The Bell™

Privacy, Security and Technology in Internet Voting

SEPTEMBER 2000 | Published Online Monthly | Vol. 1 No. 5

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.

Coming Issues

- The Private Sector, Part IV
- Internet Paradigms
- Cryptography
- Internet Voting FAQ

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.

Open Source Discussion

This issue presents two articles and a commentary on open source software. The articles discuss the different meanings of "open source" and the significance of these concepts to Internet voting, especially in the public sector. The commentary suggests that openness should include not only open source software but also open peer-review of voting standards, where vendors, developers, experts, government sectors and the voters themselves may make contributions and provide oversight. **THE BELL welcomes contributions on different perspectives, including closed source software.**

(continued on pp. 5, 7 and 9)

A Step Toward Internet Voting

As reported last month, the State of California will conduct a shadow election test this November, as a step toward Internet voting in public elections. The test period will be from October 30 to November 3. THE BELL is extending an invitation to all participating companies to present a report.

The Private Sector Won't Wait, Part III

Comments from companies interviewed for this study provide additional insight into the market and the motivation, or lack thereof, for enhancing privacy and security safeguards in proxy voting.

(continued on p. 11)

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:

I regret that this September issue was late. The delays were caused by problems in our out-sourcing chain. We expect future publications to be on time, published by the second week of each month.

Open source software is one of the main topics in the current issue. How does this relate to Internet voting? Using open source software for Internet voting raises the bar in many areas critical to the integrity of an election. Consider recounts, for example.

Recounts today generally consist of running a vendor's proprietary software on the same machine used for the election and getting the same results as those produced on election night... hopefully. Of course, if you run the same software on the same machine and get the same results, all you have demonstrated is that the software is counting consistently, not necessarily accurately. In other words, there is no independent verification of election results by another system.

With open source software, there are several options for verifying the accuracy and integrity of vote totals. Open source software can be run with different compilers or on a machine with a different CPU and you should get the same results. (A compiler is a computer program that converts human readable source code into the 1s and 0s of machine executable code.) Some of today's voting systems use specialized compilers which could contain malicious code, for example. Furthermore, because open software has been subject to public scrutiny and peer review, it should be trusted more by both the public and election officials to begin with.

The point I am trying to make is based on what we believe here at Safevote – that security should be based on diversity and comparison. You should be able to compare the results produced by diverse systems running the same open source election software and they should be the same. The current security model in public elections is based on security through obscurity and the principle of confinement. Each vendor essentially says that there is one (private) voting system to count the votes and it's the best one – the "trust me" treatment.

Recounts are not the only part of the election process that may benefit from open source Internet voting software. Security is another – for the reasons outlined in the articles in this issue. And let us not forget that the open peer review paradigm should *also* be applied to the process of designing and developing voting *standards* themselves. Standards developed behind closed doors will do little to inspire public confidence in Internet voting.

Internet voting encompasses a wide variety of overlapping technical components. Open source software is just one of them. However, each technical component will have a specific impact in the real world of election procedures. Thus it is imperative that we understand the consequences of the technological choices we face in Internet voting. Therefore, THE BELL welcomes contributions on different perspectives, including those in favor of "closed source" software.

The Interactive Glossary, IVTA and Media Watch sections will resume next month, allowing more space in this issue for the articles.

Eva Waskell, Editor
Communications Director
Safevote, Inc.

Realizing the Potential: Associations and Online Voting

by Dr. Bruce L. Egan[*]

Dr. Egan, a member of the Board of Directors of election.com, describes the benefits of Internet voting in the private sector, focusing on associations. He concludes that online voting will seem as normal a few years from now as buying books or booking airline flights are today.

What will be the seminal political event of the year 2000? The easy answer, as in any year divisible by four, would be the outcome of this fall's presidential election. Yet when the time comes to look back, there's a case to be made that the most significant event in the 2000 election season happened in March, not November, in cities and towns across Arizona.

Why Arizona? Because that's where the first-ever Internet vote took place in a binding political election – in this instance, that state's Democratic primary. While the outcome of any maiden effort can never be conclusive, the Arizona experience, which saw voting turnout surge over 600 percent above 1996 levels, suggests that online voting may well change the way we think about democracy in America. Call it the ultimate "democratizing" effect of the Internet, a network that brings down traditional barriers to information as a source of privilege and power.

While the public benefits of online voting are significant – not to mention newsworthy – it is the *private* sector that may ultimately reap the everyday benefits of Internet-based elections. More and more associations, for example, are outsourcing their elections and exploring the benefits of online voting.

Associations count on their members to cast ballots several times a year, whether it's a vote for the group's president or a move to ratify new charter amendments. But, interestingly enough, many member organizations view group votes as "necessary evils." Internal elections are complicated processes involving numerous voter lists, member authentication, ballot preparation, printings, mailings, tabulations and results reporting.

And in addition to logistical hassles and exorbitant overhead costs, association elections typically yield disappointing results. Low voter turnout is the unfortunate norm, since motivating a significant member base to cast ballots by mail or in-person is no easy task.

For some associations, elections can result in even more complex problems. Certain groups, for example, have staged elections that proved contentious, rife with accusations of fraud and illegal voting practices. After all, administering one's own balloting leaves an organization vulnerable to accusations of bias or vote tampering.

For all of these reasons, many associations are turning to outside election firms to free themselves from the hassles of conducting internal elections. Outsourcing lowers administrative costs – election companies blissfully take care of the list management, balloting, mailing, printing, tabulation and reporting for the association. Furthermore, for those groups facing potentially contentious elections, outsourcing assures constituents and detractors that member votes are run fairly, with no possibility of tampering or intervention by staff. This unbiased, third-party credibility can mean a load off the minds of association personnel.

