



Hoodwinking the censors

Revenge of the nerds

Three computer geeks at the U of T are renowned developers of anti-censorship software, including a program out this month that could allow people to outwit the world's most repressive regimes

May 7, 2006. 07:16 AM

ANDREW CHUNG

STAFF REPORTER

Looking at them you might not guess it. But deep in a basement room on the University of Toronto campus, three unassuming computer hackers with messy hair and wrinkled T-shirts are working to tear down China's "Great Firewall," the most sophisticated Internet censorship system in the world.

They are self-confessed computer "geeks." They don't go to the gym much, or see much sunlight. They talk about "routers" and "nodes" and "secure socket layers" like they were saying, "Hello," or "How are you?"

But the computer smarts of Ron Deibert, Nart Villeneuve, and Michael Hull, combined with their passion for politics and free expression, have led them to develop a highly anticipated software program that allows Internet users inside China and other countries, such as Iran, Saudi Arabia and Burma, to get around repressive censorship and not get caught.

Their innovation is called Psiphon, and it's being launched at the end of this month.

"It's enormous," says Deibert, 41, a nerd-meets-aging-punker kind of guy who directs the Citizen Lab at the U of T's Munk Centre for International Studies, where the trio work. "If it works the way we hope it does and is distributed worldwide, it will have a huge impact on freedom of speech."

Others watching Psiphon's progress agree. "We've been trying to circumvent both the firewalls and the censorship surveillance," says Sharon Hom, executive director of New York-based Human Rights in China. "So it's something we are very, very interested in."

Psiphon takes the concept of a third-party computer doing the work yours can't because of censorship, and protects it by relying on trusted friends and close family, to create a program the creators say is nearly fail-safe.

The program is needed more than ever, as the number of countries that censor or filter the Internet continues to grow. China alone has reportedly spent hundreds of millions of dollars on its Great Firewall, as it's known outside the country. Thousands of people stand guard on it.

China blocks countless websites, from ones featuring porn to those devoted to Falun Gong, a spiritual movement banned in China. Anything on human rights is off-limits. Same for democracy.

Late last month, the wildly popular website Technorati, which searches the Internet for blogs, or personal Web journals, vanished in China despite the fact that the country has one of the fastest growing blogospheres in the world. A spokesperson for the San Francisco-based Technorati told the *Star* it wasn't clear how or why the

Censorship: Foreign filters

China has the most sophisticated and effective Internet censorship regime in the world, employing North American technology from Cisco Systems Inc. and Canada's Nortel Networks Corp., among others, to filter out banned material. But China is just one of a growing number of states censoring the Internet, using primarily American filtering programs. Here's a list of states, the technology used and what's censored:

Yemen Websense, pornography, gambling, proxy servers, gay and lesbian materials

Tunisia SmartFilter, political opposition, human rights groups, privacy-enhancers

Burma Fortinet, political opposition, democracy movements, pornography

Iran Previously SmartFilter (now unclear), pornography, gay and lesbian materials, women's rights

United Arab Emirates SmartFilter, pornography, gambling, religious conversion, Israel-related

Saudi Arabia pornography, gambling, religious conversion, censorship circumvention

Source: The Citizen Lab, OpenNet Initiative

Tag and Save

[Tag and save](#) this article to your Del.icio.us favourites.

[What is Del.icio.us?](#)

POWERED BY 

site was blocked.

So the Citizen Lab taking on powerful censors such as China is a lot like David going into battle with Goliath.

"It's a huge uphill battle," Deibert concurs. "The trajectory in terms of global politics is toward greater state control (of the Internet). I see closure everywhere."

What does Villeneuve, 31, who spawned the idea of Psiphon, think about challenging the likes of China? He puts down his Che Guevara mug and thinks for a moment. He shrugs his shoulders and smirks: "It just seems like the right thing to do."

The cause of the Citizen Lab is hacktivism. Villeneuve, 31, didn't invent the term. But he played a key role in defining and shaping it.

Hacktivism is the melding of hacking and social or political activism. Hacktivists have a common enemy, Villeneuve once wrote in *The Hacktivist*, an online magazine he founded: "the repressive use of laws and technologies by private corporations and governments to increasingly monitor and control the Internet."

Deibert and Villeneuve found hacktivism in different ways. As a teenager from Vancouver's east side — the "wrong side of the tracks," he says — Deibert listened to local punk groups like DOA and watched private eye shows like *The Rockford Files*. In university, he attended nuclear weapons protests and demanded American warships not pass through the city's harbour.

