Eesti Päevaleht

Estonia Daily

Original Estonian: PDF | HTML - English Version: PDF | HTML

Michael McKibben: Facebook is built on technology stolen from us

October 14, 2013 4:35 PM EET

Ave Tampere
Editor
Eesti Päevaleht
(Estonia Daily)

Leader Technologies' founder and CEO Michael McKibben talks to Eesti Päevaleht about the row with Facebook, and the security issues facing the Internet today.

Leader Technologies' leader Michael McKibben says social media is his invention. Photo: Urmas Kamdron

Pärnu Konverentsid

On October 10-11, 2013, Michael McKibben was a keynote speaker at the Pärnu Leadership Conference 2013 – "A Matter of Faith." About 400 of Estonia's leaders in government, commerce and industry were in attendance. Pärnu is a popular resort city on Estonia's Baltic coast. McKibben spoke about his work with Estonians in the late 1970's and early 1980's who taught him about leadership, faith, courage and perseverence in the face of extreme hardship.

His friends were systematically persecuted and harassed by a militantly atheistic Communist government; some were even imprisoned and murdered by the police state.

That collaboration resulted in an unimaginable ideological thaw in which members of the Supreme Soviet and Moscow's cultural elite promoted and distributed music by Living Sound, an American Gospel music group, thorough the state-run Melodiya record label, on Soviet Central TV (CT USSR), and on the official 1980 Moscow Summer Olympic film. McKibben was Living Sound's European Director.

McKibben, an Ohio State University engineer and professional musician, said the moral fortitude of his Estonian friends inspired him to step outside the programming molds of the 1990's and invent what is now called "social networking."

A moment before the opening of the 25th Estonian Song Festival (2009) at the Tallinn Song Festival Grounds. It is one of the largest amateur choral events in the world. In 1987, 300,000 people (more than a quarter of all Estonians) gathered in this mammoth outdoor concert venue to assert national independence and protest continued Soviet occupation. Photo: Wikipeida.

Estonia joined the European Union in 2004, and ranks high for press freedom, economic freedom, civil liberties and education. Estonia is often described as one of the most wired countries in Europe.

Estonia has been settled for 11,000 years. In the last millenia, Estonia has been occupied almost continuously by foreign powers, including Vikings, Germans, Swedes, Russians, Nazis and Soviets. Despite these occupations, Estonian culture and language thrived. Song festivals have played an especially important role in Estonian national identity. Estonia's prestigious University of Tartu was founded in 1632, four years before Harvard University.

The Soviet Union occupied Estonia from the end of World War II (1945) until independence in 1991. McKibben just learned on this trip that his efforts as a part of the Living Sound musicial ministry helped inspire the choirs and musicians behind Estonia's bloodless "Singing Revolution" (1987-1991).

A member of one of those choirs, now a Tallinn harbor official, was attending the Pärnu Conference. He told McKibben that his Tallinn Oleviste choir recorded and distributed their songs on the studio equipment that McKibben and Living Sound's British supporters helped provide 32 years ago.

In 1991, Estonia's Soviet occupiers, then led by Mikhail Gorbachev, decided to leave Estonia rather than run their tanks over unarmed choirs. A number of Estonians told McKibben and his wife, Nancy, that their commitment to Estonia during those dark days "opened a window" of new possibility, faith and hope for them.

Ave Tempere took the Pärnu Conference opportunity to conduct this interview.

Ave Tampere's complete interview with Michael McKibben

Why do we need services like the ones Leader Technologies provides and who needs them the most?

Over 1 billion people on the planet use my invention. It's called "social networking." We began inventing in 1997 after I had completed the rebuilding of AT&T's email interface in time for the release of Windows 95.

Having seen the strengths and weaknesses of existing client-server technologies used in global collaboration, I saw great possibilities to rethink the way large-scale collaboration occurred using the emerging Internet.

Back then the Internet had fewer than 10 million commercial users and the browser wars were just heating up. The popularity of our invention probably answers your question, since many of your readers probably used it today.

Was there a specific "moment of recognition" or something that gave you the idea?

We were working backwards, from a product design perspective. We collectively acknowledged that none of us had the complete picture of the ultimate collaboration tool needed, so we started by employing a non-traditional approach.

We had a lot of experience with what did and didn't work. So, we started from the perspective of what didn't work, and kept crossing off those items from the list. What emerged in the end was a design that did work, clearly.