Better still, those organizations that complement their paper ballot elections with online voting capabilities further reduce costs and increase participation. When thinking of online elections, just consider the high costs of printing and mailing ballots and the relatively low return.

On the Internet, mailing costs disappear and members have the added convenience of voting at work from their office PCs, at the local library or even at home in their pajamas. One recent association that migrated its election online increased voter participation five fold, producing truly representative results.

The move toward online voting fits within the larger corporate trend of outsourcing any function that isn't core to an organization's business. Look at the rise of firms that specialize in administering 401k plans, payroll processing and business tax transactions for nearly half a million companies and over 28 million employees – freeing its client companies to concentrate on what they do best. Now this trend is moving into membership groups as more and more private organizations outsource their internal elections to firms that can perform those functions more efficiently and effectively by using online voting.

As Internet usage continues to spread and time online increases, online voting will seem as normal a few years from now as buying books or booking airline flights are today. We live in an era when the Internet offers a degree of choice and freedom that would have seemed unimaginable just a few years ago. How fitting that the very emblem of individual choice – the vote – is now being extended electronically to more and more decisions, in the private sector as well as public.

Dr. Bruce L. Egan is an economist and Senior Affiliated Research Fellow at Columbia Institute for Tele-Information (CITI) at Columbia University and is the author of *Information Superhighways Revisited: The Economics of Multimedia*. He is also a member of the Board of Directors of election.com.

From Our Readers

From Gail L. Pellerin, Elections Manager, Santa Cruz County, CA

After I read the first issue, I felt compelled to subscribe.

Everything is going in the direction of the Internet, including public elections, and I find The Bell a useful tool in keeping up to date with news and information in the area of Internet voting, especially as it relates to election procedures. However, security concerns have to be addressed.

From Kathy E. Van Wolfe, Elections Administrator, McLennan County, TX

I'm always looking for ways to better serve the public so I try to stay abreast of anything having to do with elections. The Bell is very useful in that regard. I read it to find out what's going on in the world, what the new ideas are. We don't want to reinvent the wheel. But Internet voting will have to be made secure. There can't be dead people voting. And you have to be certain that only qualified voters can vote. These are big problems today and Internet voting will have to deal with them.

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.

Open Source and Open Software

by Thom Wysong[*]

Open source software and free software are terms that are often misunderstood. In this article, Thom Wysong draws upon over 15 years of experience in computer programming and concisely explains the differences and similarities between these two types of software.

Introduction

Two terms that appear with increasing frequency in the mainstream press are "open source" and "free software." Over the next few years, they will also be appearing with increasing frequency in the Internet voting, online democracy, and public election arenas. Open Source and Free Software - besides representing concepts - also represent communities of people, organizations, and resources.

What are Open Source and Free Software?

When a consumer purchases a word processing program, the discs in the package contain the instructions which tell the computer how to receive input from a keyboard, how to format documents, and how to check spelling. Normally, the discs contain these instructions in a form only the computer can understand - in computer-readable *executable code*.

There is another type of computer software gaining in popularity. With this other type of software you not only get a copy of the computer-readable *executable code*, but you also get a copy of the program's *source code*. This *source code* is the human-readable version of the computer instructions, which computer programmers used to create the program with.

Known as "open source" or "free software," these alternate types of computer programs are sometimes created by for-profit companies. It is more common, however, for open source programs to be created by a whole collection of people, usually all volunteer, who collaborate over the Internet. The software is then made available for everyone to download and use for free. Occasionally, one of these programs will become popular enough that not only do individuals contribute to its development, but companies and organizations do as well.

Why does it matter?

Advocates claim that "open source" and "free software" offer many benefits over "closed source," proprietary software. Among these benefits are quality, speed, cost, verifiability, and freedom.

Quality. The "open source" claim to increased quality rests on the "many eyes" principle. With this principle, the idea is that some software defects - known as "bugs" - are plainly visible to some people, but not to others. With this underlying understanding, it can be seen that a software program's initial developers may (and usually do) overlook some bugs in their code. With "closed source" software, this is a problem, since a small group of people is all that will likely ever see the program's *source code*. However, with "open source" software, the initial development group's blind-spots can be compensated for by all the other people who can look at the source code and spot defects which the initial developers missed. The idea is that with "many eyes," all defects can be spotted and fixed. The "many eyes" principle does not guarantee bug-free software, but it does help to reach that ideal.

Speed. Experience has shown that once a community of developers and users for any given piece of "open source" or "free software" reaches critical mass, that community begins to operate at Internet speed. New features are added to the software, new found bugs are fixed, and users can get their questions answered (for free) on the Internet - and all of this takes place at a faster rate than any "closed source" company can provide it. The open nature of the software *enables* and *empowers* the user community to take care of itself, instead of it having to be completely dependent on a particular company to provide all the solutions.

Cost. Since much "open source" and "free software" can be obtained for no cost, there is an obvious cost advantage up front. However, what is not always obvious is that this software still needs to be installed, configured, administered, and maintained. And all of these activities cost time and, possibly, money. Even though *maintaining* an "open source" system may be just as costly as maintaining a "closed source" system, the cost of *obtaining* that "open source" system will most likely be significantly less.

Verifiability. With open software, users get an extra measure of "peace of mind." Since *source code* is provided, organizations and individuals alike can perform audits on the code. These audits insure that the computer program is (a) doing what it's supposed to do and (b) not doing what

it is not supposed to do. *Source code* audits are necessary when security, reliability, and liability are issues. With "closed source" software these audits aren't possible, users simply have to blindly trust the software and the developers.

