The Tricky Business of Democracy

For its prestigious electronic voting project, Swiss Post is relying on technology provided by the Spanish company Scytl. But reporting by Republik shows that the e-voting market leader has misused EU funds, bungled elections and encountered security problems during voting.

By Adrienne Fichter (text), Thomas Rogers and Daryl Lindsey (translation), 07.02.2019

Swiss Post should be thrilled – at least in theory. Now that CHVote, their Geneva-based competitor, is to be shuttered, the national postal service is set to have a monopoly on Swiss electronic voting, or e-voting. All other providers have given up, either because they were afraid of the high security costs or couldn't meet the demands of the federal government.

Scytl should also be thrilled. Swiss Post is one of the Spanish e-voting company's biggest clients. The leader in the sector, it sells its election software to 42 countries.

But this good mood is being spoiled by mounting criticism of e-voting. More and more politicians doubt its reliability. On January 25, e-voting opponents even launched a public initiative to fight it, with the goal of placing a moratorium on the election technology until it can be proven that online voting meets the same security standards as casting votes by ballot box.

It's a far cry from just ten years ago, when people were generally optimistic about e-voting. Skepticism and resistance are spreading, and even its supporters are getting nervous. Much is at stake, especially for Swiss Post. E-voting is a prestige project for the state company, which wants to use it to demonstrate that it can keep up with the wave of digital transformation.

But Swiss Post's partner for leading the company into the digital future doesn't have a spotless record. In 2014, Scytl bungled regional elections in Ecuador so badly that all the scanned election ballots had to be counted manually at the company's Barcelona headquarters. According to Republik's reporting, several Scytl managers were even temporarily arrested as a result.

The company withholds important information about the testing of its e-voting system or requires expensive licenses for those reviews to be carried out. The company has also funneled Spanish public funds and EU research money into client acquisition instead of investing them into further development as stipulated. Meanwhile, there was also an incident involving flawed voting in Australia.

So, why is Swiss Post still even willing to work with this technology partner?

The story of Scytl is filled with successes – and slip-ups. The company, for which Switzerland has played a central role from an early stage of its exi-

stence, has reinvented itself multiple times. Above all else, the story of Scytl shows how risky it can be to outsource a government task as important as electoral procedure to a private company.

Client No. 1: The Canton of Neuchâtel

Andreu Riera founded Scytl in 2001. The cryptography expert came up with the idea during the 2000 U.S. presidential election. Riera, who died in 2006, thought during the Florida recount, which decided the election between George W. Bush and Al Gore, that an electronic vote would have to be more effective than the business of paper ballots and hanging chads. «That was the catalyst. If the most important democracy in the world had to take one month to determine who won and bring in the Supreme Court to make a final decision, then the traditional voting system was clearly failing and could benefit from the adoption of new technology», former Scytl CEO Pere Valles said of Riera in a 2015 interview with Informilo, a business magazine.

Riera, a scientist at the Autonomous University of Barcelona, had tinkered with cryptographic solutions in the 1990s. He had long been interested in the paradox of e-voting: how to reconcile the need for confidentiality with voter verification. He brought his colleagues from the research group with him to Scytl, making them some of the company's first employees.

Things went slowly at first. The scientists weren't salespeople and it was hard to explain such complicated technology to governments. Nobody wanted to take the risk.

But Scytl desperately needed a first customer, and it found it in 2004, in Neuchâtel, Switzerland. Why did the western Swiss canton offer itself up as a guinea pig? The Swiss Confederation, the federal government, had been looking for pilot cantons where it could implement electronic voting, Neuchâtel Vice-Chancellor Pascal Fontana says in response to a query by Republik. «We were looking for the company with the best expertise in terms of security.» They ended up choosing Scytl.

Neuchâtel became a test case and a turning point for the Spanish startup. Using the project as a calling card, the company grew quickly after that.

The Florida breakthrough

The money began flowing in. Several investors came on board, including Vulcan Capital, the fund controlled by Microsoft co-founder Paul Allen. With financial injections, Scytl successfully made the jump from the academic world to the open market, registering 40 patents and hiring 600 employees around the world. Until a few years ago, Scytl's 120 million euros in venture capital made it the best-financed startup in Spain.