This is the highest of design approaches, but the most expensive and time-consuming kind. By committing to this approach, we had a breakthrough.

We invested over $10 million dollars and 145,000 man-hours into this creative work. Numerous "angel" investors financed us. These were risky investments and my investors have been cheated by unscrupulous actors.

That is why we are so determined not to allow Facebook and the Obama administration to simply confiscate our invention. If we do not correct this injustice, the message to American inventors will be not to bother inventing and filing for patents and copyrights since your ideas will just be stolen by your government inside the Patent Office, by the courts, and by the banks.

Estonians know a lot about government-led property confiscation, don't they? Is America preparing to repeat this tragedy of modern history? The answer is yes, if our experience is any indication.

How does Leader Technologies differ from others who provide analogous services?

We hold the core patents on social networking and social apps. There are many squatters on the land, but we hold the deeds.

How about from the users' end?

The best product design is unseen and intuitive to the user, yet it unconsciously guides that user through the choices to be made.

For example, in automobile design, controls and choices must be placed strategically on the dashboard so that the driver instinctively knows the choices and can select them easily.

However, these design issues, while important, took a backseat to the "secret sauce" of our innovation. How we store and retrieve data using Internet programming protocols was the magic.

For example, when you tag a photo, how that data is “wrapped” with metadata about that photo (things like other people who are tagging that photo, the text in those tags, information about the file, other related links, etc.) and the users viewing the photo is the magic.

In the past this information, if recorded at all, was stored separately from the users who created and view it. The unification of this information, accessible in real time on a large scale, was the magic.

In other words, before our invention, a person could make a photo file available on a website, and another person could download it. Then, a third person could download it too. A new copy of that file was "replicated" each time it was used.

This created many copies or versions of the same photo. Version control was a big problem. It also consumed a lot of computing resources just to move all these copies of the same file around. In addition, the file did not retain data about the people who viewed and shared it, so it had no ability to gather context information automatically about how it was being used.

For these reasons, the previous "client-server" paradigm could not support a lot of users simultaneously.

This change in the way users interact with a single piece of the data is our innovation.

You mentioned in one of your emails that you do not use Skype much. Why is that?

Skype is a wonderful program. I used it just recently to speak with my daughter who was in Tuscany on a work-study project. However, we have our own corporate web and teleconferencing service that includes video capabilities.

Also, Skype’s acquisition by Microsoft in 2011 causes us to have serious concerns. Microsoft is deeply embedded in the Facebook infrastructure where hacking and invasion of privacy have become the modus operandi. No one can be sure who in those companies is secretly hacking into one’s Skype call.

Is the Leader Technologies' web and teleconferencing service less vulnerable to hacking then?

Hacking is a combination of technological and sociological abuses. We would be remiss if we disclosed the unique combination of tools used to thwart intrusion. So the best answer I can give, without giving away the "secret sauce," is that it is combination of technical and sociological solutions.

How do you feel about the recent revelations on large-scale surveillance?

They are deeply disturbing and should be unacceptable to all free people. This level of snooping reminds me of the Big Brother intrusions of the old Soviet Union.

The difference this time is that it can all be done on a global scale by snoopers in their pajamas. I have spoken with U.S. Congresspersons and veterans of previous administrations who are equally disturbed by the revelations.

That said, I understand that linking relationships can expose bad-guy networks more quickly. I get that. But knowledge of those networks can just as easily be exploited by bad guys against law abiding citizens.

Assuming for a moment that 999 out of 1,000 actors at the NSA are honest, it only takes one bad actor to compromise millions of linking relationships carried out on a memory stick in one's pocket. If we are going to be expected to trust these institutions, then we need to know that effective checks and balances are in place. Snowden proved they are not.

The fact is the untrustworthiness is deeper than that. Last month a dozen NSA employees were caught using these surveillance tools to spy on the emails and phone calls of current and former spouses and lovers. This must be stopped systemically. Trust is hard to build, but easy to destroy.

What do you think of "the innocent have nothing to fear" excuse for surveillance?

It's laughable. Corruption is endemic to the human condition. Bad actors exist in every bureaucracy and society. Without effective third party checks and balances, abuse is inevitable.

Government institutions are comprised of people. Some of those people do the right things on principle. Most follow the rules. But, some people in every bureaucracy sneak around and do the wrong things at every opportunity. To the latter, such excuses as "the innocent have nothing to fear" are nothing more than a smoke screen to fool naïve, unsuspecting people.