Freedom. Proprietary computer programs have a tendency to lead to users being "locked-in" to a specific vendor's "closed source" software product. This type of "lock-in" can lead to vendors charging clients a lot of money for upgrades or custom modifications. Since no one else has access to the *source code*, users either have to pay whatever price the vendor charges or entirely convert over to a different vendor's system - which can be even more expensive. However, with open software, users have the freedom to control their own systems. If "Vendor A" begins charging too much money for upgrades and modifications, or the timeliness and quality of support being offered by "Vendor A" becomes unacceptable, or if "Vendor A" goes out of business, then the user can simply switch to "Vendor B" or "Vendor C". What makes this situation substantially more attractive than the closed software scenario is that *the user can switch vendors, without switching software systems.* Since "Vendor B" and "Vendor C" both would have access to the *source code*, they would be able to provide upgrades, modifications, and support to the user's existing system, just as "Vendor A" was able to. But they may also be able to provide it with better timeliness, increased quality, or at a lower cost. Users, of course, are free to upgrade and maintain open software on their own - without the assistance of a vendor - if they have the ability and desire to do so. The bottom line is that *open software provides maximum flexibility and freedom by transferring control from vendors to users*.

Does this approach really work?

The Internet depends heavily on "open source" and "free software." Some excellent examples of Internet-related open software are GNU/Linux [GNU stands for GUN's Not Unix], OpenBSD [Berkeley Software Distribution], Perl, Apache, and Sendmail.

GNU/Linux (www.gnulinux.com), also known as "Linux," is probably the most well known piece of open software. The core of this operating system, known as the *kernel*, was initially developed by a Finnish college student back in 1991. Most of the rest of the operating system was already available at that time as part of the GNU Project (www.gnu.org/gnu/gnu-history.html). Since the early 1990s, hundreds of people from around the world have contributed to expanding and improving the Linux kernel. Not only is GNU/Linux popular with the several million individuals who use it, but it is becoming accepted in the corporate world as well. According to the market research firm International Data Corporation (IDC), of all the copies of server operating systems shipped by vendors, GNU/Linux is the only operating system which increased its percentage of market share between 1998 and 1999 (news.cnet.com/news/0-1003-200-1546430.html).

OpenBSD (www.openbsd.org) is another open operating system with a reputation on the rise. Unlike GNU/Linux, the OpenBSD developer and user communities are relatively small. However, on the Internet, OpenBSD is regarded as one of the most secure operating systems available. The volunteer development team, headed by a Canadian, prides itself on its proactive approach to security - which has resulted in OpenBSD being "secure by default." The team's reputation is such that the US Department of Justice uses OpenBSD to store and transmit their "most sensitive data" using "260 copies of OpenBSD," according to a recent article in The Standard (www.thestandard.com/article/display/0,1151,17541,00.html).

Perl (www.perl.com) is a computer programming language that has been called "the duct-tape of the Internet." Many, many businesses use Perl to add functionality to their websites, including Yahoo, CNN, and Amazon.com. Every programming language has a program to translate human-readable *source code* into computer-readable *executable code*. This translating program is itself a piece of software. Many of these translating programs are "closed source" software. However, Perl's is not. The source code to its translating program is openly available and is continually being updated by a world-wide group of developers.

Apache (www.apache.org) is an "open source" web server. When a web browser is directed by a user to retrieve a web page, the browser sends its request to a web server. The web server then sends the requested web page back to the browser. The World Wide Web is chock full of web servers. Every one of the 20 million active websites on the Internet has at least one web server. And, according to the most recent Netcraft survey, Apache powers *more websites than all other web servers combined*. It has consistently been the leading web server since April 1996. A group of volunteer developers from all over the world expand and improve the Apache Web Server on a continuing basis. The home page for the Apache Web Server is at www.apache.org/httpd.html.

Sendmail (www.sendmail.com) is, more or less, an electronic mailman. It is a program that transports email across the Internet and private networks. According to an article in Salon, an estimated 60% to 80% of the email which travels across the Internet is transferred by Sendmail servers (www.salon.com/21st/feature/1998/12/cov_11feature.html). Sendmail is also open software.

Forbes magazine realized that "open source" and "free software" were on the rise some time ago. They provided their readers with an excellent introduction on the topic as the cover story for their August 10, 1998 issue. That story offers BIND and Netscape's web browser as additional examples of open software. (www.forbes.com/forbes/98/0810/6203094a.htm)

(continued on p. 14)

Why Electronic Voting Software Should be Free Software

by Jason Kitcat[*]

Current computerized voting systems run (private) proprietary software, even though they are tabulating votes in public elections. An alternative software model is free software. What is that exactly? Read this article by Jason Kitcat and find out. The author lives in England and is an advocate of a non-proprietary model for Internet voting software.

Introduction

The electronic voting market is exploding – numerous existing and start-up companies have identified the huge revenue potential that the private and public markets offer, resulting in a raft of products and services being offered.

There has been considerable discussion both on- and off-line regarding the merits of electronic voting as whole, in addition to controversy over the validity of different technologies. However, there seems to be little public debate over whether proprietary software is the appropriate way to provide electronic voting in public elections or whether its use makes the best business sense in private implementations.

Before the electronic voting community and its onlookers make hurried assumptions over how this market should develop, I am keen to put forward the arguments for a non-proprietary model: Free Software.

For those unfamiliar with the movement as a whole, I highly recommend browsing the Free Software Foundation's site on the matter at http://www.gnu.org/philosophy/ . Within this article I shall be covering the merits of Free Software (sometimes known as Open Source – though they are not quite the same thing) only within the context of electronic voting.

Openness

A key benefit of releasing software under a Free Software license is openness. The (Internet-based) electronic voting community is only starting to take steps toward becoming more accessible and open through initiatives such as publication of The Bell. Being open is key to fostering trust and accountability – these are especially needed in the world of voting software.

The IVTA's recent commitment to open protocols is another positive step in the right direction, however (as I pointed out on the IVTA tech mailing list) it is no guarantee that the software that uses these protocols will be open or even that the software implements the protocols properly. But why should we want the software to be open at all? Two key reasons are security and observability.