Founder Riera, who felt more comfortable in the research world than in the corporate world, turned the company over to the new CEO, Pere Valles, and dedicated himself instead to new research ideas. In 2006, Riera died in a car accident, missing out on Scytl's biggest phase of growth: its 2008 international breakthrough. The same year that Barack Obama inspired millions of voters online, the Spanish electronic voting wunderkind won its first American client: Florida, the U.S. state that had inspired Riera to found Scytl in the first place.

Florida wanted to be the first, not the last state, Valles later told Informilo. Election officials were looking for technology that could help soldiers sta-

tioned in Afghanistan vote. Out-of-country voters were becoming the most important sales pitch for Scytl.

The demand for online voting grew, but not as fast as Scytl CEO Valles and his investors would have liked. Elections are a unique and volatile market – a fact the company learned the hard way when a 30-million-euro contract with the Republic of Congo fell apart after the country's president decided, at the last minute, not to implement e-voting.

Twenty-four election products on offer

These uncertainties led the Spanish management to change its business model at an early stage. It became a kind of one-stop shop for all forms of voting, both online and traditional. Scytl began offering software for voting machines as well as infrastructure and on-site support. To this day, it offers 24 different voting products, from purely internet voting to the operation of digital ballot boxes.

Officials in the U.S. were initially skeptical of the Spanish company's pitches. Foreign companies selling voting technology are generally met with suspicion. But that changed in 2012, when Scytl bought its American competitor, SOE, and built up teams in the U.S. Since then, 1400 of the 3200 U.S. county governments have become Scytl customers.

In trade journals and at internet conferences, the company boasts of saving democracy in developing countries. It has also released ads pointing to the risks posed by human error and to the precision and speed of a digital equivalent. Visitors to the company's website are greeted with the slogan, «We Power Democracy».

Former CEO Pere Valles claimed Scytl could help curb voter fraud. At the NOAH Conference in London in November 2015, he told a reporter the following success story from Africa: It took three months for the votes in Ivory Coast to be counted in 2010. Three-thousand people died because President Laurent Gbagbo didn't accept that his challenger, Alassane Ouattara, had won, because of the lengthy recount. Scytl technology allowed 40 percent of the votes to be counted within 24 hours in 2015. Without any turmoil.

Despite failed deals like the one in Congo, African states like Ivory Coast became the best marketing tool for the Spanish company. Scytl repeated its advertising pitch over and over again: People are flawed and untrustworthy, but the internet is incorruptible.

Encryption as a Trump Card

That's partly why online voting has become increasingly acceptable in the mainstream over the past decade. Since 2012, the number of Scytl's customers has grown along with the security concerns. It was no longer sufficient for the company to tout how efficient three-click voting was. Voters wanted to be able to trust that their votes were also being securely transmitted and correctly counted, even if they were digital.

This wasn't a problem for Scytl. Quite the opposite: It was one of its selling points. Its founder's cryptography knowledge became an asset for the company and is even reflected in its name. Scytl is a derivation of Skytale, the name of the world's first cryptographic tool – a roll of parchment wrapped around a cylinder used by the ancient Greeks and Spartans to pass encrypted messages.

The market leader in online voting is particularly proud of its work on reconciling the need for authentication with that of voter secrecy. «We have developed technology that auditors can use to see if the votes cast were the same as those that were counted», Valles said in 2015. In professional jargon, this is known as «universal verifiability», and is intended to ensure that votes cast and delivered electronically cannot be manipulated during transmission.

So far, so good. But if one digs deeper, questions start popping up about how Swiss Post's technology partner deals with public money, failures and breakdowns and security flaws.

How Scytl Handles Research Funds

There is, first of all, the issue of money. Little is known about Scytl's financial success. The Spanish company doesn't like talking about it, and although it shares news of its high growth rates and gigantic funding injections, it doesn't publish revenue figures.

For a long time, the startup had been working toward getting listed on the NASDAQ stock exchange in New York in 2017. But Scytl managers dropped the plan that year for reasons of neutrality. «In a business sector as sensitive as voting technology, going public in the U.S. is a politically sensitive matter», says Scytl spokeswoman Gwendolyne Savoy.

