News: Cradle of Liberty Lags on E-Voting

Greg Goth

Several United States sites call themselves "The Cradle of Liberty," owing to their importance during the Revolutionary War, and the appellation is sometimes extended to the US as a whole. However, when it comes to advancing the technology of democracy's cornerstone—voting—the US is falling far behind the United Kingdom, continental Europe, and Australia. Vendors, officials, and standards groups in those regions are leading the way toward the technological and political infrastructure that can make the peoples' voices more easily heard and counted.

Markup language standard

In February, the Organization for the Advancement of Structured Information Standards (OASIS) Election and Voter Services technical committee ratified the Election Markup Language (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=election). The EML ratification, which culminated work begun in 2001, had to account for more than data formats, protocols, and APIs. "When you talk about e-voting, you're talking about a lot of different things to a lot of different people," says John Borras, outgoing chairman of the EML technical committee and CEO of the UK's Local e-Government Standards Body.

To address these differences, Borras says the TC first developed an end-to-end process of what e-voting covers—from registration to balloting and recording. Within that process, the committee didn't distinguish Internet voting from poll voting. This enables EML to play a part anywhere data must pass through voting system components. "We were clearly coming at it very much from a public voting environment viewpoint," Borras says, "although we didn't want to preclude private sector voting—like shareholder proxies, for example."
After defining the top-level process, the TC moved on to the voting process semantics in various countries. Aligning the UK and US processes took a couple of years. At that point, Borras says, "the rest of Europe started to wake up, and we spent the next couple years trying to capture the variation of voting machines in Europe. So, this version of EML is a very generic set of XML schemas that handle data exchanges that will support—as far as we know—all the known voting regimes around the globe. To be sure, there will be others, but we have taken the prime movers and are confident we can accommodate all those voting regimes."

Numerous European public entities have already championed EML. The Council of Europe endorsed EML (http://www.coe.int/t/e/integrated%5Fprojects/democracy/02%5FActivities/02%5Fe%2DVoting/01_Rec%282004%2911E_rec_adopted.asp#TopOfPage) in September 2004 for continent-wide use (with adoption schedules at the discretion of local jurisdictions), and the UK government requires EML compatibility among e-voting components.

**UK banks on EML and interoperability**

Although the OASIS EML committee includes representatives of both the private and public sectors in the US, including IBM, Oracle, Sun Microsystems, and the US Justice Department, only one of the major US-based e-voting vendors, Election Systems and Software, is a committee member.

"They've all been invited to take part and join Oasis and to contribute to EML," says Roy Hill, a committee member and technical director of Opt2Vote, a Londonderry, Northern Ireland-based vendor. Hill says he believes ESS participated because the company has a UK market presence, and the UK government requires system suppliers to comply with EML standards to ensure interoperability.

"As an example," Hill says, "in a typical election, if Opt2Vote provides the voting system, the government may decide ESS will provide the counting system, so you have two separate providers, and because both would be compliant with EML, you would be certain the ESS equipment could read the data presented to it. In this way, the architecture of the system would be seen as having no possibility of collusion; the result would be the true reflection of the ballot as recorded."
The EML-based approach to transparency, in which public officials can choose among a variety of vendor products, might be the most striking difference between the European and US approaches to establishing e-voting infrastructures.

The UK has run numerous pilots of e-voting technology in recent years to mainly positive reviews by the nation's Electoral Commission. In a review of the nation's e-voting pilots for 2003 (http://www.sosig.ac.uk/ roads/cgi-bin/tempbyhand.pl?query=1060246851-24266&database=sosigv3), the commission affirmed the government's reliance on EML. It also praised the intent of mandating separate suppliers for different parts of the e-voting infrastructure, but it recommended some tweaking as well:

The Commission also believes that interoperability is a valid aim and that it is right in principle to explicitly separate the localised means of delivery (channel) from the central vote management. In the long term this will help to promote competition and ensure a fair marketplace. However, there are risks with this approach. With no single organisation taking total responsibility for the full system integration, there are significant risks that the operational systems are not implemented in a timely manner, and significant security risks arising through vulnerabilities at the interfaces between different suppliers.