He also had a fascination with taking things apart. From amplifiers to motorcycles, it was a compulsion that, upon reflection, seems a lot like hacking to him now.

"Hacking is an important philosophy we need to recover in our society," says Deibert, now the father of four young children, "because so many systems of control are embedded in technology, most of which we're unaware of."

"The more we take the screws off and understand how things work, the more we'll have citizens in control of their lives and the technological society they live in."

He went to the University of British Columbia and was fascinated by information technology and how it changed world politics. He wrote a book on the subject. He encourages the questioning of authority, of breaking rules for the greater good. He's proud his students call him the "Hacker Prof."

The Citizen Lab was born in 2000 out of the Hacker Prof's need for a space to do cutting-edge work on activism and information technology. But lately it has turned its eye toward censorship. Along with Harvard and Cambridge universities, it takes part in a group called the OpenNet Initiative, or ONI, which calls attention to Internet filtering around the world.

Harvard researches legal aspects of Internet censorship. Cambridge organizes activists in censored countries to do research. Toronto, meanwhile, performs the technical research. It has developed the critical software the group uses to investigate censorship. And of course, it has developed Psiphon.

None of it would have existed without Deibert's first moves, says fellow Canadian Rafal Rohozinski, director of the Cambridge unit. "He managed to convince a fairly conservative university to look at this and realize this kind of thing really matters," he says.

The Citizen Lab uses the techniques of spies to secretly deploy software it developed that automatically checks for censored websites inside various countries. Sometimes the lab performs tests remotely, taking control of unprotected computers inside the censoring country without permission. This poses an ethical controversy, but Deibert says it's for the greater good: "We don't worry about that too much."

The Lab even has "black boxes," mini-sized computers that can be "planted" discreetly inside these countries to run the tests. "This kind of research is illegal in almost every country we do it in," he adds.

The Lab can also decipher how the repressive countries filter digital information, and which technology they use. It has demonstrated that Iran compels its Internet service providers to do so. China, however, blocks mainly at its borders, where the Internet enters the country, using sophisticated routers. When someone requests a banned site, the request does not get past the gateway. China also requires Internet providers, cybercafés, and websites to filter.

'If it works the way

we hope it does ...

it will have a huge

impact on freedom

of speech'

RON DEIBERT

Director, Citizen Lab, U of T

How does the filtering actually work? Last week, Villeneuve ran some tests to find out how Technorati was being blocked, and it turns out, he says, China is not just filtering out the URL itself, <http://www.technorati.com>, but the keyword, "technorati," which will capture any other sites also carrying it.

Even though others are working on anti-filtering software, Deibert and Villeneuve are now known as the foremost experts worldwide. Villeneuve has written a guide for Reporters Without Borders on getting around censorship. In February, he testified before the U.S. congress on China's system. Says Hom: "They're watching the watchers."

Villeneuve, who wears shorts and flip-flops to work, comes from the same neighbourhood in East Vancouver as Deibert, but his anti-establishment streak didn't come until after high school.

While working at a print shop, he started reading Karl Marx and Noam Chomsky, and when his roommate got a computer, he started roaming around hacker chat rooms. He found out how to extend the hours of their dial-up Internet for free.

He became a fervent anti-globalization activist, and got his first taste of tear gas in 1999 at the Seattle protests against the World Trade Organization. He started writing about the growing world of hacktivism.

Eventually he went back to college and then transferred to the U of T. There, he took one of Deibert's classes and wrote a paper on censorship in China. Deibert asked him to join the Citizen Lab. Now, he says, he's a "programming geek."

His values still colour his work. "We have a global system that doesn't value that this technology is being used to undermine people's human rights, and that's not a valid concern for the WTO to restrict the flow of trade."

Hotly debated both inside and outside the Citizen Lab is the morality of North American companies that sell their products to regimes like China. Microsoft has removed controversial bloggers from its Chinese blog-hosting service. Google, which was shut down in China 2002, launched a highly censored version of its service there in January. And information provided by Yahoo to authorities has led to the arrest and detention of at least one person, journalist Shi Tao. Cisco Systems Inc. and Canada's Nortel Networks Corp. have also been fingered for selling the network equipment used by Chinese Internet police to filter the Web.

