The Bell™

Privacy, Security and Technology in Internet Voting

JUNE 2000 | **Published Monthly** | **Vol. 1 No. 2**
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.

Next Issue

- Marketing Study, Conclusion: New York and Texas
- Overview of Certification Systems: X.509, CA, PGP and SKIP
- Internet Paradigms

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

Would You Vote Naked?

Would you accept stripping away your privacy in order to vote?

Focusing on current trade-offs between privacy and security, this essay discusses the privacy concerns that affect Internet voting – both in precincts as well as at home and office. Privacy is the most important issue in preparing voters to board the Internet train that is changing all our lives – and to question it.

(continued on p. 3)

Comments on the Inaugural Issue of THE BELL

"Paradigm shifts cannot be avoided if we wish to solve the issues involved with Internet voting. We need to deal with trust in the Internet. We need to fully understand the implications of the fact that voting and other Internet transactions involve much more than just two parties, as Ed Gerck discusses in The Bell in terms of a multi-party trust model."

- Einar Stefferud, Network Management Associates

"Very informative and enlightening...Thanks!"

- Professor Netiva Caftori, Northeastern Illinois University

"Those of us already involved in internet voting will benefit from it greatly and hope we can contribute as well."

- Pat Hollarn, Supervisor of Elections, Okaloosa County, FL

(continued on p. 15)

Contents

THE BELL™ Newsletter

Editor: Eva Waskell
ewaskell@safevote.com

Website: www.thebell.net

Address: 1001 D Street, Suite 202, San Rafael, CA 94901-2800

Phone: (415) 482-9300

Fax: (415) 482-9400

Subscriptions: See back cover.

Back issues: Free of charge for PDF, consult sales@safevote.com for hard copy.

Privacy: We will not forward to third parties any personal, address or credit information supplied to us by you. Any other information we may receive is treated as public and non-confidential.

Submissions: Contributions are welcome. All material is to be submitted to the editor as an e-mail attachment in WordPerfect, MSWord or ASCII text. Submissions will be subject to peer review but authors will have the final decision on editing. There are no deadlines for submission. Material that is timely may be published immediately. The editor reserves the right of discretion on what and when to publish.

From the Editor

Dear Reader:

The response to the first issue of THE BELL was enthusiastic! Readers from the United States and abroad expressed a keen interest in the topics covered, as well as their depth – thank you all! Readers in government and private sectors have joined the dialogue, submitting comments and proposing papers. In this issue we publish some of their comments, as well as an essay by Victor Woodward of Votehere.net. It is important to hear from a diversity of viewpoints because doing so will enrich our understanding of the issues involved in Internet voting technology and its potential impacts on society.

One of the comments received indicated that the 2-column format of the newsletter was difficult to read in a browser because the viewer had to scroll too frequently. We believe, however, that most of our e-subscribers wish to print and read their newsletter with a 2-column format.

The widespread damage done by the Love Bug has shown once again that the Internet model of security is seriously flawed: one mistake is fatal, with dire privacy consequences. Now more than ever an informed public dialogue is needed to understand the depth and complexities of Internet privacy, security and the need for solutions not just fear, uncertainty and doubt.

This issue covers public elections and continues the focus on privacy and security issues in Internet voting. In addition, there is the first part of a glossary of technical terms, which is an interactive project with our readers. Coming issues will cover private applications of voting as a collaborative decision-making process, such as proxy voting, polling, auctions, bidding and consensus.

There is currently a lot of noise and rhetoric surrounding Internet voting. But what is rarely mentioned is what is needed.

Your feedback is welcome!

Eva Waskell, Editor
Communications Director
Safevote, Inc.

THE BELL'S MISSION STATEMENT

Our mission is to contribute to the public dialogue on Internet voting as well as to lead discussions on collaborative decision-making in general. THE BELL intends to provide high-quality, non-partisan, timely and useful information regarding privacy, security, technology, voting, their markets and relevant policy issues.

Would You Vote Naked?

by Ed Gerck, Ph.D.[*]

Would you accept stripping away your privacy in order to vote? Would you vote naked? Focusing on current trade-offs between privacy and security, this essay discusses the privacy concerns that affect Internet voting – both in precincts as well as at home or office. Privacy is shown to be the most important issue in preparing voters to board the Internet train that is changing all our lives – and to question it.

Introduction

Security and the Internet are like summer and baseball. At least in the U.S., one cannot think of one without the other. But what costs are we willing to pay in order to have security in the Internet?

Of course, this question both predates the current discussion on Internet voting and affects it since Internet voting uses Internet service providers, domain names, mailboxes, routers, name servers, browsers, etc. One frequently cited answer is that we should require everyone to be identified so that law enforcement could be effective. But should we be willing to sacrifice privacy in order to have security? How about voting? Should we really accept losing some bytes of privacy in order to have a bit of security in Internet voting? Should we vote naked?

Let us think for a moment – privacy is a long term asset while security is a short term goal. Thus, anyone willing to sacrifice privacy in order to gain security is essentially making a bad bargain and deserves neither. As Benjamin Franklin said ca. 1784, "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety."

Besides reducing privacy, another "solution" frequently proposed to increase Internet security and which might be applied to Internet voting would be to raise the stakes in committing a crime. This will not go very far, though, as 30 years of Internet history tells us. Fear of punishment only works to the extent that the probability of punishment is high, which is not the case with the Internet, and is certainly harder if transactions are anonymous (as voting must be). And, even if this were effective, making crime more illegal has never stopped crime. Law is no substitute for engineering, as Bruce Schneier (a cryptographer) has pointed out. Thus, from the point of view of plain common sense, law enforcement alone cannot solve the Internet security problems involved in Internet voting.

As we consider Internet voting, we realize that here is a case where privacy *must* be protected. Arguments to justify losing voter privacy in the good name of security will simply be impossible for coming applications that may use some form of Internet voting. Such applications surely need to regard security as a *protection* of privacy — not as the destroyer of privacy.

