Parliamentary Statement for Bill L-132
Dr. Joseph Kiniry
Professor of Software Engineering and Head of Software Engineering Section
Department of Applied Mathematics and Computer Science
Technical University of Denmark
12 March 2013

Executive Summary

Moving forward with trials within the framing of the the current bill (L-132) is following the well-worn path of other nations. In general, other nations have spent enormous amounts of money and time in creating computer-based election systems that decrease public control, harm voter trust, decrease voter turnout, and, at times, caused elections to fail. Denmark has an opportunity in L-132 to do something different. I frame this distinction, and then provide several explicit recommendations for revision of L-132. If such recommendations were adopted, it opens the door for conducting high quality, scientifically-grounded, binding trials in computer-based elections at reasonable cost.

Speech

Good morning ladies and gentleman. My name is Joseph Kiniry. Thank you for inviting me here today to speak on this topic. I am going to give you a brief statement on International Experiences and Denmark's Opportunity with respect to Parliamentary bill L-132.

Firstly, a bit of background. I am what one might call an internationally-recognized expert in electronic elections, software engineering of critical systems, information security, and logic. I have worked in the subfield of electronic elections for ten years in three countries. I was a part of the active research and activist community in The Netherlands and Ireland, directly or indirectly advised both governments, and had some hand in both of those countries deciding to forbid, by law, computer-based elections.

In my decade of activity in this research field, I have rarely heard a researcher speak positively about the use of technology in elections, both in the polling booth for what we call "supervised" elections, as we have here in Denmark, and for remote elections over the telephone or internet, as we have heard about in Norway and Estonia. Virtually all public technology experts like myself are highly critical of compute-based voting, or what is colloquially known as "evoting".

I can say this with confidence because the community has had several worldwide conferences, during which manifestos summarizing the community's perspective on evoting were crafted by dozens of top researchers, including myself. I provided one such manifesto as background literature to this committee. Likewise, many independent studies and government reports written by researchers like myself have stated the same conclusion: today we do not know how to create a trustworthy traditional supervised evoting system (with a computer in the polling booth) or a remote evoting system (where one votes over the internet) that is both correct and secure and respects the fundamental principles of democratic elections.

On the other hand, I believe that technology does have a role to play in elections, but only to solve specific problems, and only if such systems are developed in a public, open, transparent fashion where correctness and security are first principles. Within the

DemTech project, which I co-lead with, among others, Carsten Schürmann who is following me here today, we call this methodology of software and hardware development Trust-by-Design, and it is one of my core research focuses today.

At its core, the primary challenge with computers in elections is that elections must have public control. The citizenry involved in the election must be able to understand and trust the electoral apparatus—the people, pieces of paper, and computers—as well as its outcome—the election result. And moreover, if information technology is introduced into an election, it must be developed in a public, open, and transparent fashion.

Unfortunately, corporations who sell electronic voting software or services are universally against public, open, and transparent IT systems. Their main argument for being proprietary, closed, and opaque is for the sake of security. It is, what we in the information security community call, “security through obscurity”. This claim is false.

A system is secure only when it is secure in the light of day, under full public view. All systems we all use every day for virtually all of our online commerce are public, open, transparent systems. To put it plainly, public, open, and transparent IT system are the cornerstone of secure online systems. All of the business that we do as corporations or individuals, all the email that we read, and all of the files we share in the cloud are secure exactly because all of the software that keeps it secure is public, open, and transparent.

Furthermore, election IT systems must be absolutely correct and absolutely secure. This means that they must be developed according to the highest levels of international standards for correctness and security. Unfortunately, no corporate, and very few academic, election systems are developed against such standards. In fact, my group is one of the few in the world that does such election systems engineering.

This is no trivial matter because, to build each new election system, (1) fundamental scientific problems, mainly involving logic and arithmetic via cryptography, must be solved, (2) technologies must be invented that turn these mathematical foundations into usable reality, and (3) those technologies must be applied in a rigorous, transparent fashion. This is difficult, but not impossible, engineering, and there are firms around the world that have these skills.

