The Bell™

Privacy, Security and Technology in Internet Voting

DECEMBER 2000 | Published Online Monthly | Vol. 1 No. 8

www.thebell.net | ISSN 1530-048X

Mission bells were used in colonial California for telling time, announcing events, and for passing on news from one city to another. Our symbol is the classic outline of a mission bell because THE BELL newsletter serves similar purposes.

Web Page

Visit The Bell's web page at http://www.thebell.net – more information, more up-to-date.

Call for Papers

Join the dialogue and submit your paper to THE BELL. See page 2. All papers are peer–reviewed. Submissions accepted at any time.

Free Subscription

THE BELL is FREE of charge for Internet distribution in PDF format, and is also available in hard copy. For information, see the back cover.

Read Also...

Election Technology Expo in Sacramento
January 16, 2001
see p. 2

Nichols Research Stops Certifying Voting System Software

Thirty-two U.S. States have relied on Nichols Research for software certification of election systems. But as of one month ago, the public sector business unit of Nichols Research was disbanded because it was not profitable. There was no tapering off period even though Nichols was the only software testing facility. What this means is that at a time when there is a clear need for certifying new voting system software, there is no one to do the job.

by Eva Waskell, p. 3

Rethinking Political Geography

When fully employed, the Internet will call into question two fundamental principles of American governance: the geographical basis of representation, and the need for representation per se.

by David M. Mason, p. 5

Fail-Safe Voter Privacy

What happens if some unqualified voters were wrongly allowed to vote in a tight election and there was a court order to seek out and disqualify their votes under best efforts?

by Ed Gerck, p. 6

A New Dimension in Democracy

In Plato's dialog "The State," Socrates debates with Pericles whether it is the experts or the people who should govern society. Can Internet voting offer a solution to this classical dilemma?

by Mikael Nordfors, p. 9

U.S. Election Administration

In the current system, elections for public officials in the U.S., including Federal offices, are undertaken by the States, which then delegate it to the counties.

by Roy G. Saltman, p. 11

THE BELL™ Newsletter
ISSN 1530-048X

Editor: Eva Waskell
editor@thebell.net

Website: www.thebell.net

Address: 1001 D Street, Suite 202, San Rafael, CA 94901-2800
Phone: (415) 482-9300
Fax: (415) 482-9400

From the Editor

Dear Reader:

The events in Florida have thrust the entire system of election administration in the U.S. under the public microscope. Federal, state and local governments are taking a fresh look at the voting process, and are considering proposals to fund upgrading the technologies now in use. Election reform is on the front burner across the nation and California is leading the way:

(1) Secretary of State Bill Jones has issued a 10-Point Election Reform Plan, which includes an Election Technology Expo in Sacramento to be held on January 16, 2001. The Expo was designed to bring together under one roof a display and demonstration of current and potential technology that can enhance and improve the election process.

(2) Legislative hearings to discuss California's voting systems and procedures will be held on January 16-17, 2001. The hearings will be held by Assembly Member John Longville, the new Chair of the Assembly Elections and Reapportionment Committee. The Election Technology Expo will coincide with the hearings.

(3) On December 4, Kevin Shelly, the Majority Leader of the California Assembly, held a press conference in which he introduced The Online Voting and Modernization Act, AB55. In attendance were, among others, Alfie Charles from the secretary of state's office, and myself. AB55 supports the reduction or elimination of punch card ballots, greater access and accuracy to the electoral process, and the willingness and ability of the county to provide online voting.

The national momentum for examining voting systems and creating change is unprecedented. This reform should take a critical look at current voting standards and their certification procedures which have, among other flaws, supported punch card systems in spite of their clear failures and shifted voting system certification into a single point of failure – as I report in this issue, p. 3.

But unless reform includes open peer review, open source code, strict standards and competing certification services, we will not solve the core issues that have created such a foul sky over U.S. elections. Perhaps, "So foul a sky clears not without a storm." The question is whether one storm in Florida is enough.

Eva Waskell
Editor

Nichols Research Stops Certifying Voting System Software

by Eva Waskell[*]

This article continues the discussion on certification and purchase of election equipment for public voting systems. On p. 5 of the November 2000 issue, Vol.1. No. 7, The Bell declared that "Nichols Research does the software evaluation" of voting systems for thirty-two States in the U.S. This is, however, no longer true. On November 16, 1999, Nichols Research Corporation announced its merger with Computer Sciences Corporation under the joint name CSC. In November 2000, the public sector business unit of Nichols Research was disbanded because it was not profitable. What this means is that at a time when there is a clear need for certifying new voting system software, there is no one to do the job.

Introduction

The decentralization of the certification and purchase of election equipment in the U.S. is an outgrowth of the decentralization of election administration as a whole.

The origins of this process and the role of ITAs (Independent Testing Authorities) were discussed in *The Bell, Vol. 1, No. 7, 2000, p. 7.*

For the past several years, Nichols Research Corporation in Huntsville, Alabama has functioned as the one and only ITA to certify voting system software for the National Association of State Election Directors (NASED).

In its role as an ITA, Nichols had been testing voting system software for compliance with the 1990 FEC voluntary voting systems standards and sending its recommendations and reports to the Houston-based Election Center and any state election official who requested a copy of a report. Thirty-two states relied on Nichols Research software certification for election systems.

On November 16, 1999, Nichols Research Corporation announced its merger with Computer Sciences Corporation (NYSE: CSC) under the joint name CSC [http://www.csc.com/about/news_stories/19991116_a.html]. In November 2000, the public sector business unit of Nichols Research was disbanded because it was not profitable. There was no tapering off period and no public announcement to the election community.

Today, the situation remains the same, as James Knode, a spokesperson for Computer Sciences Corporation stated on December 14th, 2000, for The Bell: *"As a result of this decision, Nichols is no longer accepting applications for the testing of voting system software. They will complete the contracts they've already signed and finish testing the products already in the queue. But Nichols is not accepting any new contracts in this area."*

What this means is that at a time when there is a clear need for certifying new voting system software, there is no one to do the job – and yet few people know about it.

Election officials in California, Utah, Washington and West Virginia contacted by The Bell had no information that the only ITA that certifies voting system software in the U.S. had stopped working on certification since November.

This information prompted a series of phone interviews for confirmations with the main players involved (CSC, Nichols, NASED, Election Center) in order to help understand the efforts undertaken by those involved with the ITA system. This article presents an overview of the findings as well as some suggestions for future action.

1. Findings

There are three essential elements to the certification process. Like the three legs of a tripod, all three are necessary to maintain stability: 1. the FEC standards; 2. hardware certification (Wyle Labs); and 3. software certification (Nichols Research). Now that one leg has disappeared, the certification system becomes unstable.