It is also impossible to screen voters in order to reduce the potential of fraud, as routinely done by banks and increasingly in e-commerce. For example, the credit card system works because banks control access to the system by card-holding consumers and card-accepting merchants – control which is used to assess the risks to the banks of admitting particular consumers and merchants. Internet Service Providers (ISPs) also screen customers and routinely cancel the subscription of spammers or fraudsters, for example.

What is security without privacy? A prison.

How about insurance? Indeed, the current "technical" solution for e-commerce security is insurance — 20% of Internet credit-card transactions are bogus and roughly half of these transactions result in the loss of real money. In order to tolerate such losses we use insurance, which socializes the cost. But, of course, the "insurance solution" to Internet security cannot be acceptable for Internet voting.

Especially when dealing with Internet voting, we cannot rely on security methods that depend on breaking privacy, reducing access and compensating for fraud in the next transaction. We need to discuss and devise computer protocols and algorithms that can protect privacy *with* security. We cannot allow privacy to be the first casualty in this frontier. Privacy is an essential liberty, the liberty to be ourselves and express our free opinion in voting — and must thus be preserved as the actual purpose of security. For what is security without privacy? A prison.

(continued on p. 4)

(continued from p.4)

Privacy and E-commerce

The question is whether we should be willing to sacrifice privacy in order to have security. In e-commerce the answer has been a resounding "Yes." And this approach has been quite successful. E-commerce Internet security is based on breaking privacy, from credit-card transactions to registering a dot-com domain name. For example, to request a digital certificate, you need to supply your private data including SSN to a Certifying Authority (CA) –a private company, allowing the creation of a global index of your private data. According to customer "opt-out" policies (widely used and legal in the U.S.), most private data collected in e-commerce on customers can and is sold to other companies, oftentimes with identifying information. When you buy or sell at e-Bay, background checks in cooperation with law enforcement are routinely used in order to allay fraud concerns. Anyone who registers an Internet domain name (among the almost eight million domain names in dot-com) needs to give their name, address, email, phone number and fax number ... and if the data is incorrect, the penalty is severe –you risk losing the domain name. This data, however, enters the WHOIS service and can be publicly seen with a browser from anywhere in the world, copied, stored in CD-ROMs and routinely sold as "address lists."

But loss of privacy in e-commerce is not so much of a problem because in an e-commerce transaction the buyer's credit-card must be identified, the buyer's bank account must be charged and the buyer's correct address must be used to send the goods to. Anything that is bought must be paid for and delivered. The same reasoning is valid for the merchant, who must also be identified, provide proof of purchase for the goods sold, render warranty services and answer complaints. Increasingly, e-commerce merchants may know a lot more about you than you think they know.

Therefore, e-commerce is quite unlike a cash transaction in a shop, where the buyer can and does remain anonymous. Current e-commerce practice is to subordinate privacy to security.

However, as mentioned in the Introduction, compromising privacy is not a solution to security problems –e-commerce is already suffering the dire consequences of placing too much customer privacy liability in the hands of merchants. In summary, even though prevalent in today's e-commerce, breaking privacy in order to support security has several drawbacks which are bound to become more and more significant as e-commerce grows.

Privacy and Internet Voting

How about public elections? Should we be willing to sacrifice privacy in order to have security in Internet voting? Here, the answer needs to be "No" from the start. We cannot compromise voter privacy.

In elections we need a "privacy wall" between the voter and the ballot – if I get the vote I cannot know who the voter is, if I get the voter I cannot know what the vote is. The security technology being used for e-commerce cannot preserve the anonymity of the vote, a right protected by law and considered essential to democracy.

Current e-commerce technology cannot be applied to Internet voting.

Conclusion

As explained above, there is a basic difference between e-commerce and Internet voting, which must not be ignored. This difference was also noted by the author during the Brookings Institution Symposium on Internet voting on January 20 [1], marking a turning point at that event. In e-commerce there must be no privacy, the merchant must know who I am, my credit card must be valid. In e-commerce there are laws that mitigate *against* anonymity. The reverse is true in public elections. There is thus a needed paradigm shift with a very strong technological point, which those on the political side also need to take into account – current e-commerce technology cannot be applied to Internet voting. We need to preserve voter anonymity, not only vote secrecy. Otherwise, we would be voting naked.

[1] *http://www.brookings.org/comm/transcripts/20000120a.htm*

Ed Gerck is a world leader in Internet security and cryptography. He received his doctorate in physics (Dr.rer.nat.) from the Ludwig-Maximilians-Universitaet and the Max-Planck-Institut fuer Quantenoptik in Munich, Germany, 1983, with maximum thesis grade ("sehr gut"). With a background in quantum mechanics, 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

Internet Voting: U.S. Market Intelligence Study, Part II

Safevote, Inc.[*]

The first part of this market study was presented in the May 2000 issue, Vol. 1 No. 1, with an overview covering the states of California, Florida, Illinois, New York and Texas. This issue highlights the study's findings in selected counties of California, Florida and Illinois, regarding election costs, current system status, Internet voting and other related topics. The July issue, Vol. 1 No. 3, will cover New York (Nassau County and the New York City Board of Elections) and Texas (Bexar, Dallas and Tarrant Counties).

CORRECTION: Page 3 of our May issue, under the heading "Study Scope," should read "The counties chosen within each state are among the largest counties by population." Thanks to Tony Servillo, election administrator of Harris County, Texas.

Highlights of State and County Findings

State of California

Certified Systems - Punch card, mark-sense, and touch screen.

Voting System Replacement Trends - Some counties replacing punch card systems with touch screen for early voting (Alameda, Los Angeles, Marin, Monterey, Santa Clara) and mark-sense for election day voting (Marin). Riverside County is reported to have selected a touch screen system for countywide election day voting. (*Note: Additional California counties may be changing systems, but were not uncovered in the scope of this study.)*

Early Voting - Absentee walk-in voting can begin 29 days before election day. Mail-in absentee voting is growing in popularity, with some counties reaching 30% absentee ballots. No specific reason must be cited to request an absentee ballot in California.

