

**PRE-EVENT BRIEF**  
**SWISS INTERNET VOTING TECHNOLOGY**  
Assembled by The Hollywood Hill

## **1. Why Internet Voting?**

**The argument for Internet voting is that it can increase voter participation, and it can lower costs.**

By making voting easier and more accessible from your home or office, and allowing for a longer window of voting time - over an entire week instead of one day - you can dramatically increase participation.

Lowering the costs of each election means you could have more of them, which would foster a more participatory democracy in which more questions are placed directly before voters.

### **The Success of the Swiss Model**

Switzerland has launched pilot projects enabling citizens in three Swiss cantons to vote from home using their computer. This type of electronic voting, also known as remote voting, is offered as an option, in addition to vote-by-mail and polling stations. The introduction of vote-by-mail in Switzerland significantly increased voter participation. The core goal of Swiss Internet voting is to increase participation even more. Early results have been very positive. Since the roll-out of the three pilot projects, 50% of normally abstaining voters have cast ballots online.

Switzerland already has a highly participatory democracy. From 1989 to 1998, Swiss voters were asked to vote an average of more than 32 times per year!!! This is a stark contrast to the U.S., where voters are asked to go to the polls two or three times a year at most. With so much voting activity, it's easy to see why today 95% of the voters in Switzerland's Canton of Geneva use vote-by-mail instead of visiting a polling station.

## **Can we trust computers?**

Most computer security experts believe that computer voting will lead to either lack of voting secrecy or exposure to undetectably altered or missing votes. Software used in Diebold machines and deployed in U.S. states such as Maryland has been shown by independent researchers to be vulnerable to numerous undetectable hacks. The software has been shown to not conform to virtually any security best practices, presumably because it was rushed to market after the 2000 election debacle.

The other argument against internet voting in the U.S. is that we haven't yet tried weekend voting or vote-by-mail nationwide as ways to increase voter participation. In 1998, the State of Oregon switched over exclusively to vote-by-mail and has had tremendous success. In 2004, 87% of Oregon's registered voters cast ballots.

Internet voting also introduces digital divide issues, in that internet voting would make voting more convenient only for younger and more affluent voters.

## **The Promise of eDemocracy**

*Provided by the Swiss Delegation*

First came the "parliamentary democracy", where each MP represented the whole national community. Political parties and the division of society in social classes had not been theorized yet. Then came the age of "media democracy", where the parliament had to mediate between conflicting interests. The political parties grew in relevance and seized the MPs' role as expression of the community. Media played an important role of transmitter between the people and its elected representatives.

And now we have entered the third age, the age of "public democracy". Parties struggle to retain their political basis and keep in touch with the public's demand as the population's sociological composition changes. The political parties tend to become public relation tools concentrated on electoral dates. The

class system is no longer able to express the social composition and the various overlapping social statuses. This new imbricate political landscape is reflected by the growing number of elections whose outcome is nearly a 50%/50% division of the electorates involved.

A new, more active kind of citizenship is being invented while the notion of public space is being redefined and extended. Citizenship is less and less identified with the sole election of representatives and is more and more understood as a broader involvement in public life, that doesn't correspond to party militancy. The role of new bodies such as non-governmental organizations grows, as they tend to better express the public interest by not acting along partisan lines. Through these bodies, citizens are increasing their share of power and holding their representatives more accountable of their votes and choices. In this light, however, the development of the web - whether understood as physical network or as data structure - carries the promise of a larger public involvement in public life. Just as the newspaper boom of the 19th century sparked a thirst for news - or did it simply reveal a huge existing need that compulsory education had contributed to create? - and ultimately helped expand the democratic model, the internet boom will change and expand the way democracy is being lived and experienced in modern societies. The Internet also provides citizens with an unprecedented memory. While it was fastidious to check paper registers for the votes of outgoing MPs or for the candidates' business interest, internet brings a new ease in the consultation and maintenance of this information. The bookkeeping is not anymore a privilege of the state or of the public administration.

