

# Censorship, Information Warfare and the Battle to Protect the Net: BY MARSHALL BECK a Conversation With Ron Deibert

*A University of Toronto team is working on ways of protecting internet access for people living under repressive regimes. Marshall Beck talked to Ron Deibert about the problem – and some promising technological fixes.*



“Many people took the Internet for granted for a long time because of this myth that it was invincible, that there was some kind of mysterious property to it. But that never was the case. It is just a bunch of wires and routers,

and in fact it lends itself very well to control: quite the opposite of the myth,” says Ron Deibert. “Indeed, there is a subterranean realm of the global communications environment where power politics are being played out without much public knowledge.”

Deibert speaks with considerable authority on the subject. An associate professor of political science at the University of Toronto, he founded and is director of Citizen Lab, an interdisciplinary research laboratory focusing on digital media and its relationship to global security politics, civic activism, and human rights.

**Peace Magazine spoke with Deibert about the work of his lab and the state of the Internet. Excerpts from his comments follow.**

## CENSORSHIP AND FILTERING

“One element of our Lab’s work, through its OpenNet Initiative, is to document censorship trends using technical means of interrogating the Internet. Our findings show that the scope, scale, and sophistication of Internet censorship are on the rise worldwide.

“When we first started about a decade ago, there were maybe three or four countries that we knew were engaged in these sorts of things. When we tested in 41 countries in 2006, we found evidence of Internet filtering in 26 of them. This year, we’re testing in 71 and I expect the number will be much larger. So the problem is enormous.

“Moreover, it is not just a problem in non-democratic countries. There is considerable momentum behind filtering information worldwide, ostensibly to control things like child pornography, hate speech, or copyright violations. In Canada, for example, Internet service providers are being pressured to explore shaping Internet traffic. As well, the debate around network neutrality in the US asks if the companies providing the services for telecommunications should discriminate the content that runs through their pipes. We’re now finding out that some of these companies have been discriminating already, blocking packets that have the characteristics of file sharing. There is proposed legislation to impose that kind of protocol, which would have a global impact because most tier one Internet service providers are American-owned.

“Unfortunately, there are many places around the world where such filtering is being done for political reasons. A country like Pakistan says it is blocking access to blasphemous imagery and ends up blocking access to a bunch of political content. That’s the big fear: once we open up to that remodeling of the Internet, we’re back to a world where individuals just don’t have equal access to the same communications environment.

“We have all these shared planetary problems and



eventually will have to address the fact that we live in a finite political space. The starting point, it seems to me, is a shared communications medium through which citizens around the world can discuss common problems. The Internet is that medium right now, or at least it once held that promise. Its foundational principle was of openness and the free flow of information, but now it is rapidly changing for the worse. It is being carved up and shaped and controlled, and all sorts of roadblocks are being put in place, mostly for political purposes that have to do with the exercise of national interests or economic competition.

“However, an interesting characteristic of digital and network technology is that, because of its distributed nature and the way people can create technologies that reshape the environment, it is difficult to control.

“Some have phrased this in overly idealistic terms, saying that you simply cannot control the Internet. That’s not necessarily true. In fact, core parts of the Internet have aided state control. For example, interconnection points — say, where AT&T and Verizon connect to each other — have been important nodes of control for intelligence agencies. For years the National Security Agency in the US had eavesdropping equipment planted inside such interconnection points.

“The large commercial providers running the Internet are also focal points and, increasingly, proxies for government policy. Thus, the Chinese government told Google it had to de-index certain search results to host its services in Chinese territory. Also in China, Yahoo! agreed to share private information on Internet users with the government, sending two dissidents to jail for 10 years. Some of these companies try to respect human rights, but they are also businesses and want to make money, so

they compromise those principles to invest in certain political settings. This is another structural point of vulnerability in the Internet that facilitates control.

“Nonetheless, there is something about the way related technological developments can take place swiftly, with ripple effects across the system, that make it hard for governments to keep on top of the Internet. So there’s a kind of battle going on. With the projects and the software we’re building here we’re trying, along with many others, to — as we say — protect the Net.

### PROTECTING THE NET

“These efforts of ours fall under Civisec, short for ‘security for civil society,’ a broad umbrella project of the Lab that aims to research existing security and privacy tools, to develop tools of its own, and to produce guides that help people better to understand how to use these tools. The software application Psiphon is a product of this project.

Psiphon allows individuals living in countries with a restricted Internet environment to by-pass governmental barriers by connecting to a trusted Internet user abroad — a friend, family or professional colleague — whose own uncontrolled Internet connection then functions as a proxy access point. Psiphon has garnered international attention and accolades, catapulting the Lab into the media spotlight and showering it with honorary recognitions and awards, such as the 2008 France-based “Netxplorateur of the Year Grand Prix” award.