Security

Many commercial electronic voting companies seem to rely on security through obscurity. They will not release detailed (or in some cases, any) technical information on how their voting systems work. From analysis that I have done, some of the guilty parties have good reason to hide their handiwork as their electronic voting systems are nothing more than trumped-up e-commerce systems that do not address any of the major security, privacy or reliability issues that we as a community are working to solve.

We all know that the only way to guarantee security is through peer review and careful auditing by professionals. The IVTA encourages this with open protocols, and I support that whole-heartedly. However, there are programs we could all nominate for not properly implementing freely available, publicly ratified, standards. Only Free Software, with the access to source code that it unequivocally upholds, enables anyone to verify (and repair) implementations of protocols. In other words, "many eyes make bugs shallow."

Access to the source code also allows for the easy addition of new protocols whether for secure vote recording or voter authorisation (for example, FREE's security model allows for the easy addition of new identification devices such as smart cards or retina scanners).

The FREE e-democracy project strongly feels that the slightest hint that privacy or security could be sullied by electronic voting systems may permanently damage the likelihood of such technologies being widely accepted in the public sector. Only full and permanent to commitment to a culture of openness will effectively counter such threats.

Observability

Free Software creates openness by allowing anyone to use the software, read the source code, modify the program and pass it on. People get involved and are naturally encouraged to learn how the programs work. This fosters a culture of observability where programmers expect their Free Software code to be read by a multitude of users with skills exceeding or way below their own. The result: programmers are careful to comment their source code and constantly evaluate the quality of their programming.

Furthermore anyone with the skills (or the time and willingness) can check the code themselves – helping them to trust the system. Why would you trust a similar proprietary system when the creators won't tell you how it works? What could be hiding in there? Do they know about problems or weaknesses that I don't? The very act of hiding the information creates distrust – especially when the provider is building the system for personal profit and thus not necessarily with our best interests in mind.

Anyone could audit a Free Software voting system before it went into use to guarantee the absence of Trojan horses, hidden result manipulation functions or blatant weaknesses without having to sign Non-Disclosure Agreements and with the full ability to take their findings public and/or fix them if they were that way inclined.

Freedom

As Richard Stallman (founder of the Free Software Foundation) says: "think of 'free speech,' not 'free beer.' " Free Software licenses, especially the GNU General Public License(GPL), enforce basic freedoms and rights for users of the software. While there can be no denying the strong arguments for associating these freedoms with all software, I believe they are particularly apt in the context of electronic voting software. In my opinion, the two key freedoms worth discussing with regards to this subject are freedom from dependencies and freedom from cost.

Freedom from Dependencies

Any county, state, country or organisation buying commercial electronic voting technologies is totally dependent on the strategy of the manufacturer. The company may develop the software in a direction different to one's own elections strategy or may simply refuse to provide the features you believe to be essential.

Take, for example, Iceland's struggle to get Microsoft to deliver Windows9x in their native Icelandic language. Alternatively consider the predicament users of Banyan Vines networking software were placed in when Banyan totally abandoned the networking market for e-commerce under the new name of epresence. Iceland risks being sidelined in the 'new economy' while Banyan users saw their massive technology investments become worthless. If the software had been Free Software they wouldn't have been in such dire situations.

No matter the direction, fortunes or internationalisation policy of your provider – if the software is Free Software it is totally modifiable. The user has the source code and so can develop the software however they want; thus investments in and commitments to technologies are protected. Free Software users keep control of their technological destinies.

Freedom from Cost

Thanks to the advertising of software associations and the scary licenses we get with software, we have lost the culture of sharing that once used to be a big part of the computing world. Even academics, who are dependent on the discourse and sharing of ideas that used to typify academia, now prefer to patent before sharing – if they ever do share.

Free Software lets you share, the way friends and neighbours should, without any legal repercussions. This isn't just about sharing with our neighbours in the next cubicle or building, this is about fellowship with our global neighbours. I believe we have a moral duty to empower any country to follow the (often twisted) path towards representative democracy – electronic voting may well be the best way for many countries to do so. But will commercial voting companies share their systems with less well off organisations and countries? Aren't they dependent on the income from software and associated services sales for survival?

We can share Free Software with whomever we want, wherever we want. And you can feel good knowing that license allows them to keep sharing that with whomever they want. It's a powerful thought.

One final note on the freedom from cost: Let me make clear that supporting Free Software does not mean opposition to commercial software and its developers. Software development is a good and decent way to make a living and despite what some argue, proponents of Free Software are not 'communists' against all forms of commercial activity. Furthermore, paying for Free Software is perfectly acceptable, but Free Software provides a viable (and my preferred) alternative to pure commercial licenses in the same way that shareware and public domain licenses do.

(continued on p. 15)

Reflections on the August 11 FEC Meeting

by Ed Gerck, Ph.D.[*]

Dr. Ed Gerck, CEO of Safevote, Inc., discusses questions involving open source and open protocols in Internet voting, and summarizes the suggestions presented by Safevote to the FEC. These reflections are based on experience with Internet protocols, where "open peer review" and "rough consensus and running code" have proved to be basic tenets for developing and defining standards.

Introduction

The Federal Election Commission (FEC) contracted the consulting firm American Management Systems (AMS) to update the voluntary national Voting Systems Standards of 1990. On Friday, August 11, there was a public meeting in Washington, D.C. with the FEC's project team and the National Association of State Election Director's (NASED) Voting Systems Board to discuss the current results of this work, which now goes back to AMS for consolidation and redrafting. According to the FEC, policy and technical representatives and all of the voting system vendors have been invited to participate in the meeting.

The updating and review process may take an additional year and a half or more – the target date for having the final notice of the voluntary standards printed in the Federal Register is January 2002. In terms of Internet voting, the FEC draft being considered is explicitly silent on remote Internet voting (e.g., voting from home) and deals only with recommendations for precinct-based Internet voting.