Current Voting Systems

Current Voting Systems in California **For Election Day Voting**		
	#	%
Punch Card Ballots	**39**	**67**
Mark-sense Ballots	**19**	**33**
Total	**58**	**100**

Other - Internet Voting Task Force report of January 2000 [http://www.ss.ca.gov/executive/ivote/]. By law, California counties are limited to no more than 1000 registered voters per precinct. Polling places in some suburban areas include residential garages.

California Counties

Alameda County

Election Official - Registrar of Voters

Current System Status - Votomatic punch card system with central count tabulation is at the end of its useful life. Card readers are no longer manufactured. Vote tallying is slow.

Criteria for New System - Certified in California, touch screen technology, eliminate need to print ballots in multiple languages, accuracy, and rapid vote tallying.

Election Costs -
Average cost per election: $1.7 to $2 million
Average cost per registered voter: $2.68 to $3.16

Replacement System - First phase of replacement will be conversion to touch screen system for early voting in satellite offices for November 2000 election.

Other Issues - Concern about difficulty of consolidating election results with more than one voting system, and potential need to layout ballots twice. Disadvantages of touch screen systems are increased testing, storage and transportation costs.

Internet Voting - Estimated timetable for Internet voting in Alameda County is 5 years. *(continued on p.6)*

(continued from p. 5)

Los Angeles County

Election Official - Registrar-Recorder/County Clerk

Current System Status - Votomatic system with central count tabulation is slow, but inexpensive. "Saving 4-5 hours on election night is not a reason to spend $50 million on a new voting system." Adequate back up equipment available due to consolidation of precincts.

Barriers to System Change - Cost, lengthy procurement process, technological obsolescence of new system, voter education, and political risk.

Election Costs -
Average cost per election: $10 million
Average cost per registered voter: $2.50

Replacement System - Plans to implement touch screen system for early voting in 6 district offices for November 2000 election. Does not favor mark-sense systems. "Replacing paper with paper."

Internet Voting - Willing to try an Internet voting application immediately with a small group. Internet voting is appealing as a low cost alternative to currently available systems.

Orange County

Election Official - Registrar of Voters

Current System Status - Datavote punch card system with central count tabulation. No plans to change voting systems at present. Waiting for new, cost-effective technology. Touch screen is too costly for a system that will be obsolete in 10 years. (Estimated cost = $30 million).

Barriers to System Change - Cost, new technology on the horizon, increasing absentee voting.

Criteria for New System - User friendliness, reliability (audit trail), cost, and track record.

Election Costs -
Average cost per election: $500,000 to $700,000
Average cost per registered voter: $.42 to $.58

Replacement System - Will consider replacement in 3-4 years if a cost-effective system is available. Not willing to be the first county to try a new system.

Internet Voting - Interested in Internet voting if cost-effective, certified, and proven in other counties. Views $5 to $10 million as an acceptable cost range. Estimated timetable for Internet voting in Orange County is 3 to 5 years.

San Diego County

Election Official: Registrar of Voters

Current System Status - Votomatic punch card system with central count tabulation. The system is inexpensive, well-accepted and proven. Has not experienced errors that have plagued other counties using punch cards.

Barriers to System Change - No motivation to change voting systems due to lack of cost-justification, lack of media pressure for faster election results, and bi-lingual ballot requirement limited to English-Spanish.

Election Costs -
Average cost per election: $3 to $3.5 million
Average cost per registered voter: $2.31 to $2.69

Internet Voting - May be interested in Internet voting as San Diego County is now outsourcing all IT and communications to Computer Sciences Corporation and Pac Bell. Outsourcing may give San Diego County access to the technical expertise needed for Internet voting. May be willing to test Internet voting for a small application.

Santa Clara County

Election Official - Registrar of Voters

Current System Status - Poll Star punch card system with central count tabulation. Inexpensive with capacity for a long ballot, but prone to voter error on punch cards and read errors on central counters.

Criteria for New System - Vendor customer service/ stability, preferential voting option, no single point of failure, accuracy, security, ease of use for voters and poll workers.

Election Costs -
Average cost per election: $3.2 million
Average cost per registered voter: $4.35

(continued on p. 10)

Voting Systems, Conclusion

by Roy G. Saltman[*]

This article is the final part of an overview of current voting systems and the operating principles and problems of paper-based computer-readable ballots. The May 2000 issue, Vol. 1 No. 1 covered punch card and mark-sense ballot systems. This issue concludes with a discussion of DRE (Digital Recording Electronic) systems, as well as with a comparison between precinct- and central-count systems. Other topics including election administration, software for computerized voting and documented difficulties in computerized elections, are covered by the author in the book referenced.

Direct Recording Electronic (DRE) Systems

The DRE machine is a recently developed type that performs similarly to a lever machine. However, it is constructed of electronic logic rather than mechanical components. In using a DRE machine, the voter sees a rectangular ballot display, (parties in columns and contests in rows, or vice-versa) as the voter would in using a lever machine. The DRE machine may be implemented so that the voter uses push buttons to indicate choices. In another implementation, the ballot may be seen by the voter on the face of a CRT display, and the voter may use a light pen to indicate choices.

As with a lever machine, the voter does not fill out and hand in a hard-copy ballot. The voter's choices are entered directly into the machine, and there is no ballot. Typical DRE machines are designed to give the voter feedback after a candidate selection is made. That is, after the voter selects a candidate, an indicator changes next to that candidate's name, to distinguish the choice from unselected candidates. The direct interaction with the machine also prevents overvoting. If the voter tries to vote for more candidates than is permitted for a contest, this action can be prevented by the machine.

When the voter has finished voting, he or she pushes another button or instructs the machine in some other fashion that the voting process is complete. Then, the choices made are added to the running totals for each candidate and issue alternative that have been retained as a result of the votes of all the previous voters who have used that particular machine. Once the voter has indicated completion of the voting process, no more votes can be added until a precinct official resets the machine.

A problem with DRE machines is that there is no real audit trail. That is, there is no original document filled out by the voter that can be used to verify the computer counts. A DRE machine can be conceptualized to consist of two parts: a data entry section in which the voter's choices are temporarily recorded, and a summarization section in which the running totals of the votes are kept. If each voter's choices were retained separately, a verification of the summarization section could be obtained by re-summarizing voters' choices on a different machine.