Borras says the OASIS EML committee doesn't have any illusions that the newly ratified standard will erase the gnarly problems inherent in e-voting overnight.

"You have to recognize this whole e-voting environment—particularly remote, uncivilized Internet voting—is totally new, and there's very little precedent or well-defined business requirements," Borras says. "And once you get into that environment, you start opening the door to changes in voting legislation and practice." He sees it taking several years to stabilize the procedural and cultural foundations that will allow e-voting to become the norm.

"The UK has been very active in testing the theory of e-voting across various channels, and what we've found is, EML as it's been drawn up by OASIS is fine, but then you have to customize it to your local environment, because there are different business rules within each country that will affect things at the detail level. In the UK, we have produced a UK-customized version of EML, and I hope this pattern picks up around the world."
E-voting on the up 'n' up down under

While the UK has conducted numerous e-voting pilots, the Australian Capital Territory has used e-voting in two of its general assembly elections, in 2001 and 2004. The regional government didn't mandate that separate vendors supply different parts of the overall electoral architecture, but it did require the single vendor supplying both elections to use software that was openly available to public scrutiny. The chosen vendor, Software Improvements Ltd., designed its eVACS system on the Linux operating system to meet those requirements.

In its review of the 2004 election (pdf, http://www.elections.act.gov.au/adobe/2004ElectionReviewComputerVoting.pdf), the ACT's Electoral Commission said it was satisfied the transparency requirements addressed its own security concerns:

While there were some concerns publicly raised about the need for a paper audit trail of electronic votes the Commission is satisfied that the use of open source software, the independent audit of the software code, and the security built into the system, including its physical security, ensured that the system was transparent and reliable. Therefore the Commission believes that these concerns were unfounded.

The commission review compares this approach favorably to the US reliance on proprietary solutions:

One of the concerns with the electronic voting systems used in the USA is the fact that the computer code used in their proprietary systems is kept secret by their vendors and not made available for public inspection or even inspection by courts in the event of a legal challenge to an election result. This, combined with a history of anomalous results, means that voters and other political participants have no way of being reassured that ‘what goes in is what comes out'. In this context, providing for an independently verifiable paper audit trail is a reasonable proposition.

In addition to basing the ACT system on auditable software, the commission set up the following safeguards:

- All votes are cast in a public polling place over an isolated local network, staffed by independent electoral officials.
Voters are given an opportunity to review their votes (in preference order) before committing them to the electronic ballot box.

The computer program verifies that the vote recorded by the voter is correct by comparing the voter's keystrokes with the final record of the vote.

Votes are stored in the polling place server on two identical hard disks to guard against hardware failure.

The voter receives the message, "Your vote has been accepted," but only after the vote has been successfully written to the two hard disks on the server; if the data isn't successfully recorded, the voter receives an error message indicating so. This protocol also guards against hardware failure.

The software used in the polling place is loaded from CD-ROMs containing audited program code that is made available for public inspection.

Polling place servers are physically locked away and constantly monitored by electoral officials.

Voting data is written to write-once CD-ROMs at the end of each day's polling, with the data encrypted and identified by a "hash" number that's derived from the content. The encrypted data can't be altered after the event without detection.

The use of data encryption means that a greater level of security is applied to electronic votes than to paper ballots.

The number of electronic votes counted is compared to the number of electronic votes issued at each polling place to verify that the correct number of votes has been counted.

Among voters, the system proved increasingly popular. The 28,100 votes recorded by computer in 2004 represented a 70 percent increase over the 2001 e-vote total of 16,500. Only 10 voters registered official complaints about the system. The commission recommended using the system in the 2008 elections.
Back in the USA: Laissez faire

While Europe and Australia move steadily forward to endorse standards and achieve e-voting transparency, voters' rights activists say US elections officials continue to display a mixture of arrogance and ignorance in setting up e-voting systems. Many examples have recently come to light.

