

Prise de parole de Madame la Chancelière Anja Wyden Guelpa lors du Global Forum, Washington DC, 8 novembre 2010

Dear Giorgio,
Ladies and Gentlemen,

I am delighted to have been invited by Sylviane and Sébastien to the Global Forum to tell you a few things about the Geneva internet voting system.

I guess that a number of you sitting in this room share with me the experience that producing a secure and effective transactional IT platform is an acrobatic feat. But if you nod in approval at my remark, it may be for the wrong reasons.

It is acrobatic not because of the challenges and difficulties of the task, but because to do it properly, you have to walk on your hands - to use a metaphor. This is indeed what we did in Geneva when evaluating the risks and choosing a security approach.

The risks

What are the risks linked to internet voting? Before I answer, let me underline that the risks and their countermeasures as well as the extent of the State's control over the system differ radically in internet voting from what they are for instance with electronic voting in polling stations. This is a very important point.

Now, my answer. The public will is at risk in any ballot under any form: is it recorded correctly, is it stored correctly and is it counted correctly? Record, store and count, you recognize the vocabulary of electronic data processing. And the keyword here is "data".

Therefore, the assets that we must protect are the data stored into or running through the system. By data, I mean the voters' anonymous ID, their PIN code and their votes. And we have to do that in the three different contexts or environments that these data encounter on their journey to the ballot box:

- The voter's working station
- The internet
- The State's IT system.

To say it with an image, it is as if your ballot paper would be passed round among a number of persons before being placed by one of these into the ballot box. You understand that the ballot paper has to be conceived in a way that prevents anybody to ever see its content. Our challenge is therefore to ensure data protection in uncontrolled environments.

To do this, we took three sets of measures:

Firstly, we anonymised all data. Getting hold of the exchanges between our server and a citizen will not enable you to violate the secrecy of the vote. We identify voters based on shared secrets.

Secondly, we added noise to the data running on the web. Once again, getting hold of this data does not mean being able to understand it as there is more information than needed and the excess information is randomly produced.

The third and most important one is the channelling of the data. We developed a java applet that never leaves our server and cannot be compromised. This applet is pushed from our server to your PC and adds a layer of encryption on top of the SSL. Contrary to the SSL, however, this encryption is not driven by your browser. This applet also compares your ballot

to the universe of all possible ballots and refuses it if it is compromised, for instance by a virus hidden in your machine.

I dare say we have created a trusted chain by adopting the data point of view in our approach to risk mitigation. To go back to the image I used in my opening, this is where we walked on our hands.

In this short summary, I have not mentioned the hardening of the hardware and software, the splitting of the rights and the duties between the electoral commission and the civil servants operating the system, the simple yet robust procedures we are using, nor the use of a quantum generator to obtain the various encryption keys used in the system.

As a result, we have created a platform which is application-neutral and could perform any transaction, provided you plug in the right software the way we added the electronic ballot box and voting system.

To conclude I would like to underline that we live in a world where the added value comes increasingly from the ownership of data, information and knowledge. Yet, there is often a gap between the value of the data that we, public authorities handle or own, and the protection it is given.

In my opinion, the model we applied to internet voting has therefore a value beyond this single example. Cloud computing, which we will surely discuss during these two days, calls for a reinforced data protection of the kind we have applied.

Les questions qui suivent ne sont pas nécessairement celles qui vous seront posées après votre présentation, mais elles abordent la thématique qui sera traitée par le modérateur Giorgio Priester, à savoir la démocratie en ligne et les réseaux sociaux.

How is internet voting linked to social networks and the electronic democracy?

We have for long considered voting as an almost sacred act that could compare to nothing, something of its kind. I am not showing disrespect for the democracy by saying that voting is a transaction and as such it can take different forms and can be offered in a variety of ways.

To make it short, one of the goals of electronic democracy is to lower the access threshold to collective decision making and to include in this process groups that are at the margins of society.

We must aim at the same goals with voting, we must reach to groups and communities that are on the fringe of the society, not necessarily because they are less well off, but also because debating the common good and voting do not belong to their culture, to their habits - and not to mention disabled citizens. That is what internet voting is for.

You can compare it with the media approach nowadays. The publishers try to offer their content on several platforms; they call it the media bundle. I think that the public authorities should do the same.

And the social networks?

I could not point to any sociological convergence between social networks and internet voting. I know that in the United States, social networks are an important part of eDemocracy as we have seen for instance during the 2008 presidential election. There, they were used to mobilize voters, organize meetings and volunteers to get out the vote on Election Day.

I think it is interesting to see through that example that the US conception of eDemocracy is largely one of people organizing themselves to reach a goal, be it getting someone elected or a proposal adopted.

In Europe, on the contrary, eDemocracy is largely state-dependent. The best known examples are online petition systems implemented by local councils, the possibility to reach the British Prime Minister by email or to contact MPs online. In Europe, we do not have a tradition of keeping in touch with our representative as strong as you have in the United States. That may be why our eDemocracy is state-sponsored, as it aims at bringing the elected personnel closer to the citizens.

Another reason why I do not see convergence between social networks and internet voting is the data protection issue. I do not want to say that all is white on one side and black on the other. You may have read in the Financial Times of October the 19th an article where a Facebook engineer said that part of the problem this company has had with data leaks is linked to the way the browsers work. That is why we try as much as possible to free ourselves from the browsers in the voting transaction.

But let me tell you an anecdote. Some years ago, the European Commission drafted a new legislation on chemicals. As it was a hot topic, it decided to organize an online consultation on these new rules. Thousands of emails were sent to the commission and I remember having heard the then Commissioner for the Economy and the ICT, the Finn Erkki Liikanen, saying that this consultation was useless because it was impossible to process the huge number of reactions received.

The lesson here is that eDemocracy European style has to be well thought and organized and must rely on specific online tools able to produce a usable outcome. In the USA, I am struck by the use of off the shelf solutions, such as Facebook in the framework of eDemocracy actions. There is definitely an ocean between the two continents.

Will internet voting bring about any social change in your opinion?

I think it is very much context dependent. We have seen how eDemocracy can differ on both sides of the Atlantic. To me, the United States are amazing when it comes to appropriating new tools and inventing new uses to deliver social added value.

In Europe, where we do not have electronic voting, one change brought about by internet voting could affect the elections rules. Would it still be acceptable to vote using closed party lists when you will have a tool allowing each voter to create his own list of candidates, irrespective of their party of affiliation?

Do you think that using open source software adds to the democratic aspect of eDemocracy or eVoting?

No, I don't. The open source debate is a wrong debate.

An open source internet voting application would be auditable by any computer specialist anywhere. This would promote the IT specialist to the role of guarantor for the system's fairness, even if he may not be connected at all with the community using it.

Is this democracy? Doesn't sovereignty also encompass the freedom to choose our software reviewers? I think that a solution can be found in the ownership by the state of the intellectual property of the internet voting system. That is what we have achieved in Geneva and I think it respects both our sovereignty as well as our need for transparency.