Because they understand that under these new conditions, their reelection is being played during their office time more than during the election campaign itself, a growing number of MPs maintain their own web portal which offers a real dialogue and public involvement space. First time candidates have to compete on this ground and try to voice the public concerns. This is eDemocracy on the move. Where will it go?

### **Tools For eDemocracy**

Imagine we are in the year 2020, on the eve of national elections. The political debate is rich of the many contributions citizens have posted on their blogs and web sites. Mainstream media interact with this grassroots scene.

Voters have access to a web platform that provides four modules:

- The first one allows voters to match on a number of issues their choices to those of the candidates seeking their suffrage. In Switzerland, where this module is being implemented by a private group, it is called Smartvote. The idea is simple: just fill the questionnaire candidates have also filled and the system will compose the list of candidates who best match your choices. Voters can also map their choices on six pre-defined dimensions (attitude toward the European Union, economic policy, social openness, etc.) on a spider chart to match it with each candidate's and each political party's chart.
- The second module stores the votes of the outgoing MPs. Every voter can see for herself, issue by issue, the choices of those running for reelection.
- The third module offers citizens the opportunity to discuss their opinions with fellow citizens or candidates. Citizens may share their previously stored political profiles with others and provide justifications for their choices. For the forums to be successful and their contributions to comply with legislation on, for example, racist or discriminatory discourse, they need to be moderated.
- The last module is of course the internet voting module.

These four applications already exist , although they have not been implemented in a coordinated way. Swiss citizens could for example already check their opinions against that of candidates running for office on a Smartvote module and vote online.

### **A Push Towards Direct Democracy**

The consequences of the advent of eDemocracy could be far-reaching. We can prognosticate that the rise of bottom-up democracy - or better said of network democracy - will have deeper impacts than the addition of some new "web 2.0"-based functionalities. The development of network based political exchanges and interactions will affect the political and electoral systems.

Will citizens accept to elect MPs every four of five years and retire into private life, when the society is teeming with ideas, proposals, needs or demands that find their way to the web and, far more than today, in the mainstream media? And how could they go on voting for sealed lists of candidates rather than for individuals chosen among different lists, when the electronic interfaces make it possible to match the candidates' opinions one by one against one's own?

The first impact of eDemocracy could thus be an increase of the so-called direct democracy tools, referendums, initiatives, recall ballots, etc. The second - a consequence of the former - could be an extension of federalism and of the powers of local authorities. The third could be a change of electoral rules favoring proportional ballots and the possibility for voters to make their own list by mixing candidates from different party lists or at least by choosing their preferred candidates within a single party list.

While the oracles standing by the web in its infancy decided it would shrink the planet and promote world citizenship, local issues or the local avatars of global issues (remember the "think global act local"?) prove to be the glue that holds virtual communities together and spark protests.

Not only do local issues compensate for the distance created by the democracy by delegation, as Manin observed (Manin 1995), they are also the basis of the community social interactions and ties. The local level is at the convergence of the emotional and political dimensions, it is the geographical and emotional nest of the political experience and feelings. Not surprisingly, all pilots of participatory democracy using web tools have taken place at the local level, where they are the more meaningful.

In other words, the citizens' newly gained power and relevance will be felt first and foremost at the local level. To answer the citizens' claims, local authorities will need increased competencies, thus challenging the institutional balance. In the same move, citizens will demand to handpick representative they know rather than ratify party choices.

In the end, the advent of eDemocracy will improve the subjective quality of the individuals' participation and involvement in the public life, because eDemocracy is about quality, not quantity. There might be more risks associated with refusing eDemocracy than with accepting it. The citizens' subjective feeling of the lack of available communications channels with the authorities might prove more damaging than the existence of direct

ways to interact with the elected representatives or to challenge their decisions.

