The Bell™

Privacy, Security and Technology in Internet Voting

OCTOBER 2000 | Published Online Monthly | Vol. 1 No. 6
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.

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.

California Internet Voting

The California Secretary of State has contracted with Safevote, Inc. to conduct an Internet Shadow Election test in Contra Costa County for the 2000 Presidential election. The Bell presents an interview with Dr. Ed Gerck, CEO of Safevote, Inc., about this test. The test will run from October 30th to November 3rd during the period of early voting at the main election office in Martinez and is available to anyone who visits the office.

(continued on p. 3)

The Strength of Small Numbers

In this article, Roy Saltman discusses using a small number of verification events in order to improve assurances in vote counting. How small can "small" be? This discussion applies directly to Internet voting.

(continued on p. 5)

The Private Sector Won't Wait, Conclusion

An example of proxy voting at Intel, including the process of supplier selection and evaluation. This article concludes the series on private sector Internet voting.

(continued on p. 9)

The Bell Inaugurates Editorial Board

(continued on p. 2)

Contents

From the Editor by Eva Waskell 2
California Internet Voting by Eva Waskell 3
The Strength of Small Numbers by Roy G. Saltman 5
The Private Sector Won't Wait, Conclusion 7
IVTA 14
Media Watch and Links 14
From Our Readers 15

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 State of California has begun an historic test of Internet voting systems for the November Presidential election. This is a golden opportunity to put into practice the fundamental design and development principles of the Internet community: consensus, running code and open peer-review. Our democracy, voters and election officials deserve no less. Let's put these test results under the microscope. What worked? What didn't? Are there any security holes to be fixed? How much of the system was controlled or could be controlled by election officials? What did the voters think?

The Bell is launching a new line of hard-copy publications, besides the monthly edition of The Bell and the website. The first publication in this line is an in-depth 200+ page market intelligence study of the Year 2000 U.S. public election sector, with detailed information on the public election market in five states (California, Florida, Illinois, New York, Texas) and fifteen counties, including the voting systems being used, interviews with election officials, comments on the voting system certification process, perceived attitudes toward system change, and opportunities for Internet voting in each case. The second publication contains the first six issues of The Bell, including two complete overviews of market intelligence studies (public and private sectors) and important technical articles. This volume is a great way to organize the wealth of information that has been published here in the past six months. If you are interested in any of these hard-copy publications, please fill out the form on the back cover.

You have undoubtedly noticed that the Interactive Glossary has been missing for two issues. This is because we needed to leave more room for the articles. The Interactive Glossary will continue as space permits.

An independent Editorial Board for The Bell (see the two sidebars) has been inaugurated this month and is ready to begin work on the November issue. I'd like to welcome the Board members and thank them for their participation. Members were invited to provide a balanced view of diverse technologies and regional perspectives. Nominations for the Editorial Board are always open and self-nominations are accepted. Let me know if you have any names to suggest by sending an email to myself at editor@thebell.net.

Eva Waskell
Editor

California Internet Voting

by Eva Waskell[*]

The Bell interviews Dr. Ed Gerck, CEO and CTO of Safevote, Inc., who talks about the Internet Shadow Election test to be performed in Contra Costa County, as contracted with the California Secretary of State.

In August, THE BELL was the first to report that the State of California intended to conduct an Internet Shadow Election test this November, as a step toward Internet voting in public elections. THE BELL extended an invitation to all participating companies to present a report. In this issue we interview Dr. Ed Gerck, CEO and CTO of Safevote, Inc. We also publish comments from other parties who are privy to the details of the test – the California Secretary of State's office, Contra Costa election officials, election and Internet experts.

THE BELL: What can you tell us about this Shadow Election test? Is this an official initiative? Who can participate?

Gerck: The California Secretary of State has contracted with Safevote, Inc. to conduct an Internet Shadow Election test in Contra Costa County for the 2000 Presidential election. The test will run from October 30th to November 3rd during the period of early voting at the main election office, located in Martinez, 524 Main Street, from 08:00 AM to 05:00 PM. This test is open to anyone who visits the Martinez office. The office phone number is (925) 646-4166; the website is http://www.co.contra-costa.ca.us .

THE BELL: We asked for comments from Alfie Charles of the California Secretary of State's office and from Hugh Denton, Assistant County Registrar for Contra Costa County. Alfie Charles told us that *"The Internet Voting Task Force appointed by Secretary of State Bill Jones recommended a phased, cautious approach to Internet voting. We believe that this Shadow Election test is designed to do just that."* Hugh Denton commented that *"I see this as the first step toward making voting more accessible and more convenient to everyone in the county. Our staff is very excited about this project."* We would like to know what you could add to their remarks.

Gerck: California is setting a good example with this joint project. We have provided the Secretary of State with a comprehensive 40-page Technical Report that describes the technology we are applying and we are submitting a Testbed Report with the final network configuration and protocol information that will actually help the State's technical advisors to attack our system and try to compromise the election.

THE BELL: Do you think they will succeed?

Gerck: No, and that is why we are giving all information to facilitate attacks, including information on the number, function, size and format of all secret keys – just not their value. We are also making this information public at our website and are inviting hackers as well as security experts to try to attack our system. This information will also be posted to all major hacker and cryptography lists. We invite all kinds of attack, including denial of service attacks.

THE BELL: Why make such information public? Wouldn't it be better to keep it confidential and thus make it harder to attack the system?

Gerck: It is widely recognized in the design of secure systems that security must not be based on secret methods but on secret keys. Methods can be easily exposed by use of the system itself, by collusion with one agent, by mathematical analysis, or by unavoidable leaks in distributing and certifying the methods. There are many examples of each of these cases on public record. Secret keys, on the other hand, are never exposed during use (in well-designed systems), can be divided among as many individuals as one needs in order to deter collusion, and can be changed easily and often. For example, suppose we would wish to keep secret the configuration of our network. Anyone visiting the election office may easily see our network configuration. Suppose we would also want to keep secret the IP addresses we use at the precinct. If someone discovers the phone numbers we use to connect to the Internet from the precinct, scan programs for IP addresses can easily find the IP addresses we can use from a set of possibilities (by the hacker first discovering the physical locations for the phone numbers and then correlating them with IP registration data, which data are public). So to avoid all this trouble for attackers, we will provide them with our network configuration, the internal IP numbers used and the range of IP numbers we may actually use for Internet traffic.