Reflections

I would like to summarize my observations and the suggestions by Safevote, Inc. to the FEC. *These are not IVTA recommendations and other companies may have different positions.*

First, much of the FEC text in the draft on Internet voting is written in terms of describing a solution, which many attendees – myself included – asked to be changed to specifying requirements.

Second, even though Safevote has the technology that can make Internet voting private and secure from home, office or anywhere else, we feel that we can only offer our systems for certification for public elections and can only do binding Internet public elections when we achieve "rough consensus and running code." This 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 inter-operation. 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 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, in 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.

Regarding the issue of open source code raised in the FEC meeting, we agree with the concept but suggest that *either the source code is going to be 100% open or it will not work.* Openness should include not only open source software but also open peer review of voting standards, where vendors, developers, experts, government sectors and the voters themselves may make contributions and provide oversight.

The above is my conclusion after many years of thought and making recommendations on this subject. Pockets of hidden code should not be allowed in anything that is compiled into binary code, because there would be plenty of room for mischief, errors, covert channels, etc. To move from today (100% closed code) to tomorrow (100% open code) we need a bridge and that bridge is, in our opinion, open protocols. Open protocols will serve the purpose of helping analyze the code itself, code which is usually hard to read and follow even by the programmers themselves.

Thus requirements for certification MUST include open protocols and SHOULD include open source code.

Regarding the issue of classification, we agree 100% with the FEC's plan to classify Internet voting systems under Digital Recording Electronic (DRE) machines. The DRE requirements which do not apply to Internet voting systems (e.g., the safe storage of ballot images for all votes stored in the DRE) are trivially satisfied by Internet voting systems for which the vote is not stored, just forwarded. For example, by storing 0 votes, the Internet voting system is required to keep the ballot image of 0 votes – which is trivially true. Classifying Internet voting systems under DREs also has the benefit of **not** decreasing the safety and integrity standards already discussed for DREs. Even though it may seem logical for someone else, as voiced at the meeting after my support of the FEC model in this case, to derive Internet voting from "electronic voting" as a new classification which would also branch out to DREs from a common root, this taxonomy would pre-empt the current rules already discussed and time-tested for DREs and which could be applied to Internet voting systems. This could open the door to "new" mistakes which might otherwise be prevented when seen in terms of "old" mistakes.

In summary, Safevote's main suggestions to the FEC were in support of open peer review protocols and 100% open source code, and labeling all Internet-related items in the FEC new standards as "EXPERIMENTAL." This means that we need both "rough consensus" **and** "running code" at every step of the protocol development process. This will take time. As a community responsible for introducing such a large change as Internet voting has the potential to become, our strategy should be to test, test, test and to do it right the first time. Only by establishing trust in the process, can we hope to establish trust in the results.

Open Source and Open Protocols

It is appropriate at this point to stop for a minute and explain the relationship between protocols and how they are implemented. Protocols are like a recipe. Different people can take the same recipe and produce different results depending on the quality of ingredients, for example. Likewise in software development, different vendors can take the same protocol or recipe for accomplishing a particular task and produce different implementations of it, i.e. different versions of source code. The ability to verify that the source code is an accurate implementation of the protocol upon which it is based is a thorny issue today, especially in Internet protocols where a "small" difference in interpretation often leads to large differences in results. This problem needs to be addressed if the public is to have confidence in voting protocols using the Internet.

Therefore, I feel that topics such as open source code and open protocols need to be at the heart of any discussion for Internet voting.

In this regard, the IVTA was formed based on the idea of providing a public environment for open peer review of Internet voting protocols. This idea is, of course, not new (e.g., the IETF).

The IVTA's role is to act as a neutral party in reviewing proposals, issuing recommendations, collecting responses from users and verifying eventual design faults as well as their proposed solutions. The IVTA, contrary to a vendor association, provides a meeting ground for diverse interests, for discussing worldwide voluntary public standards in Internet voting in private and public sectors. The IVTA can thus provide both reduced liability for companies as well as increased reliance by the public, which are otherwise competing goals.

Open Internet protocols also help decrease development costs and time to market. In strict business terms, these are the benefits of open protocols. Thus, in my opinion, open protocols are a win-win proposition, in spite of the fact that many may feel threatened by what may seem to be a decrease in control power and, paradoxically, an increase in oversight.

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

The Private Sector Won't Wait, Part III

Edited by Eva Waskell[*]

Comments from companies interviewed for this study provide additional insight into the market and the motivation, or lack thereof, for enhancing privacy and security safeguards in proxy voting.

Catalyst and Motivation for Internet Proxy Voting

Early adopters of Internet proxy voting served as a catalyst for their corporate peers. Harris Shareholder Services internally developed an Internet proxy voting system in 1996, which it debuted with Intel Corporation. ADP states that 1000 companies used its Internet proxy voting services in the 1998 proxy season. Lucent Technologies, who first used Internet proxy voting for beneficial shareholders in 1998, now refers to it as "a commodity."

The study identified only two proprietary software systems on the market designed to meet the voting needs of institutional investors: ADP ICS' ProxyEdge and ISS' ProxyMaster. Neither of these systems are Internet voting systems, although ISS is in sthe process of beta testing the Internet version of ProxyMaster. ProxyEdge has the dominant market share.

Corporations and mutual funds cite the following motivations for offering Internet proxy voting: cost savings; voting ease and convenience for the shareholder; faster proxy tabulation; consistency with the company's position as a technology company; desire to be up-to-date with the voting methods offered by other corporations; responding to an active Internet user shareholder base; lead-in to offering regulatory (proxy) materials over the Internet.