Countless rumors about the company's investors circulate online. Many of them cannot be sustained, like the claim that Scytl maintains connections to the CIA, or that George Soros bought the company.

But Scytl did in fact receive large amounts of research funds from the Spanish government which, reporting by Republik shows, was used in ways contrary to what had been stipulated.

Instead of spending it on cooperative work with universities, Scytl used it to stock up its product team and develop new prototypes for its customers. An injection of over 1.5 million euros from Spain's Ministry for Industry was, according to an internal document seen by Republik, used for, among other things, a «product demo» for Neuchâtel. And 900'000 euros in EU funds were spent on the development of software modules for Ecuadorian election authorities.

The document contains notes on how this use of funds is to be justified. «We wrote creative reports», one former project manager told Republik. Spain's state funders apparently didn't care, or were satisfied with Scytl's claims. No review took place. The company denies such depictions. «The money was only used for research and development», says spokeswoman Savoy.

A System Failure in Ecuador

Then there's the issue of reliability. A lot can be heard about Scytl's success, but less is known about the company's mishaps. There is, for example, the case of Ecuador's 2014 regional elections, when Scytl received a contract to run the voting machines in several parts of the Latin American country.

On Election Day on Feb. 23, its technology failed on multiple levels. In some districts, Scytl software didn't work at all. The program couldn't correctly read and interpret a large proportion of the scanned ballots, and the vast

amounts of data caused several servers to crash completely. The situation proved to be especially dramatic in the country's jungle regions, which have poor internet infrastructure.

According to a report by the Union of South American Nations (UNASUR), «the system was unable to process the amount of scanned information». Although technology bloggers later argued that the system hadn't been sufficiently tested in advance, Scytl, in turn, blamed Ecuador's poor infrastructure.

Ecuador's National Electoral Council angrily sent Scytl staff, along with the ballots, to Barcelona, where the company had 72 hours to count them by hand. The Ecuadorian government kept several of the company's managers in the country as collateral, including project leader Osman Loaiza, temporarily detaining them for «breach of contract».

All employees were called in to headquarters to count the ballots. According to a former developer, they slept on mattresses in the office. But, even so, there were too many ballots and it took one month for the company to announce who had won the districts it had been responsible for. The collaboration ended, and Scytl managers had to answer to a court.

Former employees now say it is strange that the case barely attracted any international attention. But Scytl disputes claims the elections in Ecuador ended in disaster. Scytl's spokeswoman says it marked an improvement «in the process overall compared to the regional elections in 2009».

And then there's the security issue. The most delicate incident for Scytl took place in 2015, during the parliamentary elections in the Australian state of New South Wales, where voting was carried out using Scytl software called iVote. Researchers Alex Halderman at the University of Michigan and Vanessa Teague at the University of Melbourne examined the system more closely and discovered a serious vulnerability that allowed them to circumvent the encryption between the voter's browser and the e-voting system.

If hackers had done this with nefarious intent, it would have been possible to lift voters' anonymity and manipulate the vote. It's not like Scytl bunkers down after these kinds of incidents. Indeed, the company reacted to the experts' criticism in a relatively thorough manner, but always defensively.

Which also raises the issue of transparency.

A Lack of Auditability

Scytl's leadership team is indeed aware of the potential risks to democracy posed by e-voting. They also know that their product is vulnerable to hacking attacks. That's why former CEO Valles brought scientists and encryption experts into the advisory committees and cooperated with expert reviews.

But it has remained stingy with the truly important information. Critical examination of software requires more than just familiarity with the source code. Systems can only be set up and tested with the help of detailed documentation, and according to reporting by Republik, it's precisely this information that the Spanish company won't give out.

When queried about the subject, the company claims that the release of the complete documentation wouldn't necessarily improve security. After being asked about this by the technology magazine Ars Technica in 2016, a

Scytl spokeswoman answered flippantly. «(Voters) don't have the ability to review the source code of their (online) banking either», she said.

Or the company also claims that a public examination of the documentation would jeopardize its business model because it would allow competitors free access to Scytl's software and the know-how it has built up over years. «A public review does not allow Scytl to control who has access to the intellectual property», the company wrote in one report.
Research papers show that Scytl managers try to avoid being overly transparent.

