws, by hacking a Nedap machine (Gonggrijp and Hengeveld 2007). Furthermore, information revealed by Freedom of Information (FOIA) documents showed that not only did the voting computers pose risks, there

were also major flaws in the Dutch election process. This was reflected in the setting up of two external commissions to look into the electoral process.[3] The first "Voting Machines Decision-Making" Commission was tasked with examining how decisions on the approval of voting machines had been made in the past, and what lessons the Ministry of the Interior and Kingdom Relations could learn from them (Hermans and van Twist 2007). The second "Election Process Advisory" Commission was tasked with examining the current organization of the election process and making proposals for improvements and changes where necessary (Korthals Altes et al. 2007, 10). The commission was required to find answers to, among others, the following questions: what role does IT play in the various stages of the election process? Is responsibility for organizing the election process correctly allocated, and what should the relationship be between the private sector and government with regards to the use of aids (voting machines and election results computation systems)? What is the relationship between the rapidity of technological development and the election process? (Korthals Altes et al. 2007, 11). 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. This court order was the 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 that point be conducted using paper ballots and red pencil only.[4] They rejected a proposal by several members of parliament that a new generation of voting computers be developed.

Research Methodology

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 author 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 *Wij vertrouwen*

[3] http://wijvertrouwenstemcomputersniet.nl/images/8/88/SC78610.pdf [FOIA #10] and http://wijvertrouwenstemcomputersniet.nl/images/e/e0/SC80123.pdf.

[4] See http://wijvertrouwenstemcomputersniet.nl/images/c/c5/KST118412.pdf.

stemcomputers niet foundation, and was actively involved in many parts of the work undertaken by the campaign, with the intention of making her work more relevant to practice, policy, and social action (Small 1995). This direct participation from the very start of the campaign gave unique access to crucial data. Participant observation, semi-structured interviews, and informal conversations with participants all form part of the empirical work. In addition, content analysis of internal and external emails (Oostveen 2010) and content analysis of the campaign website and all information obtained by the activists were carried out. Newspaper articles and other publications were also studied.

Similar to the work of Pickerill (2004), the research was used as a way to aid the campaign, and thus directly affected the dynamics and systems that were explored. The author tried to combine reflexive methodological practice with action-oriented research that, in Pickerill's words, "seeks to 'change the landscape' rather than just survey and map it," thereby aiming to bring social relevance to the work. The study reported here is based on content analysis of documents received by the activists after several Freedom of Information requests.

Not only was the Netherlands one of the first countries to use voting computers, it was also the eighth country in the world to adopt a Freedom of Information Act (FOIA) in 1980.[5] 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 relating to an administrative matter if it is contained in documents held by public authorities, or companies carrying out work for a public authority.[6] The requests for government-held information can be either written (letter or email) or oral. In comparison to other countries, the volume of FOIA requests is not high in the Netherlands (Vleugels 2009). Whereas in the United States the number of requests per year is 492 per 100,000 inhabitants, the Netherlands only has seven requests per 100,000 inhabitants; lagging 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 in the Netherlands, with the share of requests filed by journalists (who are still the main users) slightly

[5] Sweden was the first country to implement the FOIA in 1766. The United Kingdom (2005), Germany (2006) and Switzerland (2006) are among the latest countries in which the FOIA has come into power (Vleugels 2006).

[6] A document contains content, irrespective of the medium (e.g. paper, or 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.

declining, and the share of requests by NGOs increasing. Vleugels points out that FOIAs have on average a substantial disclosure, in 25 percent of all cases in the first decision. This figure rises to 45 percent after an administrative complaint, to 65 percent after a court appeal, and to 75 percent after a high court appeal.

In total, the *Wij vertrouwen stemcomputers niet* activists sent out 27 FOIA requests between May 2006 and March 2010 to local government agencies, municipalities, several Ministries, and the Electoral Council. Thousands of pages of reports, letters, emails, contracts, and instructions were disclosed by the authorities (see Figure 1).[7] This paper relies on an analysis of a sub-set of hundreds of documents received by the campaign as a result of seven of these FOIA requests by the activists. Once the FOIA documents were received by the activists they were scanned and published on the campaign's website to provide the information directly to the public.[8]

Figure 1. The first stack of Freedom of Information documents as delivered to the activists

[7] See http://wijvertrouwenstemcomputersniet.nl/Wob-verzoeken for a list of all the FOIA requests and received documents.