In what other profession am I expected to trust so blindly? I think the problem here is the nature of software. Its gears and pulleys are unseen electrons in bits and bytes, so a user has no way to double check.

This is where the digital professions must raise the ethical bar and stop the exploitation of people's lack of knowledge about how data processing works. We need technologists with integrity who make the moral choice not to exploit the data of others just because they can get away with it.

How do we get the "average" Internet user to realize that software providers have personal, political and economic agendas—agendas that might harm them?

Users typically focus on function and usability—how I get "x" done. They don't even think about the risks and exposures. They assume the software provider is acting in good faith. Leader strives to live up to that responsibility. We are trying to set a higher standard on behalf of users. The industry must stop the exploitation. It is immoral.

Noble societies do not exploit the innocent and ignorant, but rather, they set proper ethical standards and live by them. Must the tech world repeat the mistakes of history? The jury is still out. Right now, the exploitation is rampant. Election manipulation, abuse of privacy, bank transaction siphoning, identity theft, titillation, trend pandering.

Just listen to the equivocation of many tech expert on security and privacy. The responses are full of non-concrete platitudes and pacifications rather than practical actions. It's often just around the corner, but never here and now. The here and now is technically possible, here and now. That's what's next for trusted, secure social, we believe.

How is the court case with Facebook going? What did they steal from you?

The engine running Facebook is our invention. Essentially, everything a Facebook user does uses our invention. For example, the tagging of a photo on a friend's profile. Also, the entire Facebook API engine to build third party apps is our conception and patent. What seems so commonplace now was impossible in the prior files and folders Windows world. We changed the paradigm.

Facebook was found guilty on 11 of 11 counts of infringing our U.S. Patent No. 7,139,761 by a jury after a two-day battle of experts—four university computer science professors, two for us and two for them.

In addition, despite Facebook's global call for hackers to feed them prior art to prove we were not innovative, they failed to prove that any prior art existed. Despite Facebook's guilty ruling, the federal district court ruled in favor of Facebook anyway—citing an obscure law called on-sale bar (that we tried to sell the invention too soon).

Facebook presented no hard evidence of the on-sale bar accusation, and instead put forward attorney-fabricated evidence that the judge shockingly affirmed.

Our first clue that something was amiss came when the magistrate judge, an Obama nominee, replaced the 25-year veteran judge on our case just one month before trial. His first act was to allow Facebook to add the on-sale bar claim.

We only discovered years later that President Obama's Justice Department adviser on this nomination was a partner at Facebook's law firm. The new judge simultaneously blocked us from conducting additional discovery on this new accusation.

That judge was then confirmed to his judgeship one week after our trial. We didn't have notice regarding their new claim and had no opportunity to conduct discovery and get expert testimony to refute it. Without expert testimony on software matters, other evidence is pointless, yet that judge broke all the rules to affirm it anyway.

We appealed to the three-judge Federal Circuit appeals court in Washington D.C. That court ignored well-settled precedent that would have been favorable to us and refused to reverse the lower court. They even timed several of their rulings to coincide with key Facebook IPO announcements.

Not even that court could affirm the lower court's opinion from legal precedent, so they fabricated new evidence and argument in the secrecy of judges' chambers to justify not ruling against Facebook. Then, the U.S. Supreme Court refused to hear our petition.

As if this were not enough, investigators are finding intimate ties amont Facebook's law firms, the White House, the Judicial branch, Wall Street, Silicon Valley and certain members of the Senate and Congress. Even the Patent Office started a Facebook page during our proceedings and encouraged its 10,000 employees to "like" it and visit daily.

The Patent Office is currently attempting an unprecedented third reexamination of our patent to try and kill it by administrative fiat. They assigned a patent judge and director previously employed by two Facebook stakeholders, IBM and Microsoft, despite the fact that our claims have been affirmed three times previously.

Investigations into the judges' financial disclosures reveal that all of the judges in our case hold large amounts of stock in Facebook interests. A judge is not allowed to hold even one share of stock in a company that would bias his or her impartiality.

Recently, direct relationships have been uncovered among Faceboook, the judges in our case, key beneficiaries in the 2008 bank bailout and green energy stimulus, and the technologists behind HealthCare.gov.