Doug Lewis, the head of The Election Center and directly involved in managing reports from the ITAs, is aware of the need to find another ITA. *"I've talked with other testing organizations to see if they'd be interested in doing the software testing for voting systems. I've also asked Wyle Labs if they would like to resume the software testing they once did for NASED. But at this point it's premature to say anything more specific about who is interested. By the time of the NASED winter meeting in Washington, D.C. in early February, I hope the situation is resolved."*

Thomas R. Wilkey, the executive director of the New York State Board of Elections and chair of the NASED Voting Systems/ITA Committee, had this to say about the closing down of software certification at Nichols: *"As of December 15*

we've not yet had a face to face conversation with Nichols Research. But my present feeling is that we're hopeful that they'll be able to make suggestions for someone else who has the same level of expertise of testing that they have, and also has all of their experience with elections. We'll also be looking at solutions and recommendations and where do we go from here."

The NASED winter meeting mentioned by Doug Lewis will be held at the Capitol Hilton in Washington, D.C. on February 2-4, 2001. Questions related to the ITAs are sure to be on the agenda.

Regarding the current projects already in the pipeline at Nichols, CSC informed The Bell that by the end of March 2001, all such projects are likely to be completed. But no other project will be accepted, even though there was no tapering off period and there is no other ITA to take over Nichols' job of certifying U.S. voting system software.

This creates another problem. Assuming another ITA will be functioning as early as one month after the NASED meeting, the earliest an application for testing would be accepted under new procedures at the new ITA might be April, meaning that July 2001 is the earliest date by when any new voting system could reasonably expect to be certified. Meanwhile, only older voting systems can be sold in the U.S., without implementing any of the lessons learned in Florida – unless each State takes action and provides parallel paths for certification.

To make matters worse, there will be a backlog of applications ready to swamp the new ITA and to further stretch the average time for certification to many months, creating a further barrier for new voting systems in the U.S. and favoring older, pre-Florida systems.

2. What's Next?

State election officials may thus need to act quickly to fill the software certification void left by Nichols Research.

New software systems cannot be certified. Only pre-Florida voting system software may be sold, perhaps for one entire year. Innovation is blocked. This is how new systems can be stopped, by inaction.

But after the events in Florida, the voting system market has suddenly become a dynamic place and the certification system needs to keep pace with the changes being demanded by society.

However, the certification process must not be rushed to accommodate new products. If thorough testing and evaluation need to take more time with more complex voting systems, so be it. This is not the time to cut corners on the certification of voting systems, even after lost time.

It might be useful to consider the choices before state election officials.

1- State election officials need to carefully consider what the next steps might be. Election reform is on the front burner. Should state election officials consider a mandatory re-certification of all systems purchased after the experience in Florida?

2- The current software certification system has a single point of failure. There is only one organization in the whole country that was designated by NASED to be an ITA for software certification. When this one point fails, as it has now, the software certification system grinds to a halt.

3. The same may happen to hardware certification since there is also only one organization in the whole country that was designated by NASED to be an ITA for hardware certification.

4- There needs to be more support for and resources devoted to establishing additional software and hardware ITAs. New companies and organizations need to be found which can conduct rigorous testing *and* also understand elections. Competing certification services need to be encouraged, not dismissed as "loss of control." The Internet Voting Technology Alliance (IVTA) could help in the area of Internet voting, for example.

5- Since the states hold the liability and handle the risk of certifying voting systems, the states should be making the decisions about whether or not to rely on more than one ITA, what ITAs to rely on, and whether mandatory re-certification is enough or if new standards need to be established. ITAs are beneficial also in reducing liability for the states, while increasing reliability.

One of the sad ironies of the lengthy 2000 election is that it occurred in Florida, the state with the most stringent certification standards. And the 1990 FEC standards accepted the continued use of punch card systems. Clearly, the certification system for voting systems needs an upgrade. Let's turn this continuing election crisis into an opportunity to reform the way in which elections are administered, to reduce the single points of failure. Some people might still see having one ITA as beneficial, as a single point of control. But we need to realize that we cannot put all eggs in one basket. We should not allow one change to de-stabilize the whole system.

This is, perhaps, another indication that we need to begin a public dialogue in public places about what works and what doesn't.

Eva Waskell has been involved with the U.S. election system and computerized elections since 1985. She has a background in software programming. Her research regarding election-related lawsuits became the primary source material for a July 1985 New York Times article on the vulnerability of computerized voting systems. She is the Communications Director of Safevote, editor of The Bell newsletter and a member of the Advisory Board of the Internet Voting Technology Alliance (IVTA). She can be reached at ewaskell@safevote.com

Rethinking Political Geography

by David M. Mason[*]

When fully employed, the Internet will call into question two fundamental principles of American governance: the geographical basis of representation, and the need for representation per se. The tasks of political scientists may be more difficult than those of engineers in this process.

Introduction

I view the casting of ballots over the Internet as a "paving the cow-path" application: using a revolutionary new technology to improve a mechanism premised on an outdated technology. When fully employed, the Internet will call into question two fundamental principles of American governance: the geographical basis of representation, and the need for representation per se.

1. Discussion

British and American democracies rely almost exclusively on geographical groupings as the basis of representation; there is no proportional representation and multi-member districts are rare. This was a necessity given transportation and communication technologies that existed when our country was founded. But geographical groupings are no longer essential to representation, so we should consider what alternative representational modes are possible. And we should also consider their likely effects.

Our representational system has been a major force in the melting pot, making Americans feel like Americans first and something else second. The American system has also largely prevented the formation of ethnic, religious or class-based political parties. What political groupings are most likely to emerge under non-geographical representational forms? How would these new groupings change political outcomes?

Geography (state, local) also forms the basis for the application of many laws. There are exceptions, however, such as securities laws which apply to a particular practice and profession. Further, the Securities and Exchange Commission (SEC) has delegated significant rule-making and adjudicatory functions to voluntary groups such as the Municipal Securities Rulemaking Board, the National Association of Securities Dealers and the Exchanges. Could this model of special-purpose regulation (with representation through voluntary organizations) be more widely applicable in an Internet-enabled democracy? The home schooling community, of which I am a member, is highly resistant to all forms of regulation and has difficulty reaching consensus. However, some voluntary certification group(s) might well be preferable to existing systems under which home schoolers are regulated by local school boards whose officials neither sympathize with nor even understand what we are doing.

As to representation per se, its principal values are in refining and tempering popular opinion and in adding temporal elements to decision making. Between initiative and referendum, I'm much more favorable to referenda in which alternatives are considered and shaped by (presumably more expert) representatives with a final decision reserved for voters than to initiatives in which the most intensely interested parties set the agenda for all voters. With the Internet, referenda need not be restricted to a single election day and to a limited number that voters can address in a single balloting session. Several states now require voter approval through referendum for tax increases. Could this principle be more widely (if not universally) applicable using Internet technology?