Researchers at the University of California, Berkeley, wanted to investigate voting-machine software in Florida as early as 2008, but didn't have access to documents that were crucial to their research. As a result, the Berkeley researchers couldn't verify whether the system worked properly and weren't able to carry out test attacks on the system.

The Debacle in Norway

The same problem repeated itself three years later, in 2011, when Norway decided to introduce electronic voting. The government settled on Scytl software, and to gain the trust of the Norwegian population, the authorities published its source code.

But the code was not only unusable, but also flawed. A research group from Switzerland ultimately pointed out the weakness to the Norwegian government. Reto Koenig, a professor of computer science at the Bern University of Applied Science (BFH) who examined the Norwegian e-voting system at the time, said the «pile of code» they had received would not have worked to get it up and running.

The group working with Koenig had to improvise and, using simple programs, found «a bug that had hidden itself deep in the cryptography». This discovery didn't look good for Norway, an online voting pioneer whose e-voting system had already been in use for two years.

Other researchers came to the same conclusion as the Swiss team.
Koenig and a research delegation from BFH were invited to Oslo, and their presentation in front of a committee of OSCE election observers made an impact. In 2013, Norway restricted e-voting and, one year later, the e-voting project was shelved completely due to the concerns of citizens and because of changes in the political landscape.

But this hasn't stopped Scytl from portraying its operations in Norway as a success story. On its website, the company boasts it «has received over a 94 percent voter trust evaluation» for the e-vote project in Norway.

Contradictory Statements

How can Scytl's business practices be reconciled with the Swiss government's high security and transparency requirements? How secure will Swiss Post's e-voting offering be? And what exactly is the arrangement between Swiss Post and the Spanish e-voting giant?

Swiss Post has been a Scytl client since the end of 2014. A spokesman for the government-owned company says that a private supplier was chosen because «developing it on one's own would have been too expensive and

risky». Switzerland – with its semi-direct democracy – is one of Scytl's most important strategic markets.

But when it comes to transparency and auditability, Scytl's statements have been contradictory. At a 2017 trade conference called Swiss Cyber Storm, Jordi Puiggalí, Scytl's longtime head of technology, gave a presentation-. When one participant asked him whether Scytl was prepared to release its source code, he at first answered evasively, then added that a full disclosure, which would release Scytl's core software under a free license, was out of the question for him.

On this point, however, the Swiss Federal Chancellery is firm. Article 7b of the federal regulation on electronic voting (VEleS) states that «everyone may examine, modify, compile and execute the source code for non-commercial purposes, as well as write and publish studies on it». In other words, citizens can do anything with it except use it for commercial transactions.

Every e-voting supplier must agree to this transparency clause. To build trust among citizens, anyone wanting to test the system should make his or her findings public, says Mirjam Hostettler, project manager of Vote électronique at the Federal Chancellery. The word «trust» is mentioned in the Federal Chancellery's explanatory report multiple times.

This obligation for transparency was also a precondition in the call for tender by Swiss Post that Scytl took part in. «For Scytl, it was clear from the start that this criterium was an integral part of the collaboration», spokeswoman Gwendolyne Savoy told Republik.

Is It Safe?

When it comes to security, Swiss Post has some weighty arguments to dispel doubts. Unlike in Australia, voter verification in Switzerland isn't meant to take place via text message or another digital channel, with the cantons instead sending the code for identification and verification via mail.

Also, the systemic failure of Scytl technology in Ecuador is irrelevant to Switzerland. There, the issue was related to voting machines, whereas the system in Switzerland entails at-home voting on computers. Swiss Post also points to the fact that the e-voting system is to be managed by Swiss Post itself and that Scytl will have no access to it.

Swiss Post is currently having its project – which is to say, its system, protocol, software and procedures – inspected by KPMG, a certification body accredited by the Swiss government. If the certification is successful, the company will begin a transparency campaign in which people will be asked to hack the system.

This is called a «public penetration test» in specialist jargon. In another move, it will publish the source code, put together a test system and announce a hacker reward, thus inviting the world to test the security of its product. And all of this is required under the federal regulation.