The third member of the Psiphon team, 42-year-old Michael Hull, was hired in January to make the program user-friendly. He's been writing code ever since high school, when he created a simple program on his first computer to graph an object as it approaches the speed of light. Trained in physics, Hull sold his document encryption company in 2003. "Over the years I've been building commercial, private software to solve problems for corporations," Hull says. "So this is nice because it kind of flips it all around. It's a way to give back while I have a chance."

More than a few people view the work of the Citizen Lab, and Psiphon, as important. The ONI as a whole receives funding from several major U.S. foundations that promote peace and democracy, including a recent \$3 million from the MacArthur Foundation in Chicago. In addition, the Citizen Lab has received money from the New York-based Open Society Institute, which supports human rights projects and whose patron is billionaire George Soros.

And people are keenly awaiting the launch of Psiphon. "It's a very important contribution," says former Beijing resident Xiao Qiang, a long-time activist and now head of the China Internet Project at the University of California at Berkeley.

While it won't be a silver bullet, Qiang says, Psiphon will be a key tool for the relatively small but highly influential group of outspoken journalists, bloggers and activists inside China who dare to access information from the outside in the hope of creating a more open society.

To understand Psiphon, it's important to first understand the idea of a proxy.

A proxy is a computer server in a free country such as Canada that a user in a censored country can tap into to access censored information and relay it back to the user. For years proxies have been considered a kind of ladder to cyberspace freedom.

The problem is that in order to use a proxy, you have to know about it. This means the proxy's IP — a set of numbers that is the computer's actual "address" on the Internet — has to be publicly advertised. This is usually done on websites and through email. So, it's only a matter of time before the censors also catch wind and cut off access.

Enter Psiphon.

The program effectively turns anyone's personal computer into a proxy server. Once the software is installed on a computer in, say, Canada, that person creates a contact list of trusted friends or family members in censored countries and sends his or her IP address to them. No advertising needed.

The censored user then connects to the computer running Psiphon and accesses banned content from there, all unbeknownst to the censor.

Deibert says that Canada and its many diasporas, with links to Asia and the Middle East, is a perfect place from which to build these trust networks.

But Psiphon doesn't stop there. Unlike most Internet traffic, Psiphon data is encrypted and shoots around the world on a network reserved for secure financial transactions, so a censor cannot see what the person is accessing. And a censor wouldn't be able to tell a Psiphon request from a MasterCard purchase.

Another benefit is that most other proxy-type anti-censor programs have to be installed, so if a user is being watched, evidence is on his computer for the taking. With Psiphon, the censored user installs nothing, so it leaves no trace.

In the unlikely event a computer running Psiphon is uncovered and blocked, future versions of the program will be able to connect to other computers running Psiphon as backup.

"These initiatives are exciting," says Michael Geist, an expert in law and the Internet at the University of Ottawa. Any ethical qualms in using Psiphon to circumvent the censorship regulations of a foreign country should be put to rest, he says. "There are international instruments that override even sovereign governments, such as the Universal Declaration of Human Rights."

But there are possible problems for Psiphon, Geist and others warn.

One is that many people in a place like China are not even aware they're being censored, says Geist. Even if they are, he predicts, few will make the attempt to get around it. Qiang notes that even young urban males, the greatest beneficiaries of China's economic boom, are reluctant to rock the boat and risk their wealth.

Hom, meanwhile, says that the "trusted networks" philosophy on which Psiphon is based could be problematic, since trust was a concept shattered during the Cultural Revolution, when even family members were convinced to turn each other in.

No one is under any illusion that Psiphon is the final answer. Countries like China will always try to stay ahead in the filtering game. But the Citizen Lab trio are happy to stay hunkered down in their basement without a view of the outside, running on the fuel of hacktivist dreams of a better world.

"We're making the Internet run the way it's supposed to," says Villeneuve with his trademark little-boy smile. "Because people have broken it."

[Get great home delivery subscription deals here!](#)

[FAQs](#) | [Site Map](#) | [Privacy Policy](#) | [Webmaster](#) | [Subscribe](#) | [My Subscription](#) | [RSS Feeds](#) | [Webmaking Blog](#)

[Home](#) | [GTA](#) | [Business](#) | [Waymoresports](#) | [A&E](#) | [Life](#)

Legal Notice: Copyright Toronto Star Newspapers Limited. All rights reserved. Distribution, transmission or republication of any material from www.thestar.com is strictly prohibited without the prior written permission of Toronto Star Newspapers Limited. For information please contact us using our [webmaster form](#). www.thestar.com online since 1996.