2. Comments

I see Internet-democracy discussions as far too focused on technology and its needs (which I am confident will be solved sooner or later). The more difficult and significant questions are about how human beings use technology to restructure their government and society. I am encouraged that The Bell refers to alternate models of governance, decision-making and representation in its mission statement. These models should be grounded as soundly in concepts about the purpose of representation and the role of political geography as they are in questions of encryption or server capacity. The tasks of political scientists may be more difficult than those of engineers in this process.

David M. Mason is a former Congressional staffer, campaign manager, candidate for state office, and think tank executive. He is currently Vice Chairman of the Federal Election Commission. He can be reached at dmason@fec.gov

Fail-Safe Voter Privacy

by Ed Gerck[*]

Internet voting must allow voters to preserve their privacy, even under court order, if everyone colludes and everything fails. This requirement is closely linked to open source and open peer review of the voting protocol involved, otherwise assurances become a matter of blind trust.

Introduction

Fail-safe voter privacy is an important property of any public voting system. It means that voter privacy should not be compromised in any instance – even if everything fails, everyone colludes and there is a court order to open all ballots and all records. Voter privacy must be absolute.

The assurances of voter privacy afforded by a voting system, even under a court order that mandates otherwise, is a question of more than theoretical interest – considering all the litigation procedures used in Florida's drawn-out 2000 Presidential election.

To help investigate the issue of fail-safe voter privacy, this article considers the question of whether and to what extent a specific Internet voting system could be broken under court order – for example, if some unqualified voters were wrongly allowed to vote in a tight election using Safevote technology and there was a court order to seek out and disqualify their votes under best efforts.

Of course, the answer depends both on the technology being used by Safevote and the protocol that implements it. Thus, the analysis shall provide an opportunity to clarify both aspects as well. *This analysis applies to precinct-based Internet voting but can also be used for remote Internet voting.*

Safevote's voting systems are based on a peer three-party and n-party technology called Multi-Party™. The 8-point design strategy behind the Multi-Party technology is: (1) use a few proven and simple components; (2) allow a large number of different connections of such components; (3) define trusted introducers and trusted witnesses based on qualified reliance; (4) make every connection have a trusted introducer and a trusted witness; (5) define a multi-risk model where risk can be not only "average loss" but also "probability of loss" and/or "value at stake"; (6) favor multiple, independent communication channels over one "strong" channel; (7) define clear evaluation criteria such as voter privacy, vote secrecy, and election integrity; and (8) put voter privacy as the first criterium.

Full disclosure and open peer review are mechanisms that provide for independent oversight and redundancy, which are two main principles behind the 8-point design strategy used by Safevote. Under these two principles and for any election legal requirement, if a flaw or weak point is found in a protocol implementing the technology, the protocol can be corrected to account for the potential problem. Thus, the protocol "learns" as it is used.

However, the truism that a system can only be as good as the way it is implemented is also valid here. All elections are organized differently, and one may have to customize Safevote's system for each case – including input from the election officials. This corresponds to another main principle behind the 8-point design strategy used by Safevote, which is to account for diversity – not iron it out.

Another main principle is that election protocols need to be "expressive enough" to cope with many potential situations. Safevote's protocols implement a multi-party computation model including a trust model that provides backward-looking and forward-looking assurances at every point, a choice for open or closed loops of trust whenever an authorization is required, and a multi-risk decision model. The author frequently makes the point that any election protocol one could implement with human agents should also be expressible with this approach insofar as we humans tend to use the "computation," "trust" and "risk" primitives in the same way.

Of course, the protocols can also be used in a "bad" or weak design, in the same way that we humans can define and use faulty trust protocols. This fact further stresses the need for full disclosure, so that errors can be eventually "weeded out" of the system and not remain hidden.

"Security is only as strong as its weakest link" is the current paradigm. The paradigm shift implied above is that security can be made as strong as we desire. This is really not so new. Hindus in the Mogul period some 500 years ago knew and used it [The Bell, Vol. 1, No. 6, p. 10].

1. Intellectual Property Issues

This paper is part of a continuing effort to provide technical information for peer review. The disclosure in this paper is

not a license, but a free license may be granted for non-commercial use, as well as licenses for commercial use. This section intends to provide guidelines for usage of this information – since open source and open peer review are two important components of the fail-safe privacy assurances to be discussed.

Intellectual property protection usually relies on copyright protection for the software and patent protection for the methods behind the software, as well as for the system built with the software. In Safevote's case, it is the patent protection which allows the software to be open, with adequate protection for investors who might otherwise desire to block disclosure in defending their own interests. This is a quite common scenario in voting, where there is no open source code and no open peer review for any voting system in use today for U.S. public elections.

On the issue of patents in regard to this information, the policy followed by Safevote is in support of FREE patents where, as used in Free Software, FREE is not to be understood as "free" in free beer but as in free speech. In other words, "free" means that if I want to say anything in private, I should have the right to do so at any time. However, if I want to do so in order to earn money, such commercial right needs to respect the commercial rights of others.

Safevote's FREE patent policy thus includes a public license drafted so that anyone can use the patents and even the source code for private purposes, in non-commercial use. Commercial use requires a license, with fees according to each case. This policy is also a test in order to see whether it is adequate to protect all interests involved, including the interests of the individual. It may be changed at any time.

But how are public elections defined? Are they commercial or non-commercial? In fact, public elections can be either.

For example, if a county decides to run an election without any warranty from Safevote and without any work to be done by Safevote, and without charging any costs to anyone or paying a systems integrator to do the job, or receiving any money for it –so that all is volunteer unpaid work – then this is a non-commercial public election and Safevote would not charge for use of its patented technology.

However, if a county pays a vendor so that the vendor can run or assist the elections using Safevote's technology, then this is not a non-commercial public election. The vendor is earning money from the use of the patented technology (i.e., without the patented technology, the system would not work and the vendor would not be able to fulfill the contract). This would require a commercial license.

A further objective of this FREE patent policy is to contribute toward a reasonable patent policy to be used in Internet voting in general, as a win-win compromise in a balance of rights. That is why the author believes in the educational role of public discussions on issues of intellectual property protection, not only on technical issues. The IVTA offers an open forum where we can ponder the subjects and listen to a variety of opinions. The Bell also serves this purpose and has been available to expand upon such discussion threads – for example, with the Open Source and FREE software discussion in the September issue.

2. Technology

In a Safevote system, three qualities are essential:

voter privacy	the inability to know who the voter is
vote secrecy	the inability to know what the vote is
election integrity	the inability to influence the outcome of an election except by properly voting

These qualities are supported by the Multi-Party technology used by Safevote. This technology is based on the U.S. Patents 60/225996, 60/226042, 60/226158, 60/231600, 60/231681 and others (Patent Pending), and includes methods for: precinct-based and remote voting (e.g. voting from home); compact and mnemonic voter credentials; digital vote certificates (DVCs); electronic ballots; high entropy ballot encoding and virus neutralization; systems for detection and prevention of Distributed Denial of Service attacks; voter interfaces; and distributed firewall systems.