And last, but first in our thoughts, well-designed security must have several in-depth mechanisms – it must not be like a balloon popping, where one shot does it all. Thus, by making public everything that can help attackers in this test, we are allowing them to get closer to the inner circles

of defense, circles that must not fail. So, by publishing the methods and the IP addresses we are actually raising the bar on security. In a real election, we of course would keep secret the IP addresses, routers and firewalls we use, in order to make it as difficult as possible to attack the system.

THE BELL: Recent criticism published in "Election Administration Reports" Vol. 30, No. 20, and voiced at the NSF-sponsored Internet Policy Institute (IPI) Workshop (http://www.netvoting.org), for example by Aviel Rubin of AT&T Labs, David Jefferson of Compaq and Paul Craft, a technical expert in Florida, says that Internet voting is not possible with the current state of the technology. What is your opinion on this? And how does it relate to this test in California?

Gerck: First, these opinions highlight the usefulness of this test and of our approach to invite attacks, even denial of service attacks. Let's have the critics try to break the system –we can only profit from this. If there is a hole, we will close it next time. If there is no hole found, it means it is not so easy after all but we must still give attackers other chances. Second, this test is restricted to precinct-voting, this test is not about voting from home. I think that the security experts you cite would not find any hole they could actually exploit in our test. Of course, paper is very flexible (as we say in academic circles), and the real proof about the security (or lack of security) of our system used for precinct-based Internet voting is the same as with pudding. The proof is in the eating, in the actual test configuration and results.

THE BELL: What are the benefits of precinct-based Internet voting?

Gerck: Cost reduction by sharing costs in a client-server system with electronic data transfer, increased voter participation due to greater availability of voting places for a voter (voters may vote in a precinct closer to work, not only in one that is close to home), reduced physical transportation of ballot boxes, and reduced time for tabulating results, besides being a step toward voting from home. In precinct-based voting what we do technically is to provide for a secure, remote ballot box. Conventional voting systems may also have the voting station physically separated from the ballot box, but not remotely situated. For example, there is a separate ballot box where the voter physically deposits the ballot when a voting booth is used to provide privacy to the voter while marking the ballot, but this ballot box is in the voting precinct. Conventional voting systems may also have the voting station integrated with the ballot box, as in Direct Recording Electronic (DRE) devices used in electronic voting. In these systems, however, the ballot box is always under control of at least two election officials, which is not the case in Internet voting even when precinct-based.

THE BELL: Could you summarize the technical aspects of the system being used in California?

Gerck: The computer used by the voter is in "stealth mode" on the Internet, which means it can "see" and "talk" but cannot be seen. The voter interface is very intuitive and uses either a mouse or a touch-screen. Voter authentication as well as ballot style authentication are provided by DVCs (Digital Vote Certificates). A DVC is a cryptographically signed, unique, password protected, highly compact and mnemonic digital certificate -- for example, 6TRA9K. The DVC is a device, a name and a number. DVCs are not authenticated by how they look, as passwords are, but by how they work. The ballot itself is provided by an "Electronic Ballot" – a secure, data-independent, representation-independent and language-independent ballot. The DVC and the Electronic Ballot are two components of Safevote's Multi-Party technology, based on the U.S. Patents 60/225996, 60/226042, 60/226158, 60/231600, 60/231681 and others (Patent Pending). Further information can be found at http://www.safevote.com.

THE BELL: Apparently, there is so much happening between myself and what you describe as the remote ballot box, all of which I can't even see, that this looks like a shell game. Is it all smoke and mirrors after I cast my vote or is there any way I can make sure my vote was received for tallying?

Gerck: All that voters have to do in order to verify that their vote was received is to go to the Internet and look for their "proof of receipt" (POR) in the voter list. The POR is a short string of characters that is linked to their vote and verified during tallying, and yet does not allow a voter to prove what the vote is, nor anyone to know who the voter is. We consider such voter verification an important tool to deter fraud and increase public trust in Internet voting. It is easy to prove mathematically that 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%, for example, 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 by voters is important to foster public trust in Internet voting by allowing one to close the loop of trust – i.e., trust, but verify. Our technology also allows detailed real-time and post-election auditing by election officials.

THE BELL: This month's article by Roy G. Saltman, "The Strength of Small Numbers," seems to describe a similar situation but in the context of vote recounting. Is there a similarity between Saltman's mathematical model and the property you just mentioned?

Gerck: Yes, a small number of voters who do verify whether their votes were received can considerably reduce the probability that my vote was not received – even if I never check. And this probability is calculated by the same formulas given by Saltman.

(continued on p. 9)

The Strength of Small Numbers

by Roy G. Saltman[*]

The recounting of election results is an integral part of public sector elections. The procedures for a recount are generally described in state election law. A more detailed look at the mathematical implications of the terms and conditions of recounts is contained in Appendix B of a report by Roy G. Saltman entitled "Effective Use of Computing Technology in Vote-Tallying." Although the report was published by the National Bureau of Standards (renamed the National Institute of Standards and Technology) in 1975, the computations in Appendix B and reprinted here are still valid today and can be directly applied to both tallying and recounts in Internet voting.

Introduction

One attribute of machine-readable ballots is that it is possible to recount them by a second method, either by manually recounting them or by machine-recounting them on a different, independently-managed computer system. After some difficulties with machine-readable balloting had occurred in California, that state decreed that a manual recount of 1% of all precincts, but in no case less than six precincts, must be undertaken in each election in which machine counting was used. A question may then be asked about the reasonableness of the number "1%". Under what conditions does a "1%" recount constitute a satisfactory check, and under what conditions is it less satisfactory?

More generally, what quantity of recount under what conditions will give a high confidence level that the originally reported results of the election are entirely correct? If the recounted portion agrees completely with the original report for those precincts, it will be assumed that those precincts not recounted are also correct as originally reported. If the recounted portion differs substantially from what was originally reported, a simple decision rule could be that all remaining ballots must be recounted. Other decision rules, mathematically based, could be devised, based on actual differences between the original and recounted values, but are not considered here. It can be reasonably assumed that once any significant difference is demonstrated between supposedly equal quantities, as a practical matter political rather than mathematical considerations will be overriding.

1. An Example

To investigate the question of the proper partial recount quantity in more detail, consider the following simplified example. Suppose, in a certain jurisdiction, there were exactly 1,000 precincts, and in an election just concluded, exactly 1,000 persons voted in each precinct. Suppose also that there were just two opposing candidates and there were no overvotes or undervotes. In addition, suppose the final tally originally reported was 505,000 to 495,000, a difference of 1%, or 10,000 votes out of 1,000,000 cast.