I am also something of an academic-activist who uses hacking for good, or what some call a “hacktivist”. Hacktivists like myself analyze corporate and academic elections hardware and software for correctness and security flaws.

Disappointingly, all election systems the hacktivist community has analyzed have egregious, fundamental correctness and security flaws that make them unfit for use in local or national elections. Such flaws—many of which are known, but undivulged, by the corporations that make the equipment—are one of the reasons that evoting has been banned in the Netherlands and Ireland. Moreover, their architectures are typically so flawed that they cannot be “patch up” or fixed. Therefore, only systems developed from scratch, with the correct principles of publicness, openness, and transparency, with a focus on correctness and security as mandatory requirements, have a chance at being fit for local and national elections.

Perhaps surprisingly, it is rarely the case that an election tallying system counts the votes properly, even in simple election schemes like those in the U.S.A. and the U.K., known as a “first past the post” system. If we cannot even count who has the most votes in a trivial

scheme like that, what hope do vendors have, using poor engineering practices, to correctly implement more complex schemes like that which we have here in Denmark, like the list-based scheme in the Netherlands, and like the proportional representation by single transferrable vote scheme of Ireland?

Some academic experts in election system create free, Open Source, demonstration IT system as case studies in new mathematics, security, and engineering techniques. These systems are also created to show governments and corporations that engineering election systems to the highest international correctness and security standards is, in fact, not only possible, but is cost-effective. In my research group, we have created, or are currently working on, several such systems. Our focus is on aspects of elections like processing voter lists, tallying ballots, rigorously validating others' tally systems, and a supervised, voter-verifiable paper audit trail-based (VVPAT) electronic voting system for research experimentation in novel, low-cost, end-to-end verifiable elections.

I believe that Denmark has an opportunity to learn from others' mistakes and wisely use IT for democracy. Consequently, I recommend that the Ministry amend bill L-132, based upon the criticisms and recommendations of IT and election experts that they have already received, rather than accept the feedback and change little-to-nothing in the original bill.

In particular, I recommend that trials must have a fixed termination date and must be scientifically conducted by independent agents.

I recommend that international IT standards of quality and security must be mandated for the deployed systems.

I recommend that all IT systems must be developed in a public, open, and transparent fashion, preferably with a methodology something like DemTech's Trust-by-Design method.

I recommend that such systems are used for election management, the creation and maintenance of voter lists, generation of ballots and voter cards, the management of polling lists, and the reporting of results.

I recommend that such systems are used to count ballots, so long as risk-limiting post-election audits are conducted.

I recommend, contrary to the current path of the bill, that only the disabled use supervised kiosk-based electronic voting systems to independently cast their secret traditional ballots. I do not recommend that the general public use such systems here in Denmark.

The fundamental reason for this latter recommendation is that introducing any technology into supervised elections more complex than a piece of paper and a pen means that the election is more opaque, more expensive, and has less public control. Furthermore, there is no evidence that introducing technology into a local or national election improves voter turnout; in fact, it often harms turnout.

I recommend that ballot design is changed, by adding a box in which one makes a mark, to decrease the number of spoiled ballots.

I recommend that computers should be used to analyze and optimize existing manual election procedures to increase the accuracy and security, and decrease the cost of current elections.

I recommend that manual tallying of ballots is done via an optimized sorting process, followed by weighing, rather than counting one-by-one, sorted ballot piles.

These are the key points that DemTech has made to the Ministry, either via our høringsvar or in direct communication with Ministry officials. These are the key points that I believe should be adopted in the bill and, if they are adopted, I wholeheartedly support binding trials in digital elections here in Denmark. If these recommendations are not adopted and the Ministry says, "trust that we'll do it right", then we are following a well-worn rut carved by other nations, and hence I recommend rejecting the bill.

If these changes are made Denmark will have learned from the mistakes of others, will be listening to digital election experts early in the process, and has some hope of deploying IT in a wise fashion for future elections. By doing so, the electorate may continue to trust the election and we will have solved some of the major challenges of those responsible for running elections. Denmark would then be recognized as a thought-leader in digital elections for its willingness to think different and not swallow vendors sales pitches, hook, line, and sinker.