Safevote's software and protocols implement the Multi-Party technology in modules that can be applied as standard components to new systems and also to legacy systems. The technology allows interoperation with PKI technology (e.g., X.509, PKIX, PGP, SSL, S/MIME) as well as non-PKI technology (e.g., proprietary voting systems, direct recording electronic voting machines –also called DREs).

The Multi-Party technology defines Digital Vote Certificates™ (*DVC*™) and Electronic Ballots™ comprising an end-to-end secure system that provides for fail-safe voter privacy, cryptographically strong vote secrecy, and verifiable election integrity. When the election is over, the ballots are tallied without being decrypted (by means of homomorphic encryption techniques). This, together with the DVC mechanism, emulates a true ballot box: There is no link between voters and votes, even under court order, which could not be guaranteed using just homomorphic encryption.

DVC:
A DVC is a cryptographically signed, anonymous, random, password protected, unique, highly compact, human readable and mnemonic digital certificate – for example, **6TRA9K**. The DVC is at the same time a device, a name and a number. A DVC simultaneously encrypts and certifies data. DVCs are not authenticated by how they look, as passwords are, but by how they work. In the preferred encoding for DVCs, the confusing characters are eliminated

(for example, the letter "O" and the numeral "0") while only upper-case letters and the numbers from 1 to 9 are used, with 32 possible choices per character and a total of six characters (a short DVC increases the DVC's mnemonic potential to a voter and makes data entry easier). This preferred encoding corresponds to $32^6 = 2^{30} = 1{,}073{,}741{,}824$ DVCs –i.e., over one billion different DVC combinations.

Each DVC also contains –in spite of a very short size of only 30 bits – independent, multiple secure communication channels such as the voter's password, the ballot style to be used by the voter, and an internal secret. These channels extend the number of voters that could receive uniquely verifiable DVC/password combinations from over one billion to more than one quadrillion (1,000,000,000,000,000), a number that is more than 165,000 times the world's population.

DVCs and their passwords are unknown at the very servers that will authenticate the DVCs. There is no voter authentication file to protect at the servers. Yet, DVCs can uniquely authenticate not only each voter to a server but also the ballot style designated to each voter by the registration service, without identifying the voter and without requiring the registration service to be online.

DVCs provide for strong authentication and non-repudiation proofs within a closed-loop distributed control system. This enables an end-to-end security design that begins with voter registration and continues to ballot issuance, voting and tallying, which tallying can then be compared with earlier tamperproof entries in voter registration tables. Because they are so compact and human-friendly, DVCs can be simply printed or written down; they do not need to be downloaded, stored on a floppy-disk or in a computer, and can be kept off-line until used. The voter does not need to trust additional systems and does not have to download plug-ins, Java applets or use Javascript.

Standard browsers compatible with Netscape 3.0 and above can be used with DVCs. DVCs use a "thin client" model –the main part of the work is performed at the servers. Industry-standard SSL is used to authenticate the server to the client, but other methods can also be employed as desired. Further, DVCs can be used entirely off-line by means of additional personal and trusted hardware such as a smart-card.

Electronic Ballot:
A secure, data-independent, representation-independent and language-independent ballot, which definition can be applied as data and/or metadata and/or a distributed control structure to any voting system, and especially to Internet voting. Electronic Ballots allow for write-in votes. The Electronic Ballot further provides for dynamically generating diverse styles and formats of ballots to voters, as the voters are previously authenticated to use, and including different languages and font sizes as may be required online by the voter. However, all of these formats are based on a single Electronic Ballot that can be approved and certified once. An aspect of Electronic Ballots can also accommodate minority voters and satisfy the requirements of the elderly and the U.S. Americans with Disabilities Act, which cannot be entirely foreseen during voter registration.

Other aspects of Electronic Ballots enable:

1. An automated communication system which coordinates the secure transfer of data and/or metadata and/or a distributed control structure between databases, servers and clients in order to define, control and process ballots.
2. The inclusion of other control structures within the automated communications system.
3. The use of multiple control structures and independent channels of information, which can considerably increase the reliability and trustworthiness of network voting systems, as well as auditing, vote recounting and verifiability of the election.
4. The use of a high-entropy encoding system for dynamic allocation of candidate names, issue descriptions or any other information to be tallied, in respect to accumulator names and constants used in a program that accumulates the respective counts, which can be made unpredictable for every voter within a given modulus.
5. The use of auditing and vote recounting (including universal verifiability by voters and third-parties, and real-time auditing), all particularly difficult to define in network voting as known in the art, by means of various authentication and non-repudiation proofs that are stored and can be recalled even in real-time during the election by various parties without compromising election integrity, vote secrecy or voter privacy.

Verifiability:
The DVC and Electronic Ballot components of the Multi-Party technology allow detailed real-time auditing and post-election auditing by election officials, as well as allowing each voter to verify on the Internet whether their vote was received at the servers without compromising voter privacy, vote secrecy or election integrity. Verifiability, including voter verifiability, can considerably reduce the probability of undetected fraud.

For example, if 10,000 voters cast their ballots in an election where the probability of frauds, attacks or faults leading to the loss of any voted ballot is at most 5% and if only 300 voters do verify whether their respective ballots were received, then the probability that the loss of at least one ballot will not be detected (and thus the fraud, attack or fault will not be discovered) is less than 0.1%. This exemplifies the use of a small number of closed loops (300) in order to leverage security by a factor of 50x for 10,000 voters (reducing undetected frauds, attacks and faults from at most 5% to at most 0.1%).

Thus, verifiability is important to foster public trust in Internet voting by allowing one to close the loop of trust – i.e., trust, but verify.

(continued on p. 12)

A New Dimension in Democracy and Decision-Making

by Mikael Nordfors[*]

In Plato's dialog "The State," Socrates debates with Pericles whether it is the experts or the people who should govern society. Can Internet voting offer a solution to this classical dilemma?

Introduction

Perhaps the most difficult problem of mankind down through the ages has been how to coordinate our common affairs in an efficient, competent, creative and democratic way. Many people, including the Nobel Prize winner in economics Dr. Amartya Sen, say that our inability to solve this problem is the ultimate cause of starvation, war, economic problems and environmental destruction.

One of the main problems regarding the coordination of our common affairs is presented in Plato's dialog "The State," where Socrates debates with Pericles whether it is the experts or the people who should govern society. Socrates stated, "You don't let a mob decide how to treat your stomach ailment, you go to a good doctor." Pericles, the father of Greek democracy, maintained on the other hand that ordinary citizens were fully qualified to govern themselves.

In reality, it has most often been neither the experts nor the people who have governed, but rather power-hungry people. History is replete with many examples of this tendency.

1. The Three Dimensions of Decision-Making

The three dimensions of decision-making are:

Expertise
Values
Purpose

In order to make a satisfactory group decision, it is important that the group can arrive at a decision that integrates expertise into the group's common values and purpose.

If only the experts decide, they can easily forget about the group's common goals and values, thus separating themselves from the others in order to create a selfish elite. This is the problem Pericles was stressing.