Typically, DRE machines are not designed to retain individual voter-choices sets. In this, they are designed like lever machines which, with the mechanical construction of the pre-electronic era, could not easily store digital data unless that data could be converted to an analog form. However, in the electronic era, voter-choice sets could be retained on magnetic media, although it would be necessary to provide a means of scrambling them out of sequence, so that a voter could not be associated with his or her voter-choice set.

One way of scrambling the storage locations of voter-choice sets is to select a location based on a random number. The random number can be generated by using the time that the voter takes in voting, starting from the machine's reset by the precinct official and ending when the voter pushes the "complete" button. If the time that the voter takes is counted out in milliseconds, the fraction of a second remaining when the voter completes the process will be sufficiently random, assuming that the average voter uses at least two minutes. In addition, if the counter generating the random number is automatically reset to zero after the number is used to store the voter-choice set, the random number is not determinable again. The number was not created by an algorithm in the computer program, and a review of the computer program in the DRE machine could not be used to identify a voter with a voter-choice set.

While a recount on an alternative machine provides redundancy for the summarization section of the DRE

(continued on p. 8)

(continued from p.7)

machine, no redundancy is available for the data entry section. The data entry section must be exactly correct and it must be trusted. It is often suggested that the data entry section produce, for the voter, a printout stating how the voter voted. This printout may be incorrect; the voter may be told on the printout how his or her votes were cast, but the data entry logic may be designed to cast the votes in some other way. Unless the internal logic is known to be correct, the truth of the printout cannot be known.

A statistical verification of the correctness of a DRE machine is not easy. In a ballot-tallying machine, a large number of predetermined ballot images (taken off a magnetic tape) may be entered directly as electrical signals in replacement of the ballot reader output to verify the ballot-tallying logic of the machine. Once the ballot-tallying logic is verified, a large number of predetermined ballots may be used to verify the ballot reading accuracy. With a DRE machine, a large number of voter-choice images may be similarly entered into the summarization section in replacement of the output of the data entry section. However, the input to the data entry section is from human action, and to verify its operation, considerable human effort would be required, or a mechanical replacement of the human action would need to be used.

An advantage of DRE machines over lever machines is that write-in voting could be made considerably easier. An alphabetic keyboard could be provided with each machine, and a write-in line could be provided with each contest. Then, if a voter selects a write-in line, the machine could then request that a write-in name be provided through the keyboard.

DRE machines, like lever machines, must be used serially by voters, that is, voter-by-voter. Consequently, it would be advantageous to have more than one in a precinct. However, DRE machines are small computers, so that it might be quite expensive to provide several to each voting location. Thus, the possibility of waiting lines of voters arises, a situation that does not arise with punch card or mark-sense voting.

Precinct-Count Versus Central-Count

Systems using lever and DRE machines must be precinct-count systems, that is, votes are cast and summarized at precincts, and only grand totals are produced centrally. Punch card systems may be either precinct-count or central-count. In precinct-count systems, individual computers with card readers are located at precincts, and precinct summaries are centrally totalled. In central-count systems, there are no computers in the precincts. Punch card ballots voted at precincts are collected but not counted locally. Ballot cards are transported to a central location where they are counted. Mark-sense systems, theoretically, could be either precinct-count or central-count, but almost all mark-sense systems are precinct count. Individual computers with mark-sense readers are located at precincts where voting and local summarizing are done. Grand totals are produced centrally.

Some automation has been undertaken to enable precinct summaries to be machine-readable. Typically, the precinct summary is stored in a removable memory at the precinct machine. After the polls are closed, this memory is removed and physically transported (or the data in the memory is telecommunicated via modem and phone) to a central location. The data are copied electronically into the memory of the central machine. Often, this process is unofficial, and solely for the purpose of obtaining a quick tally on election night. With less need for haste, once unofficial results have been reported to the media, the printout of the results obtained at the precinct machine is carried to the central location, and a more manual process is used to generate official results.

With precinct-count systems, considerably more individual computing machines are required. These machines, individually programmed for the ballot style in their respective precincts, must be delivered to the precincts the day before the election or before the polls are opened on the day of the election. In general, these machines receive their programs on removable memories that were programmed from a central machine. There must be certain security concerns in delivering the machines to remote or unpoliced locations where the machines might be subject to tampering. With many machines, maintenance, as well as security, is an important factor.

In central-count systems, prime vulnerabilities are in the processes of distributing the blank ballots and collecting the voted ballots. Controls must be in place to assure that the blank ballots are fully accounted for, and that the voted ballots are not tampered with in transportation. In a central-count system, all counting is typically done on one or two very large processors with several parallel reading stations. This centralization implies that it is fundamentally important that the counting program be correct, and that the ballot-reading process be accurate.

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 fax at (410) 997-4355, or by phone at (410) 730-4983.

The Evolution of Internet Voting: Mapping the Future of Democracy

by Victor Woodward[*]

This essay from VoteHere.net concludes that poll-site Internet voting is viable today, noting that some states may adopt remote voting as early as 2001. VoteHere.net is currently in the certification process with certain states and expects to have systems approved in 2000 for binding elections.

Introduction

The transition from punch cards to one-click voting is rapidly approaching. Industry analysts predict the 2000 election may be the last presidential election to only offer in-person voting and absentee ballots. Many voters are ready to embrace digital democracy and see Internet voting as a natural next step in electronic elections technology.

However, before you envision yourself sitting at your home-office PC pushing a button and casting a ballot, it is important to understand that most of the world's major innovations did not happen overnight. They went through a series of trials and tests and stages of acceptance. The adoption of Internet voting for public elections will follow this same phased approach. Internet voting systems must pass stringent certification tests, administered by independent testing authorities before they are used in public-sector elections. In response to the challenge of creating an Internet voting system that can both meet certification standards and be practical for use in public elections in the near future, we have charted a four stage approach for introducing online voting into elections.