Now, to cause a reversal in outcome, there must be a vote-switch of more than 5,000 votes, but this is only 1/2% of all votes cast. This misreporting could be accomplished in any of several ways:

(a) by a switch of a minimum of 5 votes in each of the 1,000 precincts;

(b) by a switch of a minimum of 50 votes in each of 100 precincts;

(c) by a switch of a minimum of 500 votes in 10 precincts; or

(d) by a switch of some intermediate product of precincts and votes per precinct, still switching a total of 5,000 or more votes.

The above possibilities consider only vote-switching schemes in which the total vote for both candidates remains the same. There are, of course, an infinite set of possible incorrect outcomes that could be reported, but only those which involve a direct switch from one candidate to the other will retain the total vote constant. It is assumed that ballot and vote reconciliations are made as a matter of standard practice, so that any reporting error which does not retain the constancy of the total vote cast can be discovered in that manner.

Note, however, that a vote-switch using the schema of (a) above would be caught immediately if any single precinct were recounted, regardless of which one were chosen. Thus, this schema is not a likely one for a vote switching error to get by unnoticed. Similarly, the schema of (c) would clearly be observed by the opposition by a simple

inspection of the results reported, since it requires a switching of 50% of the vote in a limited number of precincts. An alert opposition would demand a recount in these specific precincts.

Suppose, however, that a vote-switch using the schema (b) actually occurred. This requires a switch of only 5% of the vote per precinct in only 100, or 10% of the precincts. Now it is not clear that an alert opposition could spot by inspection those precincts in which misreporting had occurred and could pick out the proper precincts for which to demand a recount.

In this case, there may be errors in some of the precinct results, but the specific precincts cannot be determined by inspection or by a minimum recount. Specific precincts are therefore randomly chosen to be recounted and hopefully, one in which misreporting (vote-switching) has occurred will be chosen. If no vote-switch precincts are chosen for recount, the error will go undetected, if there is any. The error is considered detected if at least one misreported precinct is selected for recount.

Consider the 1% rule applied to this problem. Just ten of the 1 ,000 precincts are chosen to be recounted and we want to determine the probability that one of the ten chosen for recount will be one of the one hundred in which vote-switching has occurred.

Let P be the probability that at least one precinct chosen for recount has been misreported. Thus P is the probability of detecting the vote-switch. Then 1 - P = Π is the probability that all precincts chosen for recounting have been correctly reported. The probability that the first precinct chosen is correctly reported is 900/1000. Given that the first precinct chosen is correctly reported, the probability that the second precinct chosen is correctly reported is 899/999. Given that the previous nine precincts chosen were correctly reported, the probability that the tenth chosen is also correctly reported is 891/991.

Thus, the probability that all chosen are correctly reported is Π = 1 - P, given by:

$$\Pi = \left(\frac{900}{1000}\right)\cdot\left(\frac{899}{999}\right)\cdot\left(\frac{898}{998}\right)\cdots\left(\frac{891}{991}\right)$$

or $\Pi = .345$

or $P = 1 - \Pi = .655$

The probability of discovering the vote switch by recounting 10 precincts is .655. The number .655 indicates that if there were many situations of exactly this type with the parameters of this problem, only about 2 out of 3 of them would be discovered, using a one percent recount. Many persons concerned with elections may find this fraction unacceptably low. The acceptably fraction may be at least .9, possibly .99, if not .999.

In this example, with 1,000 precincts and 100 of them misreported, it would take a recount of 22 precincts (2.2%) to assure a 0.9 probability of choosing for recounting at least one of the misreported. It would take a recount of 43 precincts (4.3%) to assure a probability of 0.99, and it would take 64 precincts (6.4%) to assure more than a 0.999 probability of choosing for recounting one of the misreported. To assure an absolute certainty (1.000 probability) of selecting at least one misreported precinct would require a recount of 901 precincts or 90.1% of all precincts. There is a certain efficiency, therefore, in not demanding an absolute certainty.

2. Undetectability by Observation

An important parameter determining the partial recount quantity is the maximum level of undetectability by observation. This is the largest percent switch of votes in any one precinct that will fail to make the opposition correctly suspicious that a switch has occurred in that precinct. The higher the maximum level of undetectability by observation, the higher the number of switched votes that can be packed into a single precinct, and the fewer the number of misreported precincts that are needed to reverse an election. The fewer the number of misreported precincts needed to reverse an election, the less likelihood there is of a vote-switching scheme being discovered by a partial recount. As a consequence, a higher level of undetectability by observation implies a larger partial recount quantity.

If the maximum level of undetectability by observation were 5% of the vote per precinct then, in the example above, the schema (b) would minimize the number of misreported precincts that could reverse an election. No other schema would minimize the probability of detection in this example. If less than 5% of the vote per precinct were switched, more than the minimum number of precincts would need to be misreported and the probability of discovery in a partial recount would be increased. If more than 5% of the votes in a precinct were switched, these results would be obvious to the opposition (by definition) and discovery by observation would occur.

It follows that an alert political party will keep good records of each precinct's voting patterns historically and with respect to similar precincts in the same election, thus minimizing the maximum level of undetectability by observation. The actual numerical value of this level may vary from jurisdiction to jurisdiction or even from precinct to precinct, and it is a problem for political scientists and election administrators to select the actual values.

It may be that a reasonable value is in the neighborhood of 5% to 10%. That is, a 5% maximum level means that a true 50%-50% vote split could be switched to 55%-45% (or a 52.5%-47.5% vote could be reversed) without arousing suspicion; and a 10% maximum level means that a true 50%-50% vote split could be switched to 60%-40% (or a 55%-45% vote could be reversed) without arousing suspicion.

(continued on p. 11)

The Private Sector Won't Wait, Conclusion

Safevote, Inc.[*]

This issue presents the conclusion of a marketing study overview of Internet voting in the private sector. Parts I, II and III were presented in former issues of THE BELL. This issue focuses on Intel Corporation, one of the Fortune 100 companies interviewed for the study, as an example of Internet proxy voting.

Intel Corporation

1. Customer Profile

With more than 80% of the PC microprocessor market, Intel is the world's #1 chip maker. Intel's microprocessors – including the powerful Pentium and the low-end Celeron–have provided the brains for IBM-compatible PCs since 1981. Intel's largest customers, top PC makers Compaq and Dell, each account for 13% of sales. Intel also provides flash memories and embedded chips for communications, industrial equipment, and military markets. The company is making a push into networking services (such as server farms) and communications infrastructure (such as Web appliances). About 55% of sales are outside the US. Intel's shareholder web page is at http://www.intel.com/intel/finance/ letter.htm.

Intel has 3 million shareholders and estimates that 10% are registered shareholders (300,000).