Per Vote Cost Data

	Shareholder.com	ADP
Mail proxy card	$.36	$.34
Telephone vote	$.17	$.18
Internet vote	$.05	$.03

Corporations that receive a single, bundled charge for all services provided by their transfer agent may not be aware of per vote cost segmentation for registered shareholders.

Electronic Voting Trends

Companies interviewed for this study indicate a steady rise in the percentage of shareholders choosing to vote over the Internet –even though the numbers are still small.

Proxy Services Corporation states that 40% of registered shareholders vote. Shareholder.com estimates that about 30% of eligible voters cast a vote by some means, paper or electronic. Among those that cast a vote, 1/3 do so electronically –out of which, about 1/3 use the Internet. Harris Shareholder Services states that over 40% of its clients' registered shareholders vote electronically (by Internet or telephone) and that 15% of voting shareholders vote via the Internet. Harris further states that the use of the Internet has increased threefold in the most recent voting cycle, as compared to the previous year. Calvert Group notes that in the January 1999 proxy covering 20 mutual funds, 10% of the votes were cast by Internet, 10% by telephone and 10% by mail.

Harris Shareholder Services observes that although Internet proxy voting grows each year, telephone proxy voting continues to maintain a share advantage. This is attributed to a current higher ease of use with telephone voting.

Satisfaction and Unmet Needs

Fortune 100 Corporations

The three corporations interviewed for this study are satisfied with the Internet proxy voting services provided by their transfer agents. Intel's transfer agent, Harris Bank Shareholder Services, reports steady growth of Internet proxy voting among Intel shareholders, with about 13% of the registered shareholder who voted in 2000 doing so over the Internet. Lucent Technologies is very satisfied with the Internet proxy voting service provided through The Bank of New York and Shareholder.com. PG&E recently outsourced the transfer agent function to ChaseMellon Shareholder Services because of a desire to access the technology and services of a professional transfer agent. PG&E is satisfied with Internet proxy voting and views it as "a natural option" to offer shareholders given its widespread use by other corporations.

Transfer Agents

The three transfer agents interviewed for this study are satisfied with their Internet proxy voting services. Harris Shareholder Service had to develop it own system for Internet proxy voting as there were no third party systems available in 1996.

2000 is the second year that ChaseMellon Shareholder Services has offered Internet proxy voting through Corporate Document Systems. Harris is pleased with the steady increase in the number of clients deciding to offer Internet proxy voting to their registered shareholders, as well as the steady rise in the percentage of registered shareholders choosing to vote over the Internet. Currently 15% of clients' voting shareholders vote via the Internet. At this time the potential impact of Computershare's acquisition of Harris Bank Shareholder Services on the choice of system for Internet proxy voting is not known. Changing technology partners in 2000 is not as difficult as it would have been in 1998, considering the limited number of alternatives that were available at that time.

Institutional Investors

Institutional investors have a limited number of system choices for proxy voting.

CalPERS is satisfied with the ProxyEdge system, but would like a more "user-friendly" report generation capability. Cut-off times for submitting votes on the ProxyEdge system sometimes cause CalPERS to use ProxyVote.com. CalPERS notes that the main disadvantage of ProxyVote.com is the lack of a field to indicate the rationale for the vote, which is an important feature of the ProxyEdge system. ProxyVote.com lacks the recordkeeping and report capability of ProxyEdge. Another disadvantage of ProxyVote.com is that it is designed for "one proxy at a time voting," rather than for the institutional investor who needs to vote on multiple proxies in a single session.

Voter Feedback

None of the corporations or transfer agents interviewed for this study currently maintain a formal method of obtaining shareholder feedback on Internet voting. Harris no longer pro-actively solicits shareholder comments on Internet proxy voting because past comments indicated that shareholders like Internet voting. Lucent Technologies states that, based on informal feedback, Internet proxy voting is generally well received by shareholders. Lucent notes that the only negative comments come from computer novice shareholders who have difficulty accessing the web site "because their browsers aren't set right or their computers aren't configured properly for accessing the Internet." PG&E prepared itself to respond to potential shareholder concerns about voting on the Internet, but the anticipated questions never arrived. Norwest Shareowner Services has received very little shareholder feedback of any kind. When comments are received they tend to be from shareholders that are not able to access a voting web page.

Web Site for Internet Proxy Voting

Companies offering Internet voting provide the web addresses where registered and beneficial shareholders can vote in their proxy statements. The online versions of the proxy statements often contain hyperlinks to the voting sites. In some case the voting sites provide a hyperlink back to the corporate issuer's online annual report and proxy statement. The proxy cards that are sent to registered shareholders provide the web site for Internet voting. All of the companies interviewed for this study send shareholders to a specific web site for voting, rather than directing voters to a hyperlink on the corporate issuer's web site.

None of the companies interviewed felt that voter confidence would be increased by sending shareholders to a voting hyperlink on the corporate issuer's web site, rather than directly to the voting web site. Some noted that sending voters to a third party site might provide shareholders with a greater feeling of confidentiality.

Privacy and Security Concerns

Privacy

In corporate proxy voting the transfer agent is under no legal requirement to protect the secrecy of the vote unless a corporation has adopted a confidentiality resolution. If a confidentiality resolution is not in place, then the corporation can receive the proxy cards and a reconcilement report. The reconciliation report identifies the shareholder by name and how he/she voted on each proposal. Changes in the shareholder's vote that occur at the annual meeting are also shown on a reconciliation report.

The corporations interviewed for this study state that they have not heard comments from shareholders indicating concerns about the privacy of the vote when voting on the Internet. However, the proxy statements for Lucent Technology's February 16, 2000 and PG&E's April 19, 2000 annual meeting include shareholders' proposals on confidential voting. Lucent Technology's and PG&E's Board of Directors recommended a vote against confidential voting [see http://www.lucent.com/investor/proxy/00/prop2.html].

Corporations benefit from advance information on the vote.