On the other hand, group decisions without access to expertise and knowledge can also be disastrous. You cannot vote away natural laws and scientific facts. This is the part that Socrates was stressing.

To solve this dilemma, Vivarto has developed a voting system that uses the Internet to offer new and unique possibilities, creating a system which combines the best from both Socrates' and Pericles' views and supports decision-making where expertise is used in harmony with a group's shared values and purposes.

2. Description

In Vivarto's voting system, one begins by choosing a representative (an expert), who can be, for example, a board member, an adviser, or even an organization or political party – all depending upon the context in which the voting system is applied. The representative may also be called a "proxy" (which term must not to be confused with "proxy" in "proxy voting" as used in private sector voting, and which refers to the document used by the voter himself to vote). Then, on those occasions when one does not have the time, energy or knowledge to participate actively, the representative votes on one's behalf. But, if one should decide to vote directly, in Vivarto's system one's own vote always takes precedence over that of the representative.

The system is dynamic and very flexible in that one may change one's proxy at will and may have different proxies for different subject fields. It is also possible for proxies to use other proxies. The system is called VPV (Vivarto Proxy Voting).

3. Purpose

The purpose of the VPV is to give the voter maximum control over his vote. But how can this be true when the voter de facto gives his vote away to a proxy? Let us consider three different scenarios for all possible ballots:

1. A conventional ballot
In this case, an absent voter cannot vote but effectively gives his vote to the majority of participating voters.

2. A ballot with conventional proxy voting
Here the voter is represented by a proxy, either as a person or as a document containing the voter's choices. The advantage of this arrangement compared to a conventional ballot is that the voter can be always represented when he does not vote himself.

3. A ballot with VPV
In this case, the voter gives his vote to a proxy, but can recall it any time by voting directly – which is enforced by software. The voter thus has more control than in the two previous scenarios because:

1. He can always vote directly.
2. When he does not vote, he knows exactly who is going to vote for him.

4. Analogy with Human Nervous System Functions

Being a medical doctor, one of the sources of inspiration when inventing VPV was the human nervous system. If we had to think consciously about everything the brain does on an unconscious level, we could not exist. There is a disease called Undine's curse. People with this disease loose the function of automatic breathing. This means they have to put themselves in a respirator every time they go asleep. Imagine having to take care of all other automatic bodily functions and habits like regulating blood pressure, digesting food, thinking about how to walk, etc. Life would be impossible. Something similar would be the case if everyone would have to be part of all decisions made in society. We would not have time to make food, take care of our children and sleep. Delegation is an important principle for our brain functions, as well as for human group survival.

On the other hand, we must also always have the possibility to learn new things and come up with new, original responses to new problems. This is what makes life truly alive. When everything in our lives is delegated, the ability to learn and adapt gets lost, greatly reducing the chances of survival and success. Therefore, it is important to always have the possibility of conscious acts where you can process and interact with new and urgent information.

Casting a ballot with representative voting corresponds to the automatic body functions and our habits, while direct voting corresponds to our conscious choices and our ability to learn new things and adapt to new circumstances. With VPV you have secure delegated decision-making, and at the same time you always have the ability for direct and conscious participation. Neither pure delegation nor pure participation is sufficient by itself.

5. Other Advantages of VPV

5.1. A safeguard against extremist groups. If the participation in an election is low, there is a risk that a well-disciplined group with extremist viewpoints will gain unfair influence. The VPV solves this problem.

5.2. Quality assurance in problem solving and deliberation. VPV is valuable in a special kind of debate and deliberation process called the Vivarto Idea Greenhouse, where participants can send in ideas and suggestions that can be rated by the other group members resulting in an "idea top chart" which can be a source of inspiration for decision makers and politicians. It has been found that the intensity of a debate often is at its peak in the beginning, while the quality of the comments increases with time. This produces a tendency for high-quality contributions submitted during the end of the discussion to get low scores because of lack of participation. This problem is circumvented by use of the VPV system.

5.3. "Spiritual," instead of geographic proxies. Instead of having to choose between two different "poisons" in your local county or district, you can have a much larger selection of proxies to choose from, regardless of your geographical location. This gives you a greater chance of finding a proxy or an expert who holds views similar to your own, and you're not forced to choose between two "poisons."

5.4. New types of representatives can have access to decision-making. The VPV system enables a broader scope of people to participate as representatives in decision-making. For example, people who are unwilling to lie in public or those who feel uncomfortable in speaking before the public can express their opinions and have a voice in decisions that effect their lives.

6. Practical Applications

The VPV system has been in use for some months on a website for a local politician in a suburb near Stockholm, Sweden. It is also being evaluated in classes in the multimedia department at Stockholm University. It is being considered for installation at many major political and other organization's sites in Sweden, Great Britain and the U.S. For more information, see www.netconferenceplus.com

Vivarto Technologies has also recently begun to co-operate with Safevote, Inc. in order to incorporate Safevote's security features into Vivarto's VPV system.

Mikael Nordfors is trained as a medical doctor, but has also been interested in politics for many years. He introduced St. John's Wort as an antidepressant in the US and Sweden with the book Hypericum & Depression and numerous scientific articles and interviews. From extensive studies in psychiatry, anthropology and politics, Dr. Nordfors has found that the most essential element for the well-being of individuals, families and society as a whole is that people are free from oppression and can stand on their own feet. Vivarto NetConference Plus is designed to make this process toward greater freedom, creativity and participation easier. Dr. Nordfors can be reached at mikael@vivarto.com

U.S. Election Administration

by Roy G. Saltman[*]

In the current system, elections for public officials in the U.S., including Federal offices, are undertaken by the States, which further delegate election administration to the counties.

Elections for public officials in the United States are a function conducted by the States and local governments. Even administration of elections for Federal officials, i.e., for the President and Vice-President (actually for the electors for these offices), and for U.S. Representatives and Senators, is undertaken by the States and local governments. In each State, a chief elections official is responsible for specifying the administrative rules under which elections are carried out, and that official also is generally responsible for certifying the results of contests for State and Federal offices. In many States, the Secretary of State is the chief elections officer, but in other States, the Lieutenant Governor or a State Administrator of Election Laws (or person having a similar title) serves in that capacity.

The Federal Government has specified the age, citizenship, and residence requirements for Federal officeholders and for voting for Federal offices, but has not generally specified the administrative procedures for voting. The Constitution states that "each House (of Congress) shall be the judge of the elections, returns and qualifications of its members," but the State legislatures are to prescribe "the times, places, and manner of holding elections for Senators and Representatives." However, Congress has retained control in that "the Congress may at any time by law make or alter such regulations." Amendments XV, XIX, and XXVI to the Constitution respectively eliminated barriers of race, sex, and age (18 and over) to eligibility for voting. Federal civil rights laws of 1957, 1964, and 1965 further assured against discrimination in the right to vote, as did Amendment XXIV, which barred the use of a poll tax. In addition, a Federal law has required that the records of Federal elections be retained for 22 months following an election.