Four-Stage Approach

This four-stage approach to the implementation of Internet voting is similar to what was recommended by the California Internet Voting Task Force. Each stage of the process represents a different type of voting system, each more technologically advanced than the last, and requiring a more complex relationship between security and convenience, but also providing increased convenience and service to voters. The four evolutionary stages are:

Stage 1 - Internet voting at polling places
Stage 2 - Internet voting at public locations
Stage 3 - Remote Internet voting for special groups
Stage 4 - Remote Internet voting from any Internet-connected computer

1. Internet voting at polling places: The simplest Internet voting system will allow voters to cast a ballot from existing poll-sites over the Internet. This basically involves setting up computers at poll-sites as an alternative voting device to whatever system is conventionally employed. This type of Internet voting system would have clear advantages over conventional systems. First, voters in the area could vote at any poll site and still receive the correct ballot. This would allow the voter to choose from hundreds of polling places, including ones that may be closer to home, work or school. Second, it would speed up the vote canvass because the ballots would be transmitted directly to the central authority instead of being held in the machine for transmission after the close of the polls. Third, it is more cost effective. Affordable Internet appliances will be able to replace old-style election equipment, which is expensive to purchase, maintain and store.

2. Internet voting at public locations: This stage would involve allowing voters to cast their ballot from an election official controlled computer or Internet appliance. This type of system would allow election officials to make better use of community resources that are already in place by taking advantage of computers and Internet connections at public places such as libraries, business/computer centers, schools, and community centers while still maintaining control over the voting machine. This phase of Internet voting provides increased service to voters by increasing access and convenience through additional voting sites.

3. Remote Internet voting for special groups: This stage would allow voters who traditionally have not been able to participate in elections to do so. This includes military personnel, residents in retirement homes, disabled persons, satellite office employees whose homes and businesses are in another city, state or country, and absentee voters. Voters would be required to request authorization for Internet voting in advance so they can be given authorization credentials for use at the time of voting.

4. Remote Internet voting from any Internet-connected computer: The final phase of Internet voting will allow

(continued on p. 10)

(continued from p. 9)

voters to cast their ballot from any Internet-connected device worldwide. Voters will be authenticated with a password and digital signature provided by their county election official. On the back end, a secure, certified election system would be used to collect the ballots and tally the election using a multiple authority tabulation method.

Widespread adoption of online voting will follow a phased approach. That is not to say that this is a path that will not vary in its course. Counties and states in the U.S., as well as international democracies, have different timelines, guidelines and regulations for upgrading voting systems and enabling Internet voting. Some may closely follow the four-step approach, while others may take a progressive stance and move more rapidly towards remote voting since it represents the greatest value for their constituents.

Conclusions

In fact, poll-site Internet voting is viable today. And some states may adopt remote voting as early as 2001. VoteHere.net is currently in the certification process with certain states and expects to have systems approved in 2000 for binding elections. The first steps towards the "future" of voting have been taken and the journey towards digital democracy has begun.

Victor Woodward is Vice President of Business Development and Marketing with VoteHere.net. He has a track record of growing successful start up companies. He started and grew the U.S. operations of Firefox, Inc. (NASDAQ FFOX) for two years before shifting to Senior Vice President of Sales for the company through the IPO process. Mr. Woodward received his Bachelor of Arts in Environmental Studies from the University of California Berkeley and completed the Stanford Executive Management Program.

Internet Voting: U.S. Market Intelligence Study, Part II

(continued from p.6)

Replacement System - Plans to implement touch screen system for early voting for November 2000 election, then expand to election day voting. Preference for a touch screen system. Registrar previously implemented touch screen system in Washoe County (Las Vegas), Nevada. Hired by Santa Clara County for experience in implementing electronic voting systems and early voting. Does not favor mark-sense systems due to higher expense, increased carrying difficulty, less accuracy than punch card. "You might as well stay with punch cards if you are going to use paper ballots."

Internet Voting - Concern about equal access. Open to testing Internet voting for a mock election in November 2000. Favors idea of schools utilizing voting system computers. Estimated timetable for Internet voting in a real election in Santa Clara County is 5 years.

State of Florida

Certified Systems - Punch card, mark-sense, and traditional DRE. No traditional DRE systems have been sold in Florida. No touch screen systems are currently certified. Touch screen vendors have been attempting to obtain Florida certification for 3 to 4 years.

Voting System Replacement Trends - Replacement has been in the direction of punch card to mark-sense. Some counties would prefer a touch screen system, but none are currently certified.

Early Voting - Referred to as in-office voting in Florida. Allowed during the two weeks prior to election day. Absentee mail-in voting is under 10% in the counties interviewed, but is expected to grow as more campaigns use absentee voting as a way to ensure that their supporters have voted.

Current Voting Systems -

Current Voting Systems in Florida
For Election Day Voting

	#	%
Punch Card Ballots	27	40
Mark-sense Ballots	37	55
Mechanical Voting Machines	2	4
Manually Tabulated Paper Ballots	1	1
Total	67	100

Other: The average number of registered voters per precinct is 1300 to 1500. There are no legal constraints on precinct size. Vendors often obtain Florida certification, then sell their systems in other states. Florida is considered the gold standard of state voting system certifications. Florida voting system standards were developed by the same consultant who assisted in the development of FEC voting standards. Internet voting may be possible as a ballot delivery system under current election code. Locational voting, whereby voters can vote at any site regardless of where they live, is under discussion. Locational voting would

require a ballot delivery system to provide the voter with the correct ballot on a touch screen or in hard copy form.

Florida Counties

Broward County

Election Official - Supervisor of Elections

Current System Status - Votomatic punch card system with central count tabulation. Time and labor intensive to load Votomatic ballot pages, and to transport voted ballots to central office for vote tallying. Hanging chads cause different election results when ballot cards are recounted.

Barriers to System Change: The Supervisor of Elections has recommended replacement of the voting system since 1993, but the Board of County Commissioners will not approve a new voting system.

Criteria for New System: Security, voter confidence, user friendliness for voters, and ease of use for poll workers.