[8] All the PDFs were scanned with OCR (Optical Character Recognition) software so that search engines like Google could index them.

DOI: 10.2202/1944-2866.1065

Findings

Lack of Technical 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 and Goldfinch 2006, 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 by the activists found that the voting computers used were insufficiently secure, the Nedap machines *did* comply with all Dutch regulatory requirements. Gonggrijp and Hengeveld (2007, 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."

Loeber (2008, 29) offers an explanation for why the use of voting computers became controversial after 20 years of use in the Netherlands: "Because the introduction went so easy, maybe the political attention for the subject was not great enough, causing neglect and a lack of knowledge with both the Ministry and the Parliament. New developments in computer science and security issues were not linked to voting machines even though there was enough reason to do so."

This lack of IT expertise resulted in the Dutch government not taking a lead role in the testing of the voting computers to make sure that 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. For the certification, one voting computer would be selected randomly out of a series of 10 machines provided by the supplier.[9] If this single voting computer passed certification, then all the voting devices of the same type could be used during elections. This did not mean that the voting computers were secure and that they could not be manipulated; as 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 complete test reports to the Dutch government; the Ministry only received a single sheet of paper stating that the device had passed the certification.[10]

When the *Wij vertrouwen stemcomputers niet* activists filed an FOIA request in which they requested 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. This would require a different way of reporting."[11] The fact that the Ministry only had a small fraction of the reports from the TNO certification institute is an indication that the government no longer viewed elections as their "core business." Even understanding how the elections worked was completely in the hands of the private sector.

---

[9] http://wijvertrouwenstemcomputersniet.nl/images/c/c3/20020204_TNO_verklaring_inzake_keuring_RS-vote.pdf [FOIA #1].

[10] For an example of a certification report by TNO to the government, see this FOIA document: http://wijvertrouwenstemcomputersniet.nl/images/6/6b/20051228_TNO_keuring_prototype_Nedap_ESN1_SSN1.pdf [FOIA #1].

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

Loss of Ownership of the Election System

Voting computers need new software whenever something changes with regard to an election. Without support, the voting computers quickly become unusable. Almost all Dutch municipalities had voting computers which were designed and built in the 1980s, 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 15, 2005 the Dutch Electoral Council sent a letter to Minister Pechtold, bringing up this issue of dependency.[12] 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't 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 the private property of the suppliers; hence, it cannot be examined by independent experts to see if intentional or unintentional glitches are skewing the vote count. In the Dutch case, the source code could not even be examined after the software had become obsolete, as one of the FOIA documents from the Electoral Council shows.[13] When the Electoral Council informed the vendor that it would like to deposit a copy of the source code of the software with a so-called "escrow organization" for safe keeping, the vendor demanded a 100 million euro guarantee from the Electoral Council in the case of anything happening to the source code for which the escrow organization could not be held responsible.[14]

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

[12]http://wijvertrouwenstemcomputersniet.nl/images/1/19/20050415_kr2bz_kiesraad_maakt_zich_zorgen_om_continuiteit_bij_Nedap-Groenendaal.pdf [FOIA #1].
[13] http://wijvertrouwenstemcomputersniet.nl/images/e/e4/Wob-14-3.pdf [FOIA #14].
[14]http://wijvertrouwenstemcomputersniet.nl/images/4/45/20061122_kiesraad2nicolai_bewaring_broncode_gaat_niet_door.pdf [FOIA #11].

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. Security by obscurity disregards Kerckhoffs' Principle, stated in 1883, which holds that a system should be secure because of its design, not because the design is unknown to an adversary. According to security technologist Bruce Schneier (2002), the prime benefit of making algorithms and protocols public is peer review: "Almost all secure cryptographic systems were developed with public and published algorithms and protocols. I can't think of a single cryptographic system developed in secret that, when eventually disclosed to the public, didn't have flaws discovered by the cryptographic community." His point was proven when in the United States, the supplier Sequoia was ordered by a judge to supply the source code of its touch-screen voting machines to Princeton University computer scientists, who consequently found several vulnerabilities with the system (Zetter 2009).