To quote Alice in Wonderland, the Leader v. Facebook circumstances just get "curiouser and curiouser."

Where do you think the future lies for young people? What's the most up and coming area worth putting effort in to guarantee success?

I think trusted, secure social—apps that respect personal property, security and privacy. We hope our platform will be central to this effort. The civilized world is starting to figure out that the current social environment hijacked our invention for illicit purposes.

They'll realize that trusted global services cannot be built on the shifting sand of privacy, property and security invasion—no matter how many Orwellian "to enhance social engagement" excuses are used.

Facebook's "one size fits all" approach is designed to do three things—snatch personal data from financial transactions, sell your data to favored third parties to maximize advertising revenue, and manipulate elections.

Hopefully, people are coming to realize that what you don't know may be hurting you in ways you cannot imagine. Estonians over 30 know a few things about snoopers and how they hurt people.

What people need are digital tools they can trust. They need tools that respect users' privacy, property and security in actual fact. Real security is much more than a catchy public relations buzz word.

Privacy and security is a lot of serious, professional engineering work backed by the integrity and commitment of moral, ethical purveyors. They need tools that can adapt seamlessly and dynamically to these requirements. That's what we invented. However, Facebook exploited only the "no security" and "no privacy" portions of our invention.

I see trusted, secure social as the next wave. It will be with an entirely new group of developers since the first waves of self-described hackers have proven themselves untrustworthy. The words of Jesus in the Sermon on the Mount come to mind: "You shall know them by their fruits."

How do we get the "average Joe" user to care enough about their privacy so that they would switch from the less private technologies and favour perhaps less popular, but more secure services? (As in, how would we get people to move away from, say, Facebook, en masse?)

Here's where the media can help much more than it has done to date. The risks and harms of "open" data must be publicized—theft, kidnaping, extortion, drug pushing to teens, harassment, etc. These real world examples will help the uninformed "average Joe" about how they are hurt.

The ethical dilema for the media is its growing dependence on advertising revenues generated by the social media providers who are the worst privacy offenders.

Democracy cannot survive without a free and independent press. We can only hope that the press figures out how to do its job in the midst of this messy conflict. We need the free press to be a watchdog against corruption, fraud and abuse.

But in the current environment, too many in the press have become little more than propaganda outlets for the social media providers who, besides their security and privacy abuses, are making false intellectual property repesentations about their software platforms. I spoke about the danger of "The Pravda Effect" in my Pärnu speech.

Soviet citizens used to joke about having to become experts at reading between the lines because their media had no independence. [Pravda (Правда) (English: "Truth") was the official newspaper of the Soviet Communist Party.]

Sadly, it appears that media independence is marching in lock-step backwards to the failed Pravda model by sacrificing itself on the altar of social media advertising revenue. This is a clear and present danger to all freedom-loving people, in my opinion.

Why would/should we trust one corporate service provider over another?

Reputation, certifications, underwritings (third party validations and certifications), indemnities, warranties (e.g., Underwriter Laboratories, etc.), deeds over words, audits, accountability systems, systems, procedures and protocols. Trust is never one thing, or a magic thing. It is a combination of consistently well-executed elements.

How much do you know about Estonia? Would you invest here?

I love Estonia! I poured much of my early career helping Estonia fight tyranny. I have been here numerous times. I was the European Director of a Gospel music group called "Living Sound." Estonia was the springboard for our work throughout the former Soviet Union. [View YouTube video on some of the Living Sound work in the U.S.S.R.]

We invested hundreds of thousands of dollars and much manpower, equipment and material into our collaboration with many brave Estonians who were standing up against oppression.

So, would I invest in Estonia? I have! Would I do it again? That has always been a dream. Perhaps this speaking invitation will be the spark. Perhaps Estonia will lead the way with trusted, secure social networking paradigms. The opportunity is real and the need is now.

• • •

Brief Introduction

Leader Technologies Inc.

- Founded 1997
- Located in Columbus, Ohio USA
- Provides web-based collaboration platforms for data, voice and e-mail, voice messages, faxes, conference calls, web conferencing, file sharing, document management, video, votes, chat, messaging, message boards, system administration, etc.
- The Company's software invention has over 1 billion users on Facebook alone.

EestiPäevaleht

Eesti Päevaleht ("Estonia Daily") is a major daily Estonian newspaper, from the same publishers as the weekly Eesti Ekspress.