As the Federal Government has delegated administrative responsibility for Federal elections to the States, the States, similarly, have delegated responsibilities to their local jurisdictions. Many States have retained the authority for selecting the types of voting equipment that may be used within the State, but these States may require that local jurisdictions actually procure the equipment. The States also mandate that state-approved specifications must be met. States also may publish regulations for use in their local jurisdictions for the administration of elections, for either the voter registration or vote-counting functions or both.

In 40 States, election officials in individual counties and county-equivalent jurisdictions are responsible for the nitty-gritty of election administration. These duties include maintaining up-to-date lists of names, addresses, other identifying data and party registration of eligible voters (a Statewide voter registration file is maintained in some States); procuring, maintaining, and testing election equipment, and preparing it for specific elections; assuring that each candidate desiring to be on the ballot has met the eligibility requirements; selecting and staffing voting sites, and assuring that each site is instrumented with equipment properly prepared for the specific ballot to be voted at that site; informing voters (in another language in addition to English if required by law) of the hours, voter-specific locations for voting, and offices and issues for which each voter is eligible to vote; and collecting, counting, and certifying the results of voter choices within the jurisdiction.

In the six New England States, the election administration responsibilities listed above are carried out at the city and town level instead of at the county level, while in Michigan, Wisconsin, and Minnesota, the responsibilities are shared between the county and its townships (Michigan and Minnesota) or between the county and its towns (Wisconsin). Only in Alaska are the administrative responsibilities retained at the State level. When all the local jurisdictions conducting parts of Statewide and Federal contests are enumerated, they amount to over 10,000.

Thus, election administration in the United States is a highly disaggregated process.

Roy G. Saltman, M.S., M.P.A., works as a consultant in computerized voting. He is retired from the U.S. National Institute of Standards and Technology (NIST) and is well-known for his reports and presentations on the integrity of computerized voting. He is a member of the Advisory Board of the Internet Voting Technology Alliance (IVTA). Saltman can be contacted by email at roysalt@aol.com, by phone at (410) 730-4983 or by fax at (410) 997-4355.

Fail-Safe Voter Privacy

(continued from p. 8)

4. Analysis

The question under investigation here deals with breaking voter privacy under court order in Safevote's system. What is possible and what are the limits under the assumptions of a court order and everyone being ordered to collaborate? For the sake of the argument, suppose some unqualified voters were wrongly allowed to vote in a tight election and there was a court order to seek out and disqualify their votes under best efforts.

Clearly, this is a problem with registration issues –not with voting issues. As a practical matter, there might be delays, for example, between various offices in the legal system, and thus the registrar of voters may unwittingly allow a convicted felon to be illegally registered at day D even though the conviction order was issued at day D - d.

First, it is useful to avoid a common confusion with the word "privacy." Oftentimes the mass media and lay usage applies "privacy" to also mean "confidentiality" or "secrecy." Thus, voter privacy needs to be distinguished from "vote secrecy." While both are provided by Safevote's system, "voter privacy" means the inability to link a vote to a voter while "vote secrecy" means the inability to know what a vote is (e.g., to eavesdrop into a communication channel that carries votes, to read stored votes). In Safevote's system, both barriers would have to be broken in the case at hand.

A court order would have thus the effect of making all parties collaborate to break voter privacy and vote secrecy barriers built-in by Safevote. These barriers, however, work under two different principles in Safevote's protocols:

1. A fail-safe principle in the case of voter privacy. Even if everyone colludes, everyone collaborates and everything fails, the voter's identity and address will not be revealed within the available choices, which are usually very large (e.g., a precinct with 1,000 voters).
2. For vote secrecy, the barriers can be made as secure as desired by they are not fail-safe. They are defined by well-known cryptographic and implementation limitations (e.g., key size, disclosure by key holders, number of key holders, password size, protocol flaws, buffer overflow, bugs, virus, etc.).

In other words, irrespective of key sizes, protocol flaws, buffer overflow, bugs, virii, and even collusion and system faults, Safevote's system makes it impossible to precisely pinpoint a voter even when all votes and system messages are known. Nonetheless we must ask, what can be done under court order?

As this analysis will show, what can be done under best efforts and full collaboration by all involved, including asking individuals to waive vote secrecy rights, is to provide a list of votes and possible voters, who must then be interviewed and screened by the court to try to assign each vote to each voter, so that the illegal voter may be found –or not –by a process of elimination.

The analysis will also show that the voter list is irreducible if a random password is used with the DVC. In a worst-case scenario, a voter list with 500 voters might be strongly reduced, but still without compromising voter privacy, if the voter's day and month of birth are used as the password with the DVC.

The fail-safe cases can be summarized as follows:

1. If the DVC password is the voter's date and month of birth and the precinct has enough voters (on average, more than approximately 500), voter privacy cannot be compromised even under court order.

2. If the DVC password is random and the precinct has more than one voter, voter privacy cannot be compromised even under court order.

It is important to note that no activity to break voter's privacy or vote secrecy depends on Safevote's involvement.

The analysis starts with the following example:

There is a court order to verify whether Joe Doe voted at precinct X, and if so, nullify the vote and recount or, at least, verify whether the vote would be relevant to the contested election and provide best efforts to nullify it in this case.

A person (hereafter known as Bob) is tasked by the court to conduct the investigation for precint X, where Joe Doe is registered. Suppose precinct X has the maximum number of registered voters allowed in California, 1000 – the average number of voters being 600. There is an official record to the effect that a DVC (Safevote's Digital Vote Certificate) was issued to Joe Doe. According to the records, it was keyed to Joe's day and month of birth. This corresponds to a worst-case example of a privacy-intrusive password and record-keeping of passwords by the election office (which is not the recommended procedure). However, the value of Joe Doe's DVC is unknown.

Also as a worst-case example, all ballot styles at precinct X are the same and no other precinct in the county uses the same ballot style. For example, the ballot style used in precinct X is 100. This defines the parameter BSI = 100 for Joe Doe.

The log file at the election office for all issued DVCs is obtained by Bob. This may require the use of a physical key Ka, to open a physical lock for a vault where the log files are archived. The log file is encrypted and can only be decrypted by a secret cryptographic key that is divided into a group of three (for example, it could be one or ten) election officials (hereafter, EOs), in chunks Kb1, Kb2 and Kb3, which are all obtained by Bob. Generally, the secret key Kb is a 2048-bit private-key with a well-known secure asymmetric encryption algorithm such as RSA. The decrypted log looks like this:

Event	Date	Time	DVC-khash	BSI
.	.	.	.	
23	8/17/2000	14:00:12	D76BC3A..	67
24	8/17/2000	14:20:44	A310CF5..	100

Bob is interested in all entries with BSI=100, which is the only BSI used at precinct X. Note that this list (for security reasons) still does NOT include the DVC itself but just its keyed hash. In other words, if one *knows* the DVC and a key, one can verify that the DVC is in in the list but one cannot calculate or guess a DVC that is in the list. The hash is protected by a secret cryptographic key that is divided into a group of three (for example, it could be one or ten) EOs, in chunks Kc1, Kc2 and Kc3, which are obtained by Bob. Generally, the secret key Kc is large (128-bit or more), and is used in message authentication with a well-known secure hash algorithm such as SHA-1.