## 2. How The Swiss Technology Works

### **Pilot Project #1: Geneva**

Five years ago Geneva began developing its e-voting system. The application has been developed by the cantonal administration, in partnership with private companies. The system is based on existing voting material and does not require any special features on a client computer.

Swiss registered voters already receive their polling cards and voting material (incl. ballot paper) by mail before each election or referendum. The license must be presented when voting at poll stations or sent with the postal ballot by mail.

If a voter wants to cast a vote electronically, he accesses the e-voting system through the Internet. The voter must then enter his polling card number to gain access to the secure electronic polling booth. He then submits his vote and confirms or alters the choice before being authorized again by the system. This time the voter enters a secret ID code, his date of birth and place of origin, all of which are difficult to guess or counterfeit. The system then confirms that the vote has been successfully transmitted and recorded.

The Geneva project has solved the problems of voter identification, a major challenge of any e-voting solution, by means of a simple scratchable field on the voter's polling card. Under a metallic strip there is a secret ID code that the system checks before casting the vote in the electronic ballot box. Polling cards where the metallic strip has been scratched off are no longer valid for votes in person at the polling stations or for postal votes unless it can be proven by means of a barcode check that the person has not already cast a vote electronically.

The electronic ballot is encrypted. Two keys are necessary in order to open it. To ensure security, the keys are given to members of different political parties that are represented in parliament. Since a voter's identity and ballot are kept in two distinct files, it is not possible to match a given ballot with a voter. Geneva also carried out several hacking tests that proved the system to be very safe.

### **Pilot Project #2: Neuchatel**

This pilot project is using a different approach to e-voting. Close collaboration between the canton and its 62 communes has given rise

to the creation of a one stop e-counter – the “guichet sécurisé unique”.

Similar to Internet banking today, the canton’s residents will receive a user-ID, password and alternating transaction code to access the one-stop e-counter, which offers a variety of government services. Before each popular vote, voters will receive an additional code that will allow them to cast their electronic ballot.

### **Pilot Project #3: Zurich**

The canton of Zurich has a total of around 820,000 registered voters. The geographical and political landscape consists on the one hand of Switzerland’s largest city (Zurich) and, on the other, of many smaller communes, some of them with less than 200 voters. Each commune uses its own administration system, manages its own electoral register and counts its own votes.

Because voting is carried out at cantonal and local levels, close cooperation between both levels of government is vital for success. The plan is to implement e-voting at the local level and have the communes pass on the results to the canton. For this reason, the Zurich project is currently the most ambitious. Zurich has created a canton-wide shared database of voters that will constantly be updated by the communes, while barely changing the existing network of information systems in the communes.

The system had its first successful rollout in the course of elections to the student parliament at the University of Zurich in December 2004.

### 3. *Wired Magazine* on Voting

#### **Election '08: Vote by TiVo**

by Kevin Axline, 11.14.06, *Wired Magazine*

In the wake of yet another election marred by technical glitches, critics of electronic voting machines are repeating their call to restore old-fashioned paper to the increasingly computerized election process. But a smaller, quieter group is convinced the real solution lies in the other direction. Now is the time, they say, to make elections completely electronic, and allow voters to cast their ballots from home, over the internet.

"The technology is done," said Jim Adler, founder of election-auditing firm VoteHere. "It's really an issue now of politics and people's will." If it seems insane to put democracy's most crucial function on wires shared by viruses and spam, consider that it's already happening. The 2000 Arizona Democratic primary was the first binding election that offered online voting, and 41 percent of voters (39,942) voted using the internet. The 2004 caucus conducted by the Democratic Party in Michigan offered internet voting and 46,000 of 163,000 votes were cast online.

Switzerland, Estonia, England and Canada all have run successful small-scale trials of internet voting. Estonia now plans to use national internet voting for its 2007 parliamentary elections; the internet will, quite literally, decide the future of its government.