What Will Remain Secret About the Deal

The test will also be decisive for Swiss Post's image. The company wants to avoid giving the impression that «digital democracy» in Switzerland is being driven by private companies. Although Geneva has said it will move to shut down its CHVote e-voting system, it does plan to go ahead with use

in 2019, albeit in a limited capacity due to missing certifications. The system is public and financed by taxes, and the software code is available on Github, meaning citizens can download it onto their computers and test it to their heart's content.

The same isn't true of Swiss Post and Scytl. Thus far, they have only given access to a small circle of auditors.

The deal between Swiss Post and Scytl remains murky. The Spanish company has emphasized on multiple occasions that transparency has its price, but a Post spokeswoman confirmed to Republik that they did not have to pay for a special license.

The state-run company isn't revealing how much money it is paying Scytl and a formal request for information by Claudio Zanetti, a member of the lower house of parliament, the National Council, with the right-wing Swiss People's Party (SVP), on this issue still hasn't been answered. The only publicly known figure at this point is the 250'000 franks that the federal government and the cantons are paying to carry out the penetration test.

The Hackers Are Ready – And, So Far, Successful

Despite the many precautions being taken by the Swiss Confederation and Swiss Post, critics aren't staying quiet. They have a knockout argument: How can we know that the software that will be tested will be the same one that will be used on Election Day in 2019?

«Even under ideal circumstances, the trust problem won't be solved, because the citizens can't check whether the source code that is published is the one that will really be used», says Hernani Marques of the Chaos Computer Club, one of e-voting's most vocal opponents.

Mirjam Hostettler of the Federal Chancellery contradicts this argument. «When they implement updates», she says, «the operators need to show which functions they have changed. If it is many functions, then new certification is required».

A «hacker performance» might also be in the offing. Marques, a software developer, and his colleagues would like to simulate and crack Swiss Post's e-voting project. «We can show on camera how the system can be infiltrated so that it perceives everything as being clean, but the results still don't reflect the voting choices of the groups taking part in the simulation».

It wouldn't be the first time an e-voting project would be ended in this way. In Geneva, a computer scientist named Sébastien Andrive hacked the system, leading the project to introduce individual verifiability. The Chaos Computer Club then conducted a hacker attack on that system, and a few weeks later, the Canton of Geneva announced that it would shelve its e-voting product.

An Unsolvable Dilemma

That's why SVP National Council member Franz Grüter seems unimpressed by Swiss Post's transparency offensive. «Our country isn't prepared for recognizing and warding off cyberattacks», he says. Meanwhile, the initiative for a moratorium on e-voting is about to start collecting signatures. The committee behind the initiative is broad and diverse and includes Tamara Funiciello of the Young Socialists, the youth wing of the Social Democrats,

as well as Benjamin Fischer, the president of the youth wing of the SVP, and Balthasar Glättli, a member of the National Council with the Greens.

For now, a solid majority of Swiss citizens are still positively disposed toward e-voting, and only a small number of people seem interested in the debate surrounding the technology. Political scientist Uwe Serdült argues that according to the most recent poll by the Center for Democracy Studies, most people don't care whether the source code is published or not.

Nevertheless, Swiss Post is nervous. Although it doesn't yet need to convince the population about its product, it does need to bring the relevant political leaders in the cantons on board, and they are becoming less and less well-inclined toward e-voting. The Canton of Zurich is considering withdrawing. The Canton of Glarus has canceled its plans and politicians have also become skeptical in Aargau. At the moment, Swiss Post's only e-voting partners are the cantons of Basel City, Fribourg, Neuchâtel and Thurgau.

If the growing doubts keep anyone else from joining, the e-voting project will have failed even before the law has been changed to accommodate it. Most Swiss citizens would then still vote with pen and paper in 2019.

And even if the product tests do go perfectly, it wouldn't make the Scytl dilemma disappear. Democratically elected governments are dependent on the trust of their voters – and, as such, must communicate in a transparent manner.

A private, profit-oriented company that provides a service that is central to state policy, wants to sell its products to as many customers as possible and at the same time protect its trade secrets?

Those are two interests that ultimately cannot be reconciled with each other.

It's your turn!

What do you like about this article? Is there anything that should be added? Do you disagree with certain parts? Your fellow readers and the editorial team are looking forward to your knowledge and your perspective. Join the conversation on our dialogue page.