Election Costs -
Average cost per election: $500,000
Average cost per registered voter: $.60

Replacement System - Preference for mark-sense system because "You know exactly where the mark is and pencil marks don't fall off the paper." Touch screen systems lack an audit trail, but save in printing costs. However, with the high cost of touch screen systems break even vs. ballot printing will take many years.

Internet Voting - Does not foresee Internet voting in Florida in the near future due to Florida's reputation for slowness in approving new voting systems. Estimated timetable for Internet voting in a real election in Broward County is 5 years.

Dade County

Election Official - Supervisor of Elections

Current System Status - CES punch card with central count tabulation. Satisfied with punch card system, but may be forced to change due to capacity constraints on ballot length and multiple language requirements. Punch card system is easy for voters and has no requirement for electrical power. Disadvantages are hanging chads and slowness of tallying election results. Supervisor of Elections prefers central count as he does not trust poll workers to handle in-precinct tabulation.

Criteria for New System - Ability to continue voting in a power outage, easy for voters to understand, cost.

Election Costs -
Average cost per election: $800,000
Average cost per registered voter: $1.00

Replacement System - With mark-sense systems light markings cause misreads. Mark-sense systems use more paper than punch cards, and are used with in-precinct counters. Mark-sense systems are easy for voters to understand. Touch screen systems present a concern in power outages.

Internet Voting - Internet voting offers fast results, minimizes set up time and errors, and reduces labor requirement. Concerns about security, vote secrecy, and ease of use for voters. If an Internet voting system is certified in Florida, the Supervisor of Elections would consider implementation for absentee or small-scale in-precinct election after 2002.

Hillsborough County

Election Official: Supervisor of Elections

Current System Status: CES punch card system with central count tabulation. Punch cards are accurate, but labor-intensive, slow, and allow over and under voting. Hanging chads are a problem in recounts.

Barriers to System Change: Favors a touch screen system, has held open houses for poll workers to demonstrate touch screen technology, but is not ready to proceed with a purchase recommendation. Changing voting systems is a huge undertaking and should be done in a low turnout election. Would like to change voting systems in the next 5 to 6 years.

Election Costs:
Average cost per election: $300,000 to $350,000
Average cost per registered voter: $.85 to $.76

Replacement System: Preference for a touch screen system, but preliminary cost estimates of $10 to $12 million make it a pricey system. Advantages are cost savings through consolidation of some precincts and convenience of allowing voters to vote outside their assigned residential precincts. Disadvantages are lack of paper ballot backup and voter education.

Internet Voting: Targets existing voters, therefore no increase in turnout. Internet voting must be available to all. "Voting systems should be the great equalizer." Does not favor making voting system computers available for classroom use because of suspicions regarding tampering with the voting system. Other

(continued on p. 12)

(continued from p. 11)

concerns with Internet voting are lack of community experience and potential for problems if voters have difficulty logging onto the Internet on election day.

State of Illinois

Certified Systems: Punch card and mark-sense. DRE voting systems are not allowed under current Illinois election code. An effort is currently underway to pass a bill to allow DRE systems, but the results of this effort are not known at this time. An additional bill that provides for a more generic authorization of voting system technologies is scheduled to be drafted. This bill may allow Internet voting.

Voting System Replacement Trends: Replacement has been in the direction of punch card to mark-sense.

Early Voting: Not currently allowed in Illinois. Traditional mail-in absentee voting is only allowed with one of 6 approved reasons and therefore tends to be under 5%. Expansion of absentee voting and introduction of early voting are under discussion in Illinois, but no decisions are imminent.

Current Voting Systems:

Current Voting Systems in Illinois For Election Day Voting		
	#	%
Punch Card Ballots	102	93
Mark-sense Ballots	8	7
Total	110	100

Internet Voting: Congressman Jesse Jackson Jr. of Illinois has asked for an Internet Study Group, which will be made up of members of election organizations around the country.

Illinois Counties

Cook County

Election Official: County Clerk

Current System Status: Punch card with precinct ballot counters. Cook County and Chicago recently made the decision to purchase a new punch card system. Media and political groups wanted faster election results. Precinct ballot counters wearing out.

Barriers to System Change: Civic and watchdog groups wanted to maintain in-precinct counting. Touch screen systems are not currently allowed in Illinois. Cost estimates for touch screen systems ranged from $35 to $50 million per jurisdiction and do not provide a paper trail. Ballot size requirements exceed the capacity of mark-sense ballots on a single piece of paper. Highly charged political atmosphere, frequent last minute changes of candidates allowed on the ballot, and a history of election day problems.

Criteria for New System: Speed, minimize voter education, cost, longevity, and adaptability with election judges.

Election Costs:
Average cost per election: $5 million+
Average cost per registered voter: $3.85+

Replacement System: Cook County is changing from ES&S punch card with PBC 4.5 to ES&S punch card with PBC 2100. Primary differences are change from 312 to 456 punch positions, change to voter insertion of the voted ballot into the precinct ballot counter vs. insertion by the election judge, and wireless transmission of election results.

Internet Voting: Using only schools for Internet voting creates problems of too many voters in one polling place, and related security and parking difficulties. Potential difficulty transporting and installing classroom computers to gyms and cafeterias where the election judges can control them. Also limitation of electrical outlets in gyms and cafeterias. Other concerns are security, verification of voter identity, loss of information in a power outage, and loss of community contact. Start with in office absentee voting. Estimated timetable for Internet voting in Cook County is 5 to 10 years.

DRE Systems: The cost of DRE systems will fall in the next few years or the vendors will be out of business. The recent purchase of a DRE system for election day voting by Riverside County, California will be a good model for other jurisdictions.

Other: Cook County is one of the largest election jurisdictions in the U.S., with some of the most complicated elections.

Lake County

Election Official: Supervisor of Elections

Current System Status: Punch card with central count tabulation. New voting system for 2001 necessitated by punch card capacity limitations. Desire to cut labor and printing costs, card readers are not reliable, replacement parts are difficult to obtain.

Criteria for New System: Accuracy and integrity, cost, and ease of use for voters and elections judges.