The *Wij vertrouwen stemcomputers niet* activists also argued for open source: "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 and Hengeveld 2007, 19–20). Not only was Nedap/Groenendaal's software 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 municipality did not own the e-voting system and therefore could not grant permission.[15]

Besides having no ownership over, or insight into, the software running on the e-voting computers, (local) government 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 were the computers 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

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

would run on computers at SDU premises, and that election officials would only receive the results at the end of the day.[16]

Loss of Control Over the Election Process

As already explained, around 90 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."[17]

Electronic voting computers represent only 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 the 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 the retirement of key players, governments should also be concerned about the possibility of the vendor firm perhaps being taken over, or going bankrupt (Cordella and Willcocks 2010).

[16] http://wijvertrouwenstemcomputersniet.nl/images/6/66/Evaluatie_Sdu_stadsdelen.pdf [FOIA #2].

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

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 FOIA request #11 to the Electoral Council by the *Wij vertrouwen stemcomputers niet* campaign. The documents show that the vendor was more or less blackmailing the Dutch government. On November 10, 2006, an email was sent by the e-voting supplier warning the Ministry that they would cease all activity if one of the leading figures of the campaign (and a computer expert) became a member of the external Election Process Advisory Commission which was to investigate the future of the electoral process. The vendor wrote:

> "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."[18]

The vendor, sensing that the Commission'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 four months later).

On November 22, 2006, the day of the national elections, the vendor wrote a letter to Minister Nicolaï, in which he indicated his need to sell

[18]http://wijvertrouwenstemcomputersniet.nl/images/7/7e/20061110_groenendaal2bzk_koop_mijn_bedrijf_of_ik_kap_er_nu_mee.pdf [FOIA #11].

quickly because of his immediate retirement.[19] But when that letter failed to elicit a fast response, he wrote an email to the Electoral Council saying: "We are heading towards a very dangerous situation." Right in the heat of election preparations, he went on to write: "I have ordered my employees to halt all activity until we have received an answer that is acceptable to us," and asked the secretary-director of the Electoral Council to intervene on his behalf. In reaction to these revealing FOIA documents, the *Wij vertrouwen stemcomputers niet* campaign sent an open letter to the newly 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."[20]

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 out the lack of government involvement, first by noting how the Ministry of Interior Affairs had sat for decades on the sidelines, then by stating that:

> "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."[21]

[19] http://wijvertrouwenstemcomputersniet.nl/images/e/e6/Letter-nicolai-translation.pdf [FOIA #11].
[20] http://wijvertrouwenstemcomputersniet.nl/images/d/d9/Open_letter_Bijleveld.pdf.
[21] See note 18.

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 various 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 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 gave 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, vote counting, 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 commission reports (Hermans and van Twist 2007; Korthal 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 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.

So far, experiences with binding local and national elections using DRE or remote e-voting have been limited. Many countries are still experimenting with the new technology, and have only had small numbers of citizens casting e-votes. Even Estonia, which became the first nation to hold legally binding general elections over the Internet, and is often seen as a successful example of an e-voting country, only had 3.4 percent of people casting a vote online in 2007, and 9 percent in 2009. This means that there is still scope for new adopters to learn from the mistakes being made by others. In the Netherlands, the DRE voting system and pilot remote e-voting projects seemed to be driven by technological possibilities and bureaucratic convenience, rather than by democratically 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 J. Nagler. 2000. *The Likely Consequences of Internet Voting for Political Representation*. The Internet Voting and Democracy Symposium. Loyola Law School, October 26, 2000, Los Angeles, CA.

Anttiroiko, A.-V., and M. Mälkiä. 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 M. Hermans, and L. van Twist, 2007 report. http://www.minbzk.nl/aspx/download.aspx?file=/contents/pages/90850/reactiekabinetadviesinrichtingverkiezingsproces.pdf.