Elections in 2002 and 2003 in Swindon, England, included an online option. VoteHere electronically audited the election from its Seattle offices, and Adler estimates the voting system handled a total of 600,000 votes from multiple counties that were cast over a variety of channels, including TV, internet, telephone and text messaging. The system's performance was "excellent, no problems at all," said Alan Winchcombe, the head of electoral services in Swindon. "People did try to hack it, but no one got through. The security levels were very high."

Such successes aside, internet voting is considered heresy in security circles, where the concept has been repeatedly and violently pilloried since at least 2000. If American voters are not ready to trust Diebold, are they ready to vote for president using their Windows machines? The nay saying has its roots in well-understood vulnerabilities, but now some voices are wondering whether the criticism may have gone too far in seeking to rule out discussion on the topic, rather than

explore solutions. After years of grappling with electoral problems, maybe it's time to re-open the debate by weighing the risks of this radical alternative against the benefits, rather than comparing it to an unattainable ideal of perfect security.

"We're in a world of error. The question is: how much can you tolerate?" said Adler.

Skeptics dismiss claims of past online voting successes, saying the elections officials evaluating those elections aren't qualified to pronounce them a security success. They point to four major breakdowns in any internet voting scheme that they claim are intractable:

- General purpose PCs are inherently insecure and vulnerable to viruses and other attacks that could compromise votes without detection.
- Denial of service attacks could disenfranchise voters.
- Database hacks could change vote tallies.
- Putting voting into the home would destroy poll-booth privacy, exposing voters to intimidation and bribery.

"The folks who decide to use (these systems) don't understand the technology," said David Wagner, an associate professor in the Computer Science Division at the University of California at Berkeley who specializes in computer security. "They don't know how to distinguish between good marketing and good technology." Wagner respects VoteHere's work. "Their cryptography is really brilliant, tour de force stuff," he said. But he maintains that voting in a public election "over the internet is crazy."

David Jefferson, a computer scientist who has worked with Compaq and HP on election security, and has one of the longest track records of studying online and electronic voting, agrees.

"There's really no way to secure the transmission of votes over the internet," Jefferson said, pointing out that home PCs' vulnerability to viruses and other malicious code makes it impossible to assure that a vote is cast and counted the way it was intended.

Jefferson's views helped shut down a Department of Defense online

voting program that was scheduled to take place in 2004. The \$22 million project would have allowed up to 100,000 military personnel abroad to vote over the internet.

During the planning stage, the DOD formed a blue ribbon panel of 10 experts in voting and security systems to evaluate the program, entitled the Secure Electronic Registration and Voting Experiment (SERVE). In January of 2004, four of the reviewers -- David Jefferson, Avi Rubin, Barbara Simons and David Wagner -- published a report labeling the SERVE program, along with any other voting system that used the internet, as inherently insecure. The project was closed shortly thereafter.

The SERVE report is one of a handful of papers published by experts since 2000 that have put the brakes on online voting options in the United States. But the decision wasn't unanimous. The other six reviewers did not issue a contradictory report, but at least two of them take issue with the absolute stance of its authors.

"By saying it's impossible to do it, we're cornering ourselves," said Ted Selker, one of the SERVE reviewers, who currently teaches Industrial Design Intelligence at MIT. "We're not allowing ourselves to solve the problem.

"The downside was very small," said Michael Shamos, a former IBM engineer and computer science professor at Carnegie Mellon who has taught classes on electronic voting. "I thought SERVE was a great idea."

Critics of internet voting say the general-purpose computer is inherently insecure. An internet election would become a free-for-all of competing malicious code, battling over users' home computers to elect the authors' favorite candidates. Hackers would control vast botnets of voting malware. The internet itself is also unreliable, and cruder attackers will launch denial-of-service attacks that suppress unwanted votes by killing internet access for entire voting precincts at a time.

Vocal opponents to online voting such as Jefferson and Aviel Rubin, the technical director of the Information Security Institute at Johns Hopkins University who co-authored the SERVE report, argue that acceptable security is impossible with PCs and the internet as they are.