Election Costs:
Average cost per election: N/A
Average cost per registered voter: N/A

Replacement System: Proponent of mark-sense system. Cost savings through reduced printing and labor costs. Mark-sense enables one ballot image to be used for the sample ballot, the election day voting ballots, and absentee ballots. Eliminates the need to print, crimp, test and load Votomatic pages. Eliminates the need for a dedicated voting booth and vote recorder. Ease of use -- "Every voter knows how to pick up a pen and fill in an oval." Informs voter of overvoting. Anticipated new system cost =$2million.

Internet Voting: All townships in Lake County have T-1 lines. Internet voting should employ GIS to assign ballots and distribute results. The ability to offer features that address Americans with Disabilities (ADA) issues would support the use of technology in voting systems. Illinois is conservative and may be the last state to have Internet voting.

In the JULY 2000 issue – conclusion of the Marketing Study, Part III. Selected counties in New York and Texas.

Interactive Glossary: An Introduction

coordinated by Ed Gerck, Ph.D.

This new monthly section begins an interactive glossary project with the readers. Definitions will be discussed before they are entered into the glossary. The underlined sentences represent proposed definitions for discussion. Comments are welcome.

We begin by discussing the definition of identification –what should we understand by identification in Internet voting? This discussion follows a line of reasoning first presented by Ed Gerck in 1998 [1], with the objective of defining identification without a circular reference to identity.

Identification is often understood as an act of identifying, or of establishing an identity, which is a circular definition. On the other hand, identity is usually defined in dictionaries as "the distinguishing character or personality of an individual" – which is comparative rather than affirmative.

In addition to the above, there are other shortcomings when such definitions are applied on the Internet. Why? Because any mention of "identity" on the Internet is a mere "name" for something else –for example, you may think you are talking to "Doris" but "she" is really Boris ... a computer. On the Internet, you can only control your end of the connection, not the other end and not even the path between you and the other end.

Identification is also a difficult problem in the real-world, outside the Internet. On 15th April 1997, The Daily Telegraph, a well-respected UK newspaper, reported on Alan Reeve – a convicted criminal and triple killer who was described as "friendly, caring, dependable and loving" by his fiancée when he was arrested under false identity in Ireland.

Clearly, the indeterminacy of "identity" in the real-world is by itself a reason to doubt extending such credentials to the Internet. Moreover, on the Internet, we also need to identify hosts, routing, software, etc. –not just humans.

What is the solution, if any? As given in [1], we need to revisit the concept of identification– what is identification, that we can identify it? To fulfill this goal, our methods should apply to Internet protocols as well as to non-Internet communication modes (e.g. personal).

What does it mean "to identify"? To identify is to look for connections [1]. Thus, in identification we look for logical or natural connections. For example, connections:

- between a fingerprint and the person that has it,
- between a name and the person that answers by it,
- between an Internet host and a URL that connects to it,
- between an idea and the way we can represent it in words,
- conversely, between words and the ideas they represent,
- etc.

Do you, the reader, agree that to identify is to look for connections? If you do, you have just identified. If you do not, you have also identified. The essence of identification is thus to find connections –where absence of connections also counts.

Identification can thus be understood not only in the sense of an "identity" connection, but in the wider sense of "any" connection. Which one to use is just a matter of protocol expression, need, cost and (very importantly) privacy concerns. Thus, as further defined in [1], identification is a measurement of coherence – where coherence is a natural or logical connection as defined in dictionaries.

[1] www.mcg.org.br/coherence.txt

Internet Voting Technology Alliance

The IVTA Opens Online Discussions

As agreed at its Founding Assembly, the IVTA is opening online discussions for technical issues in Internet voting and internal administrative topics. The charter for each listserver is available at the web site http://www.ivta.org. Two listservers will be available at the end of May. To subscribe to the technical forum send an email to majordomo@ivta.org with body 'subscribe tech'; to subscribe to the administration forum send with body 'subscribe adm'; or visit the website.

Media Watch & Links

(These and more links are available online at THE BELL website – www.thebell.net)

Bills to Protect Privacy Need Public Support
You can almost feel privacy gaining strength as a public issue. The Internet Age has opened people's eyes, because people are beginning to see the consequences when all kinds of data ends up in databases that are open to anyone with sufficient cash.
http://www.mercurycenter.com/svtech/columns/gillmor/docs/dg032800.htm

Cybersnooping Reaching Down to the Keystroke
Welcome to the world of cyber snooping. Because there is software now available - for as little as $99 - that can track your ``raw thoughts'' through keystrokes. So the memo you thought went into cyber never-never land actually ended up being captured and sent to the supervisor.
http://www.sjmercury.com/svtech/news/breaking/merc/docs/085400.htm

U.K. Plan to Open Internet Spy Center Draws Criticism
(CNN) -- The United Kingdom Home Office is responding to the concerns of civil liberties groups over a government plan to open a facility designed to intercept and monitor Internet traffic, including e-mail and encrypted messages. A report in the Sunday Times of London said the 25 million pound center will have the power to tap incoming and outgoing Internet traffic from Britain and that major Internet service providers are providing hardwire links to the surveillance station.
http://www.cnn.com/2000/TECH/computing/05/01/british.spy.building/index.html

Netscape Tests Patches for Security Hole
Netscape is testing patches for a newly discovered security hole in its Communicator Web browser that could expose private files. The vulnerability lets a hostile Web site glean private information from a visitor, including but not limited to that visitor's bookmarks.
http://news.cnet.com/news/0-1005-200-1717169.html

Microsoft Browser Bug May Access Private Files
Microsoft is looking into a newly discovered security hole in its browser that could expose people's private files to malicious Web site operators.
http://news.cnet.com/news/0-1005-200-1717460.html

Microsoft, Netscape Squabble Over Browser Scripting Hole
Microsoft and Netscape Communications are pointing fingers at each other over a browser-related security problem that neither company has any intention of fixing.
http://www.nytimes.com/cnet/CNET_0_4_1820959_00.html