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

Brown, M.M., and J.L. Brudney. 1998. "A "Smarter, Better, Faster, and Cheaper" Government: Contracting and Geographic Information Systems." *Public Administration Review* 58: 335–345.

Chen, Y.-C., and J. Perry. 2003. "Outsourcing for E-government: Managing for Success." *Public Performance & Management Review* 26 (4): 404–421.

Chen, Y. C. and J. Grant (2001). Transforming local e-government services: the use of application service providers. Government Information Quarterly. 18: 343-355.

Cordella, A., and L. Willcocks. 2010. "Outsourcing, Bureaucracy and Public Value: Reappraising the Notion of the "Contract State"." *Government Information Quarterly* 27: 82–88.

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

Feldman, A.J., J.A. Halderman, and E.W. Felten. 2007. "Security Analysis of the Diebold AccuVote-TS Voting Machine." *Proceedings of the Usenix/Accurate Electronic Voting Technology on Usenix/Accurate Electronic Voting Technology Workshop* (Boston, MA). USENIX Association, Berkeley, CA.

Gauld, R., and S. Goldfinch. 2006. *Dangerous Enthusiasms: E-Government, Computer Failure 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* 116 (4): 561–583.

Gonggrijp, R., and W. Hengeveld. 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.

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

Hermans, M., and L. van Twist. 2007. *Stemmachines, een verweesd dossier*. Rapport van de Commissie Besluitvorming Stemmachines. ["Voting machines: an orphaned subject". Report by the Advisory Commission on the decision making process for voting machines]. The Hague: Ministry of the Interior and Kingdom Relations.

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.

Loeber, L. 2008. "E-voting in the Netherlands: From General Acceptance to General Doubt in Two Years." In *Electronic Voting 2008, GI Lecture Notes in Informatics*, eds. R. Krimmer, and R. Grimm. P-131, Bonn, 21–30. Bonn: Gesellschaft für Informatik.

Mohen, J., and J. Glidden. 2001. "The Case for Internet Voting." *Communications of the ACM* 44 (1): 72–85.

Moynihan, D.P. 2004. "Building Secure Elections: E-Voting, Security, and Systems Theory." *Public Administrative Review* 64 (5): 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 *The European Union and E-Voting: Addressing the European Parliament's Internet Voting Challenge*, eds. A. Trechsel, and F. Mendez. London: Routledge.

Oostveen, A. 2010. "Citizens and Activists: Analyzing the Reasons, Impact and Benefits of Civic Emails Directed at a Grassroots Campaign." *Information, Communication & Society* 13 (6): 793–819.

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.

Pickerill, J. 2004. *Participatory research and internet activism*. http://www.geog.le.ac.uk/orm/ethics/ethdebriefing.htm.

Phillips, D., and H. von Spakovsky. 2001. "Gauging the Risks of Internet Elections." *Communications of the ACM* 44 (1): 73–85.

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

Schneier, B. 2002. "Secrecy, Security, and Obscurity." *Crypto-Gram Newsletter*, http://www.schneier.com/crypto-gram-0205.html (accessed May 15, 2002).

Small, S.A. 1995. "Action-Oriented Research: Models and Methods." *Journal of Marriage and Family* 57 (4): 941–955.

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

Trechsel, A.H. 2007. "E-Voting and Electoral Participation." In *Dynamics of Referendum Campaign—An International Perspective*, ed. C. de Vreese. London: Palgrave, 159–182.

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

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

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

Wolchok, S., Wustrow, E., Halderman, J.A., Prasad, H.K., Kankipati, A., Sakhamuri, S.K., Yagati, V., and Gonggrijp, R. 2010. Security Analysis of India's Electronic Voting Machines. *Proceedings of the 17th ACM Conference on Computer and Communications Security* (Chicago, IL, October 4–8, 2010). CCS '10. New York, NY: ACM, 1–14.

Xenakis, A., and A. Macintosh. 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, GA, May 15–18, 2005). dg.o, vol. 89. Digital Government Society of North America, 191–197.

Zetter, K. 2009. "In Industry First, Voting Machine Company to Publish Source Code." *Wired*, 10, 2009. http://www.wired.com/threatlevel/2009/10/sequoia/.