2. Current Voting Methods

Methods - Intel's registered shareholders are able to vote their proxies by mail, telephone or Internet.

In its notice of annual meeting, Intel provides the following information to shareholders regarding voting methods:

> You may vote your shares in a number of ways. You may mark your votes, date, sign and return the proxy card or voting instruction form. If you have shares registered directly with the company's transfer agent, Harris Trust and Savings Bank ("Harris Bank"), you may choose to vote those shares via the Internet at Harris Bank's voting Web site (www.harrisbank.com/wproxys), or you may vote telephonically, within the U.S. and Canada only, by calling Harris Bank at (888) 266-6795 (toll-free). If you hold Intel shares with a broker or bank, you may also be eligible to vote via the Internet or to vote telephonically if your broker or bank participates in the proxy voting program provided by ADP Investor Communication Services. If your Intel shares are held in an account with a broker or a bank participating in the ADP Investor Communication Services program, you may choose to vote those shares via the Internet at ADP Investor Communication Services' voting Web site (www.proxyvote.com) or telephonically by calling the telephone number shown on your voting form.

Intel's proxy statement provides additional information on "Voting via the Internet or Telephone."

The telephone and Internet voting procedures are designed to authenticate stockholders' identities, to allow stockholders to give their voting instructions and to confirm that stockholders' instructions have been recorded properly. Counsel has advised the company that the Internet voting procedures that have been made available through Harris Bank are consistent with the requirements of applicable law. Stockholders voting via the Internet should understand that there may be costs associated with electronic access, such as usage charges from Internet access providers and telephone companies, that must be borne by the stockholder.

Length of use - Intel's Relationship Manager at Harris Bank Shareholder Services states that 1996 was the first year that Harris offered Internet proxy voting, and notes that Intel was Harris' first client for Internet proxy voting.

Suppliers - Internet proxy voting for registered shareholders is provided by Harris Bank Shareholder Services. ADP provides Internet proxy voting for beneficial shareholders.

Cost - Per vote costs are:

	Harris Shareholder Services	ADP
Postage-paid	$.10 to $.20 *	$.34
Telephone	$.24 for U.S. $.84 for Canada	$.18
Internet	$.10 to $.20	$.03

* Note: The Relationship Manager states that the cost of paper votes is generally built into the (bundled) standard fee charged to clients. Incremental costs (over the standard

fee) would only be incurred if the corporation has a large number of unusual proposals.

3. Selection Process

Intel's Retail Investor Relations Manager notes that no other alternatives to the transfer agent's Internet proxy voting system were considered.

Intel's Relationship Manager at Harris Bank Shareholder Services states that Harris initiated the idea of Internet voting with Intel "knowing that they are high tech and always looking for new, innovative ideas." Prior to offering Internet voting Harris had developed an electronic proxy consent system, whereby shareholders could sign up to view the proxy statement and annual report at Intel's web site in lieu of receiving hard copy documents in the mail.

The Relationship Manager notes that Harris did all of the development on the Internet proxy voting application. Intel provided substantial feedback on test versions of the application during the development process. In particular, Intel provided input from the standpoint of the shareholder in terms of the usability and image of the system.

4. Supplier Evaluation

Motivation for Internet Proxy Voting - Intel's West Coast Investor Relations Manager hypothesizes that Intel was motivated to offer Internet proxy voting because of the potential for substantial cost savings given the company's large base of approximately 3 million shareholders.

Shareholder Participation: Intel's Retail Investor Relations Manager states that the number of shareholders consenting to viewing proxy materials and the annual report online is still small. He notes that Intel sent a mailing to its nearly 3 million shareholders and only a small percentage signed up for this option. Secondary sources indicate that 10% of Intel's registered shareholders consented to electronic viewing of proxy solicitation materials during its 1997 proxy season, just below its break-even point for the cost of the this service [http://www.ffhsj.com/firmpage/CMEMOS/0143034.htm]

Intel's Relationship Manager at Harris Bank Shareholder Services provided the following statistics on Intel's May 17, 2000 annual meeting:

Proxies cast by registered shareholders	60,000	
Number of telephone voters	16,000	27%
Number of Internet voters	8,000	13%

Note: 60,000 proxies cast represents a 20% voter turnout.

In 1996, the first year Internet voting was offered by Harris to Intel shareholders, 1900 proxy votes were cast over the Internet.

The Relationship Manager notes that 21,000 registered shareholders (7% of registered shareholders) consented to viewing their proxy materials electronically in 2000. He was not able to provide a number reflecting the total number of consents that Intel has obtained to date.

The Relationship Manager observes that people with a large number of shares tend to vote, and that younger shareholders are less likely to vote than older shareholders.

Privacy and Security Concerns - In responding to the interviewer's questions on Intel's concerns with the privacy and security of Internet proxy voting, the Retail Investor Relations Manager states that "The whole world is concerned about privacy and security. We are putting enormous efforts into our microprocessors, and servers. One of the foundations of our new server chip is security. I think it is one of the biggest concerns about the Internet that there is. Everybody is concerned."

The Retail Investor Relations Manager further notes that he has two large binders of information from ADP and Harris that contain information on the privacy and security of their respective Internet proxy voting systems. He notes that ADP and Harris "use very serious control numbers and have secure sites."

Proxy Voting Web Site - Intel's registered shareholders are directed to Harris' web site for Internet proxy voting: www.harrisbank.com/wproxy where they select Intel from a drop down list of companies. Beneficial shareholders are directed to vote at ADP's www.proxyvote.com The Retail Investor Relations Manager is not aware of any discussion that has taken place on directing voters to vote through a link on Intel's web site vs. at a third party site. He notes that directing registered shareholders to the transfer agent's web site is a logical choice since the transfer agent is responsible for providing a range of support services to shareholders, including providing account balances, handling address changes, transferring stock ownership and distributing dividends.

Intel's web page on proxy voting instructions (http://www.intc.com/intel/finance/proxy00/proxy16.htm) provides the following instructions for shareholders:

> *For Shares Directly Registered in the Name of the Stockholder.* Stockholders with shares registered directly with Harris Bank may vote those shares telephonically by calling Harris Bank at (888) 266-6795 (within the U.S. and Canada only, toll-free), or via the Internet at Harris Bank's voting Web site (www.harrisbank.com/wproxy).
>
> *For Shares Registered in the Name of a Broker or a Bank.* A number of brokers and banks are participating in a program provided through ADP Investor Communication Services that offers telephone and Internet voting options.

(continued on p. 14)

California Internet Voting

(continued from p. 4)

THE BELL: How about the voter interface? Is it easy to use in spite of the privacy and security features?