"I think this is such a bad idea that getting into specific solutions is dangerous," said Rubin. "I feel like you're asking me if it's a good idea for people to explode nuclear bombs in their bedrooms.

Selker and Shamos agree there are very real and complex security concerns, but they see them as puzzles to be solved. "This is an engineering project," said Shamos, "To decide in advance that it will fail is unscientific. It's like saying, 'I don't think we could ever send a man to the moon so I'm not going to work for NASA.'"

Proponents argue they can address specific security concerns of internet voting from an engineering perspective. The threat of DOS attacks on servers and infrastructure can be mitigated by extending the window of time people have to vote -- maintaining a DDoS attack for a week would be a challenge for even the most determined electronic election-rigger.

The susceptibility of home PCs to malicious code could be resolved with closed set-top boxes that only run open-source, verified and digitally-signed software. The large variety of ballots between counties, coupled with a potentially large sample of audit firms handling the elections, could also make a unified hack of national elections more difficult.

Conventional voting techniques have always been error prone; the question is one of risk management, says Adler, who worked on rockets as an engineer for Lockheed-Martin before getting into data security and signal processing. You can never guarantee that nothing bad will happen in any situation. "That's an impossible bar," said Adler.

While Adler does not claim to guarantee 100 percent secure online elections, he is sure that fraud can be detected. By providing a serial-numbered receipt to the voter, which can be checked against the ballot-box results, he says, "You can guarantee that nothing bad can happen without anyone knowing about it. Our products are barking dogs, not higher walls."

The issues with internet voting go beyond computer security. In many ways, in-home voting represents a paradigm change, obliterating the perceived sanctity of the polling booth, and raising questions about privacy and safety, the looming specter of voter intimidations and vote-purchasing. And to be truly fair, internet voting would require every segment of the population to have access to the internet. Proponents already have answers for some of these problems. To prevent coercion or intimidation, for example, voters could be allowed to vote as many times as they want, with only the last vote counting. If a boss or spouse were forcing you to vote a certain way, you could change your vote later on. The potential for selling votes could be disrupted by serial-coded receipts decipherable only by the voter.

Despite early setbacks, the idea isn't going away easily and it promises to grow in power as more countries give it a try as a way out of the failures of the current systems.

Public support for the Swindon elections was extremely positive. Winchcombe says it increased turnout for younger voters, and that there was no time over the six to seven days when someone wasn't voting -- even at 2 or 3 in the morning. Though increase in turnout was slight, he says online votes jumped 75 percent the second year it was offered, and he received many disappointed calls the next year when it was no longer available.

The main chokepoint for secure internet voting is the vulnerability of the home PC. The scientists interviewed for this article agreed that a closed set-top box would address many of their concerns, though not all of them.

Pushing hard-coded voting appliances into American homes wouldn't be easy, but the functionality could be built into other devices, with tight controls over what software can run on the box, and how the code is audited and authenticated. Consider the brainpower that went into making HDTV video resistant to high-quality copying. Apply that, under strict government regulations, to making secure home voting hardware, and voting machinery could be embedded in your television, Tivo or cable box in time for the 2010 midterms.

Meanwhile, the problems with current elections remain. The FBI is investigating a voter-suppression effort in Virginia, in which callers posing as elections officials phoned voters who were likely Democrats and told them they'd be arrested if they visited their polling place on election day; similar schemes have dogged every election in recent memory. Many citizens abroad still aren't able to vote, due to logistics and problems obtaining absentee ballots.

The future of online voting lies in whether the threshold for adoption is perfection, or functionality. "Nobody has a good solution that doesn't in some way use the internet," said Shamos.

Until internet voting arrives, a mishmash of bad solutions occupy its space. With the computerized SERVE system deemed too insecure, this year, Missouri, Iowa and other states allowed military personnel to e-mail and fax their ballots instead.

That left soldiers with the choice between truly abysmal security and simply not voting at all.