This secret information (physical key Ka, DVC log file and two sets secret keys Kb and Kc) is thus collected by Bob.

Next, Bob obtains the ballot log files for the election machines used at precinct X. This may require the use of a physical key Kd for each election machine. Each ballot log file (i.e., for each election machine) is protected by a secret key Ke (e.g., a 2048-bit private-key) that is divided into a group of three (for example, it could be one or ten) EOs, in chunks Ke1, Ke2 and Ke3, and is indexed by a second DVC keyed hash (e.g., a 128-bit symmetric key) with a secret key Kf that is divided into a group of three (for example, it could be one or ten) EOs, in chunks Kf1, Kf2 and Kf3, which are obtained by Bob. For each ballot log file, each EV (the encrypted canonical vote defined in Safevote's protocol) contains the digital signature of the DVC that was actually used by a voter to cast that EV at the precinct (but does not contain the DVC itself). A ballot log file looks like this:

Event	DVC-khash2	EV
.	.	
111	28BD9A2..	a67Bn2Kj4ev...
112	4CD29F0..	10pYtwMNk87c..

The ballot log file does not include the BSI. For each election machine used in precinct X, Bob uses the corresponding Ke and Kf together with a program that verifies all such EV log entries versus DVC-khash2, which digitally certifies EV. Then, Bob uses the BSI and the DVC-khash obtained earlier, together with DVC-khash2, to calculate the DVC used for each ballot entry, for 1000 (maximum) to 600 (average) entries.

This generates list L1, with the verified DVCs used at precinct X. In the worst case, there will be 1000 entries (the maximum number of voters in that precinct) in L1. Thus, Bob now has the DVCs actually used at the precinct where Joe Doe voted.

Next, with these DVCs as listed in L1 and using the election office DVC log together with secret key sets Kb and Kc, Bob verifies which DVCs match the DVC log file at the election office and have BSI = 100. This is list L2.

The maximum number of matches is 1000 (maximum number of voters); the average number of voters per precinct is 600.

Next, for all such DVCs Bob uses the same program used for voter authentication in the election in order to verify which combination of (DVC, BSI=100) in L2 works with Joe's password of DOB = 1/28. This is list L3.

Since there is an average of 365 days in a year, if all 1000 voters do vote in a precinct, it is expected that there will be an average of 3 and at most 20 entries in L3. All entries for DOB = 1/28 and BSI = 100 will have different DVCs. Thus, L3 has from 3 to 20 entries that could correspond to Joe Doe, with the same DOB and BSI.

If the precinct has an average number of actual voters, i.e. 600, the list L3 will shrink to two or three possibilities. This explains, by counter-example, why a password such as a three-character combination offering 32,000 possibilites would be preferable to day and month of birth with 365 possibilities – in order to protect the voter's privacy in a balance of probabilities.

However, if day, month and year of birth are used as passwords for the DVCs, (a bad case to protect voter privacy), the search ends with just one possibility and Bob is able to readily name the voter and vote to the court.

Let us continue with the example where the password is the day and month of birth, as a worst-case scenario for Joe Doe. Bob collects the certified databases used in the election (for which physical keys Kg may be needed; the certification keys are public). With the DVCs, the BSI = 100, the now known password (the DOB), the encrypted canonical votes EV, the sets of secret keys Kf (one for each election machine in the precinct) and the certified databases, Bob uses an auditing program to reconstruct the voted ballot images for those expected maximum number of 3 to 20 DVCs in L3, recovering from 3 to 20 ballot images. This is list L4.

If all those votes in L4 were such that they are NOT involved in the contested election result, the search ends and Joe Doe did not influence the result.

Otherwise, to narrow down L3, Bob uses the election office's voter database and cross matches everyone who has the same DOB (month/day), BSI and precinct as Joe Doe and notifies them to contact the court – there are perhaps from 3 to 20 persons to notify (the same maximum number as in L3). Bob will then ask each one of these persons to identify their vote in L4 (i.e., how they voted). If all these persons agree to disclose how they voted, this may allow Bob to either identify what is left as being the vote by Joe Doe or, to conclude that Joe Doe's vote was not significant to the contested result.

This example thus highlights some secure aspects of Safevote's fail-safe design principles which absolutely protect voter privacy, even for a very small number of password combinations (365):

1. Even though there was a court order and everyone was ordered to cooperate under best efforts, dozens of election officials had to become involved, voter registration and ballot databases had to be accessed, dozens of physical and cryptographic keys had to be used and possibly voters would also have to be summoned and asked to cooperate.
2. Still, in spite of this concerted effort by everyone involved, there is no guarantee that Joe Doe's voter privacy would be broken, nor how long it might take to break it.

Of course, one needs to know if in a balance of rights whether voter privacy is considered more important than the possibility of correcting registration errors. The use of just day and month of birth as a password (worst case) would still allow a court of law to summon from 3 to 20 individuals in a contested election.

Alternatively, the authentication procedure may not include the date of birth information and might use a password with 32,000 possibilities to protect the DVC, in which case the court would be presented with the full voter list. For remote Internet voting, just the DVC and month/day of birth may thus not be enough and a third identifier (e.g., biometric, password) may be imbedded in the DVC and required from the voter. Or, just the DVC and a biometric key or password may be required –with no date of birth information at all.

When a biometric key is used together with the DVC, the system is set up such that identifying one voter could happen only when all voters (e.g., 600 average) are summoned and their biometric data are matched –in other words, if you have the biometric key you cannot find the voter but if you have the voter you can find the corresponding biometric key. This is called a "one way wall." The strength of this "wall" may be perfect, as well-known from the work of Claude Shannon – even if an attacker has all desired computational resources and unlimited time.

In summary, Safevote's system has no back-door regarding voter privacy. There are no tags in the system that can identify a voter by calculations or by record storage. Even after a complex manual process of elimination involving dozens of secrets and people, the result is a sizable pool of equally probable names.