“I wanted to do things in the Citizen Lab that were experimental and had a very clear normative underpinning to them, a political orientation, and actually to go so far as to create technologies that would surmount the usual division of the world ‘out there’ and the university. So we’ve zeroed in on a specialty, which is advanced research and development around Internet technologies in support of human rights. That’s where Psiphon fits in.

“A university producing such a political piece of software is unusual; this software contravenes local laws in many places. Most circumvention technologies have been grassroots tools meant for the serious hacker crowd. What Psiphon did was take the basic concept and develop a tool easily used by the average person. Some 150,000 people have downloaded the software to date.

“It is inevitable that, at some point, determined governments are going to find a way to isolate

*Yahoo  
agreed to  
share its  
customer  
information  
with the  
Chinese  
government,  
sending two  
dissidents to  
jail for ten  
years*



Psiphon traffic and block it. So we have to try and continually stay one step ahead of the game, a difficult challenge for a project like this that is not revenue-driven.

### AN ARMS RACE IN CYBERSPACE

“Through the Infowar Monitor, the Lab has also collected information about the use of the Internet and other computing technologies as a means to engage in warfare.

“There is an arms race in cyberspace of which most people are unaware. Without being alarmist, I must assert that it is definitely a problem. We have the military viewing cyberspace as an arena within which they should fight and win wars.

“From a philosophical perspective alone, it is disturbing that the public sphere is being viewed as a military battleground. The attitude also opens the possibility for instability in the system, if governments are taking down servers containing information they find objectionable. The Chinese could be zapping the Falun Gong servers in Canada, and the US might be taking out an al-Qaeda server based in Belgium, and next thing you know it’s a wild west. But a country as powerful and large as the US has developed a strategic command for cyber war, equivalent to its strategic commands for outer space, air, and the sea.

“Targeting servers for elimination is now common practise. If it is considered to be a strategic threat, they’re going to put it in a target list and attack it. A real problem is that you cannot distinguish between regular glitches that happen to networks on a daily basis, and deliberate attacks directed by a military actor. Such attacks are easy to hide. This is especially problematic because, before you have an arms control agreement, you need some verification methodology. The lack of such a methodology sometimes hampers the ability to come to terms to an arms control agreement, or may be used as an excuse to prevent one. There have been some proposals for cyberspace arms control, and some models exist for verification that could be built upon, but the political will is absent.

The Russian government put forward a proposal at the UN for cyberspace arms control a few years ago, but this went nowhere.

### A SEA CHANGE

“As people become disabused of the illusion that the Internet is invincible, much attention is being directed towards how we maintain the system. People are mobilizing and asking: What should be the rules, how should the technologies be constructed, what should be the operating principles, where should there be openness and accountability? This is a very encouraging development.

“Here, the notion of ‘hactivism’ is relevant. It’s about encouraging people not to accept technology at face value, which is the dominant paradigm. We need to encourage citizens to take a more experimental approach to the technologies that surround us, precisely because they are potential levers of control; they are the vehicles through which power is exercised today.

“Interesting analogies can be made between the degradation of the global communications environment and the natural environment. You have a similar dynamic at work. There’s this commons that’s been taken for granted and gradually destroyed. We need to rescue the communications environment, in the same way we are thinking about rescuing the natural environment.

“We need to promote the notion of protecting the commons, making it foundational that the Internet be a seamless network where anyone can access any information, no matter from where they connect. Then, from that foundation, you start making exceptions in rare circumstances, with a great deal of transparency and accountability. Rather than what we have now: a crazy, mixed up myriad of borders and closed networks, dubious practices and secretive filtering.

“I’m hopeful that, with all this percolating grassroots activism that’s going on, there will be a sea change around how people approach technology. And that’s the most important safety mechanism. It’s not going to be technological; it won’t be Psiphon or another tool. It’ll be people’s attitudes changing around how to preserve this environment.”

■ Citizen Lab: <http://www.citizenlab.org/index.php>

*Access Denied: The Practice and Policy of Global Internet Filtering*, co-edited by Ron Deibert and other principal investigators of the OpenNet Initiative, hit the bookshelves on 29 February 2008. *Ron Deibert was interviewed by Marshall Beck for Peace Magazine.*

*determined governments are going to find a way to block Psiphon traffic. So we have to try to stay one step ahead of the game*

Copyright of *Peace Magazine* is the property of *Peace Magazine* and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.