Gerck: The voter interface is a very intuitive design using a mouse or touch screen. There is no keyboard needed. Users clearly see the benefits of eliminating the keyboard, with all of its 103 keys. Our interface is self-explanatory. One touch to vote each candidate, a second touch to clear the vote if desired. Blank votes are accepted at any time. Overvoting is not allowed. Voters cannot vote twice. Voters will be able to verify that their votes are actually received for tallying by visiting Safevote's website.

THE BELL: How about voting from home? Could the same system be applied ?

Gerck: A substantial part of the system used by Safevote for the California test is also a part of our system for Internet voting from home. Voting from home, however, introduces additional challenges – and also decreases some. Our solution in both cases is based on a multi-party distributed system, where rather than asking for a mythical "trusted system" as some panelists in the IPI seminar called for, we take the stance that we need to favor multiple, independent communication channels over one "strong" channel. We need to avoid what I call the "Fort Knox Syndrome" – the putting-all-your eggs-in-one-basket approach, even if the basket is reputedly "strong." We expect to submit our system for voting from home to practical tests in the future, in which we shall also make all methods public in order to facilitate attacks in the testing phase. Forestalling automated fraud is an important consideration in this scenario.

THE BELL: Do you think that the Internet can in any way be used for U.S. public elections now?

Gerck: In spite of our technology and our trust in it, NO. My opinion is that one can have binding Internet public elections only when we achieve "rough consensus and running code." Even for precinct-based Internet voting, as done in Contra Costa. That is why this test is important. It serves to test the running code and to develop consensus.

"Rough consensus and running code" is the time tested, two-prong test often mentioned at the IETF (Internet Engineering Task Force) as a rule for defining Internet standards. Internet standards are very complex and involve so many different systems and nuances that anything less than a requirement for both a conceptual agreement (manifest in "rough consensus") and a perceptual agreement (manifest in "running code") could easily lead to disaster in spite of the best intentions and efforts. Perfectly adequate methods may have imperfect implementations, imperfect interfaces and imperfect interoperation. There are many examples of such problems, especially in Internet security protocols.

Further, we feel we need to develop trust in Internet voting before we place it in such a central role in our democracy. To develop trust, takes time and effort.

At this time, however, we see nothing of this. There is no consensus, no trust. There is not even consensus regarding what an "electronic ballot" might be and how it might be controlled. And there are laws that need to be passed. So rather than asking for laws to advance technology, we need time – enough time to do it right the first time. Our focus in the public sector is thus not so much on time, but on *doing it right the first time.*

Therefore, Safevote suggested to the Federal Election Commission (FEC) that all Internet-related items in the next FEC standards should be labeled "EXPERIMENTAL," which will also help prevent their hasty adoption as anything but experimental rules. Our experience with the Internet, which dates back to 30 years on our team, tells us that there are many, many details in any Internet protocol that only "rough consensus and running code" can deal with.

Also, using our particular case as an example, Safevote's technology provides us with many suitable answers for Internet voting. We need to grade them in time from short-term to long-term and also test which ones are better in terms of an overall design that includes legacy systems, legacy code and the regulatory environment. Our strategy is to test, test, test – and we feel that this strategy is not only to our benefit but to the benefits of others as well, including voters.

This is also what I said to the FEC, personally and in writing, as well as to the California Secretary of State. A copy of my statements in this regard was published in The Bell's September issue, pp. 9 and 10.

THE BELL: Will the Internet eventually be used for U.S. elections – given all the privacy, security and integrity assurances required by law?

Gerck: Yes. You may recall that Internet voting from home is already legal in more than 28 U.S. states, for the private sector. Public sector voting, however, not only involves higher assurances for privacy, security and integrity but is not even legal in any U.S. state. This may change in a few years. But keep in mind that in science and business a "no" is also an answer. So, any of our efforts toward finding and proving that Internet voting can be made less costly, less fraud-prone and less time consuming are to be seen in such light. I would never accept being the CEO and CTO of a company that would put the answer before the test. On the

other hand, I find it intellectually misleading to say that "there is no answer," or that "this is impossible" and other such "expert opinions" which history books are cluttered with. This type of attitude, which however I hear less and less in regard to Internet voting, is not helpful even if the prediction would be correct. After all, science is based on openness of mind.

THE BELL: Did Safevote ask outside experts to take a close look at the technology being used in this California test? What was their opinion?

Gerck: Outside experts, even if not entirely independent because they are selected and hired by the company, are nonetheless useful for the company and for those relying on the company's statements. We selected Roy G. Saltman, a well-known election expert who is a frequent contributor to THE BELL and Einar ("Stef") Stefferud, principal of Network Management Associates and a pioneer of the IETF who has been involved with Internet standards and protocols since 1975, before the Internet was called "Internet." Both experts agreed that the California Internet voting test to be conducted by Safevote provides significant assurances for privacy and security.

Saltman summarized his analysis with the statement that *"The six-character DVC appears to be a clever implementation that authenticates both the voter and the ballot style. The interface uses a mouse or touch-screen which the voter should find simple and easy to use. The system is designed to provide voter privacy and employs a thorough application of security techniques from end-to-end."*

Stefferud summarized his review by saying, *"I have reviewed the Technical Report for the Safevote system being used in the Contra Costa County Shadow Election test, and I find that it is based on a truly comprehensive set of requirements, and that the test system meets the stated requirements. In short, it does provide proper ways to conduct elections without compromising privacy in the interest of security."*

THE BELL: The U.S. election administration system has always been based on voting systems that the election officials control. In view of this historical fact which is rooted in a legal mandate, what do you think about some voting companies that now propose to control Internet voting systems and in fact run them?

Gerck: A disaster waiting to happen. Safevote's approach differs from the "Fort Knox Syndrome" implicit in your question – after all, where is the "trusted system" that will allow election officials to trust that which they cannot control? Furthermore, one may think that adding a 24x7 human interface providing vigilant monitoring with real-time penetration detection and response (as oftentimes done in e-commerce) might be the security solution required for optimum protection in voting systems. However, this still does not guarantee that the network will not be attacked, and if network surveillance would fail due to human error or collusion, then the whole system would fail. I also frequently make the point that trust is an open-loop control system. So you never really know what is happening at the other side. E-commerce security solutions can tolerate some degree of failure and fraud as the cost of doing business, which cost is usually shared with the clients themselves as insurance costs. Public elections need, however, a higher level of assurance – there is too much at stake and insurance solutions are simply not possible. We need fail-safe systems.