Corporations have access to information on the level of participation (progress toward reaching a quorum) and on the voting trends, prior to the annual meeting. In some cases the transfer agent publishes this information on a web page that the corporation can access. Corporations can use the advance information to determine if additional shareholder mailings or proxy solicitation activity are needed, or to prepare their reaction to the voting results.

The Council of Institutional Investors indicates that concerns about privacy vary across the membership. The Council notes that members that have concerns about privacy hold a fair number of their shares in street name. Many public funds make their guidelines public and are even publishing their votes on the Internet. CalPERS' Principal Investment Officer creates a web page listing CalPERS' voting for its top 300 holdings. The Council of

Institutional Investors anticipates that more public funds will be following this direction, but observes that private funds, corporate plans and union funds may have a different perspective.

Interest in Enhanced Privacy or Security

Proxy Monitor indicates that some institutional investors are concerned about maintaining the confidentiality of their share positions.

Current Privacy Mechanisms

Interviewees cited the following mechanisms for protecting voter privacy: secure web sites with secure socket layers (SSL, https); secure data bases; information on shareholders' votes is stored in the transfer agents' back-end systems, which could only be cracked by a hacker; voter selects PIN number.

Security

Corporations interviewed for this study express a high degree of reliance and confidence in the security of the Internet voting systems provided by their transfer agents and technology partners. Transfer agents note that some corporations ask only a few questions about the security of the Internet voting system, while others perform more extensive due diligence. Transfer agents generally serve as Inspector of Elections.

ChaseMellon Shareholder Services and Norwest Shareowner services indicate that they performed a thorough evaluation of the security of their technology partner's Internet proxy voting system. ChaseMellon had assistance from a corporate parent and Norwest received assistance from WellsFargo's Internet Security Department in evaluating the security of the systems. Harris Bank Shareholder Services obtained suggestions from clients on security issues as it developed its Internet proxy voting system.

Shareholder.com indicates that in some cases the legacy systems of the transfer agent are a barrier to implementing higher levels of security, such as combining the control number with validation of personally identifying information stored in the transfer agent's systems.

CalPERS states that it trusts that the votes go to ADP and has not evaluated the security of the voting systems it is currently using.

Current Security Mechanisms

Providers of Internet proxy voting systems note the use of the following security mechanisms: firewalls; secure web sites with secure socket layers (SSL, https); secure data bases; storing the vote in a separate data base not accessible to the Internet; encryption; passcode invalidation if voter attempts to perform any action other than voting the proxy.

Comments from companies interviewed for this study provide additional insight into the motivation, or lack thereof, for enhancing privacy and security safeguards:

Corporations

"The privacy and security issues are the responsibility of the transfer agent and the [technology partner] since the contract for Internet proxy voting is between those two entities."

"Security is of interest to us, and is included in our contract with the transfer agent. Any improvement in security is good, but would be up to the transfer agent since it is their product."

Transfer Agents

"Greater privacy and security safeguards would only drive a decision to change technology partners if there was a big [problem]".

"What level of security is really needed? You may find out that you really don't need that much."

Technology Partners

"We are limited in the security mechanisms that we can implement because we are in the business of providing the voting for the transfer agents however they need it to be done… It is not in our best interest to provide any additional security."

"A breach of security in Internet voting is 'inevitable' because hackers are smarter than programmers are."

"We do not want to have to install additional software on our system or involve another company in authenticating the voter and receiving the votes."

"Large institutional investors, such as mutual funds, avoid transmitting votes over the web because of concerns that their share positions can be known or altered."

"We have an extremely secure environment – over and above anyone in this industry."

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

Open Source and Open Software

(continued from p. 6)

Two Definitions of Open Source

The term "open source" is somewhat confusing because it has two different definitions. There is an assumed definition and a more correct definition.

The assumed definition of "open source" is something like "software whose human-readable 'source code' is available to be viewed by the general public." Without further explanation, people simply assume that this is what the term means. It should be noted, however, that this assumed definition of "open source" is considered to be an incorrect use of the term. The more widely used definition of "open source" is "any software released under licensing terms which comply with the 'Open Source Definition.' " The "Open Source Definition" is spelled out at www.opensource.org/osd.html. The definition of "open source" involves thus more than simple access to source code. Sometimes (though not always) people use a capital "O" and a capital "S" when they refer to Open Source in their writings.

Key People, Organization, and Resources of Open Source

The "Open Source Initiative" (OSI), founded in 1998, is the organization which defines the Open Source movement. Eric Raymond and Bruce Perens were two of the people who were fundamental in getting OSI off the ground. Eric has both written and spoken extensively on the topic of Open Source. Bruce was the primary author of the 'Open Source Definition.' Both are still relatively visible in the Open Source world.

When reading Open Source related material on the Internet, it's not unusual to come across a few common acronyms - which are usually unexplained. The Open Source community is, just as the broader technical community is, rather fond of acronyms. When accessing this material, it's good to keep in mind that OSI stands for "Open Source Initiative;" ESR stands for "Eric S. Raymond;" and OSS stands for "Open Source software." It should also be noted that "OS" is the acronym for "operating system" and should **not** be used to refer to Open Source - OSS should be used instead. A history of Open Source is available at www.osdn.com/history.shtml. More information on Open Source is available at www.opensource.org.

Two Definitions of Free Software

"Free software" is a term used in some of the same circles that "open source" is used. To most people, the meaning of this term seems obvious. However, the obvious interpretation of the term is not necessarily the correct interpretation.

Just as with "open source," the term "free software" has a double meaning. Again, there is both an assumed definition and a more widely used definition.

The assumed definition of "free software" is something like "software which costs nothing to obtain." Without further explanation, people automatically assume that this is what the phrase means. However, it should be noted that, here also, the assumed definition of "free software" is considered to be an incorrect use of the term.