Ed Gerck has been at the forefront of developments in Internet security, with five recent patents filed on Internet voting. He received his doctorate in physics (Dr.rer.nat.) from the Ludwig-Maximilians-Universitaet and the Max-Planck-Institut fuer Quantenoptik in Munich, Germany in 1983, with maximum thesis grade ("sehr gut"). He has worked in cryptography since 1987. Dr. Gerck is the founder of the Meta-Certificate Group (MCG), chief executive officer and vice-president of technology of Safevote, Inc., and chairman of the board of the Internet Voting Technology Alliance (IVTA) of Washington, D.C. Dr. Gerck can be contacted at egerck@safevote.com

From Our Readers

From Einar Stefferud, Principal, Network Management Associates, Huntington Beach, CA
"Of course, we cannot continue to allow voting systems to be wrong in 120,000 out of 6 million votes, or to cost $3 or even $1 dollar per vote. Voting requirements need to be realistic, strong and practical, and cost us no more than a few cents per vote. I think that the 16 requirements published in The Bell reflect current law and what is needed today from voting systems in the U.S."

From Douglas A. Kellner, Commissioner, Board of Elections in the City of New York
"I am very happy to be on your subscription list for The Bell. I read it religiously and I find it very informative, particularly because you are not afraid to venture into a level of technical detail that I have not seen anywhere else!"

From Bill Huennekens, Elections Program Coordinator, Office of the Secretary of State, Olympia, WA
"I find The Bell very informative."

From Jason Kitcat, Founding Partner, Swing Digital Ltd., United Kingdom
"Direct democracy and other ideas may be coming thanks to electronic voting but we're gonna implement existing democratic systems electronically first. There are dangers with more direct forms of democracy and this delay is a welcome one.

Directly allowing people to make big decisions at first blush seems more democratic but I don't believe is. Firstly, people become apathetic if they get asked to vote too much. Can you really expect people to go to the effort of learning all the issues before voting on every decision? Don't they have lives to lead which is why they entrust representatives?

There is also the risk of emotional votes which are soon regretted. In the UK we often get calls for drastic legislation after tragedies such as a child being abducted and murdered or unnecessary accidents. People get caught up in the moment and don't think through the full (civil liberty, economic, etc.) implications of what they call for. Direct democracy might not leave room for such reflection."

Media Watch & Links

Legislation Would Allow Approval of Online Voting Systems
California could become the first state to allow online voting, under legislation drafted by Assembly Majority Leader Kevin Shelley. "This will bring the election system into the new millennium because it is still stuck somewhere not in the 20th century, but in the 19th century," the San Francisco Democrat said Monday. The first online computers would be placed at polling sites to avoid problems with at-home voting.
http://www.sfgate.com/cgi-bin/article.cgi?file=/news/archive/2000/12/04/state1704EST0173.DTL

Election Day Winner: Online Voting
Voters in six states cast ballots over the Internet, and the procedure won overwhelming endorsements from voters and election officials. Most of the votes were non-binding ballots cast in experiments in Arizona and California. But about 85 were live votes cast by U.S. military personnel in an experiment that could lead to widespread use of the Internet for voting by personnel stationed around the world.
http://www.fcw.com/fcw/articles/2000/1106/web-elect-11-10-00.asp

Digivote
Thanks to the election debacle, voters will soon have a better place to cast their ballots: the Internet. Political and technical experts expect online voting to take hold over the next few years as more jurisdictions pass online voting laws. Jeremy Sharrard, who analyzes public policy for Forrester Research, predicts Americans could be voting for the President online by 2008. "Public sentiment is turning in favor of a different system," says Sharrard.
http://www.forbes.com/forbes/2000/1211/6615058a.html

Jury Still Out on E-voting
Americans have clearly had it with pregnant chads and butterfly ballots. But dot-coms aiming to take the electoral process online have yet to win the campaign for hearts and minds. The findings of a survey issued by the Gartner Group Monday state that while voters like the idea of voting electronically, many are still not convinced voting online is the best way to go.
http://www.localbusiness.com/Story/0,1118,SFO_543072,00.html

All Vote-counting Machines are Vulnerable to Errors
The 2000 election raises issues about voting technology, certification of voting machines, and the human element in the voting process, say two national organizations designed to protect voting rights. Key problems with today's system include voting-system failures not being reported to the FEC; voting-machine errors much higher in actual voting than allowed in equipment tests; and certification of voting equipment being voluntary.
http://www.sun-sentinel.com/news/daily/detail/0,1136,3600000000127179,00.html

A 'Modern' Democracy That Can't Count Votes
Special Report: What happened in Florida is the rule and not the exception. A coast-to-coast study by The Los Angeles Times finds a shoddy system that can only be trusted when the election isn't close.
http://www.latimes.com/news/nation/20001211/t000118473.html

Time to Streamline, Reform and Update Voting System
Postmortem analyses of the Florida fiasco are certain to demand reforms to avoid the problems that raised doubts about the validity of the national vote count and the integrity of election processes in general. Human error and bias will always be part of politics, but the process and technology of voting can and should be on the cutting edge to ensure that every legal ballot is properly counted.
http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/12/06/ED120527.DTL

Internet Societal Task Force Conducts Global Online Election Using election.com
election.com and the Internet Societal Task Force (ISTF,) the international organization for open development and widespread Internet usage around the world, today declared the success of their all-Internet election to select new members for the Internet Societal Steering Group (ISSG).
http://www.election.com/us/pressroom/pr2000/1207.htm

Teledemocrazia
Nella Contea di Contra Costa, Safevote, uno dei maggiori produttori di software per il voto on-line, ha recentemente simulato le elezioni presidenziali americane fornendo a hackers e specialisti della sicurezza le informazioni tecniche...
http://www.cittadigitali.it/teledemocrazia/sde.php#studi

In Need of an Overhaul
http://www.washingtonpost.com/wp-dyn/articles/A30148-2000Dec5.html

THE BELL c/o Safevote, Inc.
1001 D Street, Suite 202
San Rafael, CA 94901-2800

FIRST-CLASS MAIL
U.S. POSTAGE PAID
SAN RAFAEL, CA
PERMIT NO. 896

DATED MATERIAL
Please Expedite

FIRST-CLASS MAIL

Nichols Stops Certifying Voting System Software

See p. 3

To enter your FREE monthly subscription, visit the website www.thebell.net or use the form below.

cut here **MAIL ORDER FORM** cut here

Enter your one year monthly subscription to THE BELL: visit the website www.thebell.net or fill out the form below

Privacy Notice: We will not forward to third parties any personal, address or credit information supplied to us by you.

NAME/TITLE_____

COMPANY_____

ADDRESS_____

E-MAIL_____

[ ] PDF 12-Month Subscription – FREE

[ ] Printed 12-Month Subscription – $ 30.00 SUBJECT TO AVAILABILITY

[ ] Year 2000 Public Sector U.S. Market Intelligence Study, 200+ pages – $ 850.00 SUBJECT TO AVAILABILITY

[ ] Hard-copy Six Issues of THE BELL, 96 pages, from May to October/2000 - $ 15.00 SUBJECT TO AVAILABILITY

INSTRUCTIONS: Mail completed order form to the address below. Pay by CHECK or MONEY ORDER, payable to Safevote, Inc. Allow two weeks for processing.

THE BELL c/o Safevote, Inc.
1001 D Street, Suite 202
San Rafael, CA 94901-2800