And voting companies cannot be judge, jury and executioner. That is why Safevote's technology was designed so that nothing that is under Safevote's control can in any way influence or hinder the election even if everything that Safevote controls fails and all of Safevote's personnel colludes. This is valid both for our precinct-based as well as voting from home systems. The software we supply is developed to be open source and is 100% under the election official's supervision. The private and secret keys are generated without our intervention. The services we supply are ancillary and do reduce cost and time but if they fail, redundancy would still allow the election to go on. Integrity is verified by log files generated under the control of election officials. Tallying involves pre-authentication as well as post-authentication and cannot be done without secret keys and data from the election officials. Auditing involves voter registration files and the tallied votes, both controlled by the election officials.

THE BELL: Is this a new kind of security paradigm?

Gerck: In a way, it is as old as history itself. For example, one of the earliest references to the security design I mentioned can be found some five hundred years ago in the Hindu governments of the Mogul period, who are known to have used at least three parallel reporting channels to survey their provinces with some degree of reliability, notwithstanding the additional efforts. On the other hand, with the "Fort Knox Syndrome" design so widely seen in the Internet security community, the solution is "make it stronger!" But in this model an entire chain can still be compromised by failure of one weak link – even if that link is made stronger. The solution in our design is to use a multifold of links, arranged in time and space such that rather than making the impossible assumption that "this part will **not** fail at any time," we can design a system where up to M parts can fail at any time, even the entire number of parts. Further, rather than seeking "infinite protection" at one point (for example, the vendor), which is clearly impossible, we set up a system where a measure of protection as large as desired can be attained by using an open-ended number M of points, each one individually affording some "finite" protection (for example, from one or more vendors) and contributing to higher-orders of integrity.

THE BELL: What are the main principles in this design?

Gerck: The design strategy behind the Multi-Party technology used by Safevote 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 criteria.

THE BELL: How are the evaluation criteria defined?

Gerck: In a Safevote system, three criteria are essential: voter privacy (the inability to know who the voter is); vote secrecy (the inability to know what the vote is); and election integrity (the inability of any number of parties to influence the outcome of an election except by properly voting).

THE BELL: What about open source, open standards and third-party use of Safevote's technology? There are proprietary vote-counting systems today and that is problematic to say the least.

Gerck: The specifications for Safevote's products and services under the Multi-Party technology will be made fully public and documented with open protocols, and protected by flexible intellectual property rights that allow free non-commercial use.

The technology is patented but is available for licensing in commercial use. Full information on Safevote's technology is available for expert review and testing by Safevote's Advisory Board, an independent panel of experts in various areas of Internet protocols, security and elections. Safevote's protocols will also be subject to open peer review at the Internet Voting Technology Alliance (IVTA).

These initiatives intend to help Internet voting move quickly but prudently toward public open standards, open source software, responsible self-regulation and voter oversight, as mechanisms to foster public trust in Internet voting. Safevote profits in this open arrangement by sharing the benefits of interoperation and open protocols in the pursuit of worldwide applications in various market segments.

The Strength of Small Numbers

(continued from p. 6)

3. Development of a Recount Formula

Consider now the development of a general formula to determine the necessary partial recount quantity to assure a particular probability of detection of misreporting based on a given maximum level of undetectability by observation.

As before, let P equal the desired and given probability that a partial recount will select, for recounting at least one vote-switched precinct. The value of P also, whether 0.9, 0.99, 0.999, or some other value, must be selected by subjective decision since it depends on the trade-off between effort expended on recount and confidence that the true voted results are mirrored in the published figures.

Then, as before 1 - P = Π is the probability that no misreported precincts will be selected for recounting.

Let p equal the total number of precincts; f equal the number of misreported precincts; and r equal the number of precincts recounted. Then, by analogy with the example above:

$$\Pi \geq \prod_{k=0}^{r-1}\left(\frac{p-f-k}{p-k}\right) \qquad (1)$$

Equation (1) is essentially a formula for independent sampling without replacement. The precincts being recounted are the samples. The probability of the first sampled precinct being correctly reported is (p - f)/p and sampling of precincts for recounting éontinues until that value of r is reached at which the cumulative probability of selecting only correctly-reported precincts is equal to or less than the given P. An inequality is shown in (1) because it is assumed that P is known in advance and the problem is to find r, the number of precincts to be recounted. As r must be an integer, it is unlikely that the right-hand product in (1) will equal the given P exactly.

Now, solving for P,

$$P \leq 1 - \prod_{k=0}^{r-1}\left(\frac{p-f-k}{p-k}\right) \qquad (2)$$

If x, the maximum level of undetectability by observation is given as a fraction, and d, the difference in the candidates' votes plus one (in a two-candidate race) is also given, then f, the minimum number of vote-switched precincts that will overturn the contest is easily computed.

First, d/2 (plus 1/2 if d is odd) is the minimum number of votes that must be switched in order to reverse the election, and let n be the total number of votes cast. Then, n/p is the number of votes per precinct, (assuming an equal number of votes in each precinct) and nx/p is the maximum

number of votes in each precinct that can be switched without detection by observation. Then the minimum number of vote-switched precincts required to reverse the election is:

$$f = \frac{d/2}{nx/p} = \frac{p}{x} \cdot \frac{d}{2n} \qquad (3)$$

In (3), d/n is the fractional difference between the candidates and d/2n is the minimum fractional difference between the candidates that needs to be switched in order to reverse the election. As f must be an integer number of precincts, if it is not as a result of calculation from (3), the next highest integer is selected.

By substituting (3) for f into (2), the number of precincts to be recounted, r, is determined as a function of P, p, x, and d/2n. Of these independent variables, P, p, and x are determined independently of the election results and d/2n is established directly as a result of the originally-reported tally.

One can now use equation (2), with (3) substituted for f, in order to calculate the number of precincts to be recounted for various values of P, the probability of selecting at least one vote-switched precinct for recounting, as a function of d/2nx. This can be done for values of P such as 0.9, 0.99, and 0.999. Then, given a desired value of P, the number of precincts to be recounted is known as a function of p, the total number of precincts, and d/2nx.

These calculations show that, for constant p and x, as the candidate fractional difference d/n gets smaller, the number of precincts to be recounted becomes larger and approaches the total number of precincts. This accords with what one would intuitively expect, and what actually occurs in practice. When there are very small reported differences between candidates, there is a high likelihood of a recount being demanded.