Doctors Shaken to Find Personal Data on the Web
Fremont family doctor Susan Hsu rarely gives out her home address, but she made an exception to receive her license and other mailings from the California Medical Board. Little did she know that information would later be sold by the board and posted on the Web.
http://www.sjmercury.com/svtech/news/indepth/docs/priv041700.htm

A Rogue Software Program Attacks Computers Worldwide
A rogue software program, borne by an e-mail message proclaiming "I love you," propelled itself around the world yesterday, jamming and crashing e-mail systems and destroying data on hundreds of thousands of computers.
http://www.nytimes.com/library/tech/00/05/biztech/articles/05virus.html

Experts Estimate Damages in the Billions for Bug
A new virus sweeping through computer systems today will likely be the most costly yet, analysts said.
http://www.nytimes.com/cnet/CNET_0_4_1814907_00.html

Survey Shows Few Trust Promises on Online Privacy
Trust in the Internet industry, it seems, does not run deep among the online masses. A notable 92 percent of online households agree or agree strongly with the statement, "I don't trust companies to keep personal information about me confidential, no matter what they promise."
http://www.nytimes.com/library/tech/00/04/biztech/articles/17data.html

Why Not Internet Voting?
Another obstacle to online voting is that each political party may fear an increase in voting convenience will benefit the other party. Oregon took a decade to implement vote-by-mail, and Pennsylvania isn't anywhere near there yet, because of skepticism by citizens and concern by elected officials that their jobs may be endangered by any new system.
http://www.seventy.org/news/netvote.html

Internet Explorer "Open Cookie Jar"
Any Web site that uses cookies to authenticate users or store private information -- including Amazon.com, HotMail, Yahoo Mail, DoubleClick, MP3.com, NYTimes.com, and thousands of others – could have cookies exposed by Internet Explorer and intercepted by a third-party Web site.
http://www.peacefire.org/security/iecookies/

Graphic, Visualization & Usability Center's Seventh WWW User Survey
The GVU survey asked questions regarding electronic privacy, security of transactions, information gathering behavior and Internet banking.
http://www.gvu.gatech.edu/user_surveys/survey-1997-04/

Internet Voting: Proceed Cautiously
After studying the issue for nearly a year as members of California Secretary of State Bill Jones' Task Force on Internet Voting, we have come to recommend great caution in any move toward Internet voting.
http://www.sjmercury.com/premium/opinion/columns/e-voting.htm

BOOK REVIEW: Losing Privacy in the Age of the Internet
DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY by Simson Garfinkle (O'Reilly & Associates, $24.95) Simson Garfinkle details insidious threats to privacy that arise from the Internet, from public and private surveillance cameras, from biometric devices and medical technology, from spy satellites and computer chips, and above all from the unrestrained gathering and unauthorized sharing of personal information through computer databases.
http://www.nytimes.com/library/tech/00/02/circuits/articles/10revu.html

Links

CORRECTION: The link listed in the May 2000 issue for the Federal Voting Assistance Program was incorrect. Carol Paquette (FVAP) kindly provided the correct URL – http://www.fvap.ncr.gov

Democracies Online - http://www.e-democracy.org

Federal Election Commission - http://www.fec.gov

Hacker's Dictionary - http://www.tuxedo.org/jargon

League of Women Voters - http://www.lwv.org

Opensource.org - http://www.opensource.org

Operation Opt-Out - http://opt-out.cdt.org

Privacy.net: The Consumer Information Organization
http://www.privacy.net

RSACryptoBytes Newsletter
http://www.rsasecurity.com/rsalabs/cryptobytes/

From Our Readers

(continued from the first page.)

"Enjoyed the first issue of The Bell. Internet technology is becoming so pervasive that in the next decade it will touch on and affect most aspects of people's lives. The focus of The Bell on Internet voting uniquely facilitates practical discussions (on such topics as privacy, security, trust and related policies) which are desperately needed to prepare for this eventuality."
- Don Mitchell, Dunn Loring, Virginia

"The Bell (Kolokol) was the name of the newsletter published by Alexander Herzen in the 1850s. Herzen was an advocate of the Russian peasant commune pre-emancipation of the serfs. While I consider myself internet technology savvy, one of the intriguing things about what these folks [at The Bell] are on to, as I am coming to realize, is that the technology issues of voting on the internet are generally not at all understood. It looks like they may be able to play a very useful educational role."
- Gordon Cook, Editor of The COOK Report on Internet

"Writing about the new internet voting newsletter, Ed Gerck explained that in naming it "The Bell" .... 'the idea was to use the image of a bell because mission bells were used in colonial California for telling time, announcing events, and for passing on news from one city to another.' And perhaps subliminally there was, romantic tho' it be in these internet speed times, the bell-associated ideal of liberty, even if occasionally cracked in practice."
- Michael Krieger *on Internic's Domain-Policy list*

"Thank you for the copy of your first edition. I read it with interest and found it very interesting and informative.... Good luck with the publication."
- Richard Kimball, Director, Project Vote Smart

"Very good newsletter. I would love to continue to receive it."

"I found "The Bell" quite informative."

We thank our readers for their comments and apologize for not being able to include them all.

THE BELL™ Newsletter on Internet Voting

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

FIRST-CLASS MAIL
896
U.S. POSTAGE PAID
SAN RAFAEL, CA
PERMIT NO. 1

DATED MATERIAL
Please Expedite

Would You Vote Naked? See p. 3

To enter your FREE monthly subscription, use the form below.

cut here ORDER FORM cut here

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

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_____

[ ] FREE – in PDF format sent to the above e-mail address and/or

[ ] $30.00 – in printed format sent to the above mail address.

[ ] PAY BY CHECK OR MONEY ORDER Make check or money order payable to Safevote, Inc.

[ ] PAY BY CREDIT CARD Complete the information below.

[ ] Visa [ ] MasterCard [ ] Am Express [ ] Dinners [ ] Discover [ ] MasterCharge

Card Number_____ **Expiration Date**_____

Signature_____ **Print cardholder's name**_____

INSTRUCTIONS: Mail completed order form to the address below. Allow two weeks for processing.

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