For instance, late in 2005, the Alaska Democratic Party compiled some evidence that electronic databases manufactured by Diebold, the state's e-voting vendor, might contain errors. When they asked for the complete electronic databases of the 2004 election, state elections officials told them the file formats in which the information resided were proprietary. In effect, the data within the files was public information, but the specific formats in which the data resided were the property of Diebold and therefore not accessible to the public. After local media and voting transparency activists publicized that stance in early February, the state officials backed down somewhat and agreed to release the data but only in consultation with Diebold who might be allowed to manipulate data to protect proprietary information. But in late February, the state reversed itself once again (http://www.bradblog.com/archives/00002467.htm), and told the Democrats that the state's chief security officer, Darrell Davis, had decided releasing the information in the database "would be providing an outside entity the ability to modify the structure using commonly available tools like Microsoft Access."

In January, Connecticut's Secretary of State, Susan Bysiewicz, abrogated a contract with the state's chosen vendor, Danaher Corp., claiming the company had misled the state about the federal certification status of its DRE (direct recording electronic) voting machines. The state must begin its vendor search process again. Voting technology watchdog group VoteTrust USA pointed out that independent verification of certification is available through the National Association of State Election Directors. This means Connecticut officials could easily have avoided a last-minute crisis by improving its due diligence. Connecticut officials had no comment.


Johns Hopkins University professor Avi Rubin, one of the nation's foremost experts on the e-voting climate in the US, says several factors have contributed to the widespread confusion. First, he says, "the "Election Assistance Commission (http://www.eac.gov)
took a while to come out with guidelines and they're not actually providing concrete guidance. They're hemming and hawing, saying 'if you use paper here are some guidelines, if you don't here are some guidelines,' but they don't actually address the security concerns." This keeps vendors from complete certainty about what to build and makes government officials afraid of investing money in systems that that might not be qualified.

"So there's a huge sense of uncertainty about what equipment is OK to use," says Rubin. "The other factor is you have such a disparity in the opinions of election officials. There's a strong split between those who back paper ballots and DRE proponents. These arguments continue in legislatures and among election officials and it's creating a bit of a stalemate in some places."

VoteTrust's policy director, Warren Stewart, says that HAVA precipitated a land-rush mentality. Poorly defined public interest requirements appeared suddenly amid existing technology with known shortcomings. "It's not a very profitable business," Stewart says of e-voting. "You sell a bunch of machines to a county and then—theoretically, anyway—you don't have a sale for 15 years." The 2000 presidential election changed the scene. When Congress passed HAVA to address that problem, Stewart says it was "the first time ever the federal government had provided any money for election administration. So there's US$4 billion out there, this fantastic windfall, but everybody knew it was a once-in-a-lifetime opportunity and that began a feeding frenzy. There was zero incentive to produce a better machine, but a ton of incentive to sell the inadequate machines they had."

**Conclusion**

In the short term, both Rubin and Stewart are among those who advocate the paper ballot backup. Rubin is heartened by the increasing number of states writing paper backup into their new voting laws. For people who are alarmed by voting systems that run on private and proprietary software, the paper backup might supply a degree of transparency. However, OASIS 's Borras suggests a different approach to the problem.

"Within EML, we have not attempted in any way to solve those basic problems," he says. "What we've tried to build into EML is sufficient checks and balances so that your security regime, whatever that might be—and it will vary from country to country—can operate and see what's going on. This wish that if you get into e-voting, you want a printout—it can be done, but it seems to be a waste of the whole principle."
Related Links

- DS Online's Security Community, cms:/dsonline/topics/security/index.xml

- RIES: Internet Voting in Action", http://doi.ieeecomputersociety.org/10.1109/COMPSAC.2005.132

- "Discursive e-Democracy Support", http://doi.ieeecomputersociety.org/10.1109/HICSS.2006.125


Cite this article: Greg Goth, "Cradle of Liberty Lags on E-Voting," IEEE Distributed Systems Online, vol. 7, no. 4, 2006, art. no. 0604-o4004.