4. Effect of Larger Number of Precincts

An interesting phenomenon, not intuitively obvious, can be seen from an inspection of the calculated results. For equal values of d/2nx, the number of precincts to be recounted is roughly the same for significantly different quantities of total numbers of precincts. For example, if d/2nx =0.1 and P = 0.9, then 22 precincts must be recounted, for total number of precincts equal to 500, 1000, 2000, or 5000. The percentage of precincts recounted is very different if 22 of 500 are recounted rather than 22 of 5000. The results show, therefore, that to minimize the absolute number of ballots recounted, there should be more precincts. More precincts are obtained by having fewer voters per precinct, but this may raise the cost of general administration.

5. More Complex Situations

At this point, only the simple situation of just two candidates, equal numbers of voters in each precinct, and no overvotes and undervotes, has been considered.

In an actual election, the number of voters per precinct is variable, not constant as has been assumed. The validity of the analysis presented depends upon the type of misreporting of precinct results with which the election administration expects to be confronted. If it could be assumed that vote-switched precincts occur randomly such that the mean size in voters per precinct of these precincts equals the average size of all precincts, i.e., n/p, then the expected number of misreported precincts will be the same as that computed by equation (3).

On the other hand, it may be noted that if vote-switched precincts were larger than average size, fewer of them would be needed to overturn an election than the number computed by (3). One strategy that could be employed to guard against this possibility is for precincts to be selected for recounting with a probability proportional to the number of voters that each has. Other strategies could be adopted and there appears to be ample material for further investigations.

When there are undervotes and overvotes, as well as candidate votes, a vote switch can occur between a candidate and either an undervote or an overvote instead of between two candidates. If one candidate's votes are increased at the expense of overvotes or undervotes, an error could be introduced without disturbing a second candidate's votes at all. In this case the second candidate's fraction of total candidate votes remains larger than it would have if that candidate's votes were actually reduced by a vote-switch.

Thus, there is less likelihood of detection by observation unless records have been kept on undervotes and overvotes, enabling unusual conditions to be discovered. However, undervotes and overvotes are nearly universally not reported at this time. [Editor's note: Undervotes and overvotes are reported much more frequently today.]

Similarly, with more than two viable candidates, the maximum level of undetectablity by observation, as a practical matter, would be somewhat higher since the election would be more difficult to predict. A vote switch could take small numbers of votes from several opposition candidates to benefit one candidate, thereby minimizing detection by observation.

One mitigating circumstance is that the calculations of equations (2) and (3) made to determine recount quantities were based on the minimum number of votes needed to switch an election outcome. The probability of a vote-switch with the minimum number of votes to overturn an election is small. Any smaller number of votes switched would have no effect on the outcome, and any larger number of votes switched (to further assure a specific outcome) would increase the probability of detection, either by partial recount or by observation.

6. Findings

An adequate partial recount quantity depends on the closeness of the vote, the total number of precincts involved, the value of the maximum level of undetectability by observation, and the desired probability of detection by recount. The latter two quantities can only be determined subjectively at this time.

In a close election, a flat 1% recount is insufficient to detect vote-switching of sufficient magnitude to overturn it.

Ballot reconciliations and reporting of overvotes and undervotes will reduce the opportunities for undetected vote switching.

Election administrators, candidates, and others interested in honest elections should keep well-documented records of voting patterns and expected numbers of overvotes and undervotes so that abnormal voting results can be more easily spotted and investigated. Such records may be used to develop a quantitative basis for such parameters as the maximum level of undetectability by observation.

Dividing the electorate into a larger number of precincts will reduce the total number of ballots required to be recounted to maintain the same capability of detection of vote-switching.

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.

The Private Sector Won't Wait, Conclusion

(continued from p. 8)

This program is different from the program provided by Harris Bank for shares registered directly in the name of the stockholder. If your shares are held in an account with a broker or a bank participating in the ADP Investor Communication Services program, you may vote those shares telephonically by calling the telephone number shown on the voting form received from your broker or bank, or via the Internet at ADP Investor Communication Services' voting Web site (www.proxyvote.com).

5. Voter Feedback

Individual vs. Institutional Shareholders: As of 5/31/00 Intel had 3.3 billion shares outstanding. 46.6% of shares are owned by individual/retail investors and 53.4% of shares are owned by institutional investors.

The Retail Investor Relations Manager states that approximately 90% of Intel's shares are held in street name. Registered shareholders (handled by the transfer agent) hold 10% of Intel's shares. He notes that ADP and Harris are the best information sources on voter reaction to Internet proxy voting. The West Coast Investor Relations Manager made the following comments on shareholder response to Internet proxy voting: "Not everyone gets around to it. The people who use it like it. Some people prefer to vote by telephone." The Relationship Manager notes that the feedback that was obtained from shareholders during the initial years of offering Internet voting was positive, with the exception of the first year when shareholders experienced difficulties using the 128 bit encryption that was used that year. Harris is no longer using a formal shareholder feedback mechanism.

6. Additional Information

Selection of Transfer Agent - The West Coast Investor Relations Manager notes that customer service is a key factor in the selection of a transfer agent. In the case of Intel, the ability to handle a large shareholder base is another critical selection factor. The West Coast Investor Relations Manager states that, based on her overall experience in Investor Relations, smaller transfer agents tend to provide poor customer service as they lack sufficient staff to handle all of the small accounts they maintain. She notes that larger transfer agents are able to attract large corporate customers and can cut costs through economies of scale. Larger transfer agents also are able to invest in technology which enhances customer service and lowers labor costs. She notes that the transfer agent business is very labor intensive. She observes that these factors are likely causes of the consolidation that is taking place in the transfer agent industry.

Electronic consent and notification - The Relationship Manager states that to meet SEC evidence of delivery requirements Intel prefers to obtain paper-based consents from shareholders. Harris mails the consent forms and the proxy card containing the web site where proxy materials are located to shareholders. The Relationship Manager cites the frequency of email address changes, the need for additional steps to cross reference shareholders and email addresses, and tracking rejected emails as difficulties with using an email notification process.

This article concludes the series "The Private Sector Won't Wait."

Internet Voting Technology Alliance

The Internet Voting Technology Alliance (IVTA) serves the public by acting as an information center, discussion forum and voluntary standards setting body and web publisher focused on Internet voting.

The IVTA Discusses Open Communication

The idea for an Editorial Board for THE BELL, inaugurated this month, grew out of a discussion on the IVTA ADM Workgroup. A suggestion was made by Ed Gerck that The Bell could eventually be published by the IVTA or some other open organization. A first step toward this goal would be to set up an independent Editorial Board. Internet voting technologies and the related policy issues are very complex. Everyone benefits from having the broadest possible sources of input. Complex changes should not happen overnight. The market needs time to mature. The technologies need time to be thoroughly tested. Standards and legislation are not yet in place. But the idea is to begin providing for open communication channels now, so that input from as many sources as possible can be included in the dialogue.