The more widely used definition of "free software" has nothing to do with cost, it has to do with your rights once you obtain the software. It has to do with your *freedom* to do with the software almost anything you want to, once you obtain a copy of it (even if you paid for that copy). Sometimes (though not always) people use a capital "F" and a capital "S" when they refer to Free Software in their writings.

Key Person, Organization, and Resources of Free Software

The "Free Software Foundation" (FSF) is the organization which defines the Free Software movement. Closely related to FSF is the "GNU Project," which was launched in 1984 to develop a complete operating system - the GNU system - which would be available as Free Software. The increasingly popular GNU/Linux operating system is a variant of the GNU system. FSF and the "GNU Project" were both founded by Richard Stallman.

Just as with Open Source, the Free Software community has its own set of acronyms. When accessing Free Software related material, it's good to keep in mind what these acronyms are. FSF stands for the "Free Software Foundation." GNU often refers to either the "GNU Project" or some piece of software related to that project. RMS or simply "Stallman" refer to "Richard M. Stallman." "Copyleft" refers to a unique, inverted-copyright concept which FSF has pioneered. And GPL stands for the "GNU General Public License" - the granddaddy of all Free Software and Open Source licenses.

More information on "Linux and GNU" is available at www.gnu.org/gnu/linux-and-gnu.html and on "copyleft" at www.gnu.org/copyleft/copyleft.html. The full text of the GPL is available at www.gnu.org/copyleft/gpl.html. And a more complete explanation of Free Software is available at www.gnu.org/philosophy/free-sw.html or at www.gnu.org.

The Relationship between Open Source and Free Software

As for the relationship between Open Source and Free Software, the answer you get depends on whom you ask.

Open Source advocates tend to view Free Software as a subset of Open Source. All of the licenses which are approved as Free Software licenses (www.gnu.org/philosophy/license-list.html) are all also approved as Open Source licenses (www.opensource.org/ licenses/). However, the reverse is not true. Open Source advocates consider the *pragmatic benefits* of open software development, and the inherent weaknesses of closed software development, to be the primary issue. Free Software advocates, however, consider *freedom* to be the primary issue and tend to view Free Software as a movement which is entirely separate and distinct from Open Source.

More on this distinction is available from Richard Stallman, with the Free Software perspective, at www.gnu.org/philosophy/free-software-for-freedom.html.

And from Eric Raymond, with the Open Source perspective, at www.tuxedo.org/~esr/writings/shut-up-and-show-them.html.

As a side note, ESR's use of the words "hacker" and "hacking" simply mean "someone who loves to write code" and "writing code," respectively. The entire Open Source and Free Software communities use these words basically the same way. Eric's use of these terms, in the article referenced, has no connection to the common misconception that "hacker" and "hacking" are synonymous with "computer criminal" and "illegally breaking into a computer system." These are definitions which have been spread by the popular media, but which are inconsistent with the words' original meanings. A better feel for the correct meaning of these words can be obtained by reading Steven Levy's book "Hackers" (published in 1984) or Eric Raymond's essay "How to Become a Hacker" (www.tuxedo.org/~esr/faqs/hacker-howto.html). The terms "system cracker" (analogous to a "safe cracker"), "malicious hacker," "black-hat hacker," or simply "black-hat" are more commonly used to refer to "computer criminals" by those who understand this distinction.

As can be seen from the articles just referenced, the debate between the Open Source point person (ESR) and the Free Software point person (RMS) can be quite contentious on the surface. However, if you follow the dialogue long enough, it can be seen that there is actually quite a bit of respect which flows in both directions.

Hopefully this article will help everyone to successfully navigate the somewhat confusing labyrinth of the Open Source and Free Software worlds.

Thom Wysong has been programming computers as a hobby since 1982 and professionally since 1994. He recently moved to Washington, DC to create Open Source software for Internet voting and online democracy. Wysong is a frequent contributor to the IVTA. He can be reached via email at tgw@technodemocracy.org.

Why Electronic Voting Software Should be Free Software

(continued from p. 8)

The FREE e-democracy project

So how does our project follow through on some of the promises that Free Software offers? The project has a number of aims that we keep at the top of our minds when developing the software and when running the project as a whole:

Software Development Aims: (1)provide a secure and private system; (2) create scalable and reliable software; (3) offer a non-commercial, non-partisan voting alternative; (4) use the GPL to create an open system that Internet users will trust; (5) release a system that can be used to support the growth of effective democracy anywhere in the world.

Project Aims: (1) develop a leading electronic voting system; (2) advocate the free software paradigm; (3)evangelise the use of technology to strengthen democracy within a holistic understanding of the current malaise, i.e. Internet voting alone is not going to solve turnout problems.

With these aims in mind, we have developed software which has been through several iterations, currently standing at version 1.3. The software has been downloaded hundreds of times and a wide number of groups, ranging from the Valley Industry and Commerce Association to the Free Software Foundation, are assessing it.

Jason Kitcat is the co-ordinator of the FREE e-democracy project. He designed and implemented the project's software in Java as part of a final year thesis while studying for a joint Computer Science and Management Science degree at the University of Warwick, UK. The software and its accompanying papers were awarded 'Best Project of the Year.' Kitcat continues to develop the project (http://www.thecouch.org/free/) while setting up his consultancy Swing Digital (http://www.swingdigital.com). He can be reached at jeep@thecouch.org.

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
U.S. POSTAGE PAID
SAN RAFAEL, CA
PERMIT NO. 896

DATED MATERIAL
Please Expedite

The Private Sector Won't Wait, III

See p. 11

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

cut here **MAIL ORDER FORM** **cut here**

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

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

NAME/TITLE_____

COMPANY_____

ADDRESS_____

E-MAIL_____

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

[ ] $30.00 SUBJECT TO AVAILABILITY – 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