Web Archives of TECH and ADM Workgroups

The messages in the TECH and ADM WGs are archived at http://www.mail-archive.com under the names tech & adm.

Media Watch & Links

1. Four California Counties to Test Voting via Internet
This month, Contra Costa, Sacramento, San Diego and San Mateo Counties will launch the first online voting projects in the state. They're out to test the latest technology and the concept that the click of a mouse is the key to a more democratic future.
http://www.sjmercury.com/svtech/news/front/docs/vote100300.htm

2. Technology and Risks
"Current paper-based public election technology...is fraught with problems that do not even allow one to even say with some degree of certainty whether an election was honest or not," said Internet technology and security expert Ed Gerck. Gerck is CEO of Safevote.com, which provides encryption technology that allows users to vote over the Internet. He's also chairman of the Internet Voting Technology Alliance. Published In "Accepting Risk" by Edward Mazza, Techtrends 2000 (a supplement to Government Technology), August 2000, page 26.

3. Abuse of Electronic Voting Systems in Australia
The Australian Broadcasting Corporation ran a television show recently in which viewers were invited to vote either by toll number or by an online voting form. Apparently there was nothing to stop someone voting early and voting often. Mediawatch did some research and has raised some questions about the results.
http://catless.ncl.ac.uk/Risks/21.06.html#subj1
http://www.kuro5hin.org/?op=displaystory&sid=2000/10/1/112341/127

4. Compaq Teams with VoteHere.net to Deliver Online Voting Pilots for Fall Presidential Elections
Compaq Computer Corporation has announced an agreement with VoteHere.net, a leading worldwide provider of online voting services. The companies will work together to deliver complete solutions for state-sponsored online voting pilots for the November presidential election. The agreement combines Compaq's experience in delivering solutions to state and local governments with VoteHere.net's online voting software.
http://www5.compaq.com/newsroom/pr/2000/pr2000100302.html

5. election.com Partners With Compaq and Microsoft
To increase the scalability of the election.com voting application, election.com worked with Microsoft to establish a real online data center that runs on a rack of 42 Compaq front-end Web servers and a 32-way Compaq Proliant ML770 back-end server. Windows 2000 Datacenter Server, operating on new hardware from Compaq, enables election.com to scale up its back-end to 32 processors and 64GB of memory to handle even the highest level of voter turnout.
http://www.election.com/us/pressroom/pr2000/0926.htm

6. Is There a Future for Voting in Pajamas?
The wave of the future could be remote voting via the Internet. But some people are urging caution. "The companies, government and citizenry need to work together and there needs to be an experimental phase before we implement anything," said Michael Cornfield, director of research for the Democracy Online Project at George Washington University. Cornfield added that the problem is that the technology behind remote Internet voting can't be worked out on the second day.
http://www.washingtonpost.com/wp-dyn/articles/A30266-2000Sep18.html

7. Can the Net Revive the Vote?
Internet voting fraud needn't be high-tech at all. The time-honored methods of election fraud–such as duplicate registrations, registering unqualified voters and voting using identifications and registrations of those who have moved away or died–could be incorporated into Internet voting. "All those possibilities are there and are real," said Paul Craft, manager of voter systems at the Florida Division of Elections. "But the fact that risk exists does not mean Internet voting is impossible; it simply means you have to address the risk." And companies in the Internet voting business are addressing the risk, said Craft, who is studying Internet voting's potential for use in Florida.
http://www.fcw.com/civic/articles/2000/September/civ-cover-09-00.asp

8. A Vote for Electronic Balloting
Riverside has become the first California county to do away with the venerable paper ballot, adopting instead an electronic system that will enable voters to make their choices in November's general election by touching a computer screen.
http://www.latimes.com/business/cutting/20000927/t000091697.html

9. ICANN Selects election.com to Conduct One of World's Largest All-Internet Votes
The Internet Corporation for Assigned Names and Numbers (ICANN), the technical coordination body for the Internet, and *election.com*, a leading global Internet election company, announced today that *election.com* will conduct ICANN's first worldwide online vote.
http://www.election.com/us/pressroom/pr2000/0921.htm

10. Technology: A Change Agent for Democracy
"And Brazil, the world's second-largest democracy with 90 million electors, is also looking to give its citizens an opportunity to vote over the Internet. An internet voting system is being put in place by Modulo Security Solutions, a Brazilian company known primarily for providing network system integration for online banking. Other partners in its voting system project are Microsoft, Cisco, Safevote, Entrust Technologies and Compaq.....

There is a need to ensure public confidence in online voting: nobody wants to risk a public backlash by moving too quickly. This concern should result in security and confidentiality standards higher than those used currently for conventional paper ballots. In the end, e-voting should in fact serve to prevent and eliminate election fraud like ballot stuffing."
http://www.microsoft.com/uk/business_technology/gov/912.htm

11. Electoral Reform Society
Founded in 1884 (as the Proportional Representation Society), the Electoral Reform Society is probably the oldest organization in the United Kingdom concerned with electoral systems and procedures. The Society is membership-based and campaigns for the strengthening of democracy through changes to the voting system and electoral arrangements. The Society's Commission on Electronic Voting and Counting was launched in January 2000 to examine the security implications of new methods of voting. Some believe that it is only a matter of time before other forms of electronic voting are used in the UK. Hence the need for an independent commission to consider the implications of these changes.
http://www.electoral-reform.org.uk/

LINKS

http://www.net-security.org

http://www.mercurycenter.com/svtech/news/breaking/merc/docs/068986.htm

http://www.guardian.co.uk/internetnews/story/0,7369,372676,00.html

From Our Readers

From Constance A. Kaplan, Community Services Director, Chicago Board of Election Commissioners

"Thank you for keeping me up to date with issues of The Bell. It is exciting to watch the progress that is being made in the area."

From Paul F. Chamberlin, International Technology & Trade Associates, Inc., Washington, D.C.

"Thanks for providing this excellent newsletter."

From Steven Clift, in Democracies Online Newswire
http://www.e-democracy.org/do

"I encourage you to read this study [on U.S. public sector elections] in this newsletter [THE BELL]. It bullets out the concerns and positive reactions of real life election administrators to the potential of Internet voting. Election administrators are ones that hold the real power in any transition toward Internet voting."

THE BELL™ Newsletter on Internet Voting

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

DATED MATERIAL
Please Expedite

California Internet Voting See p. 3

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

cut here **M A I L O R D E R F O R M** **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