

A CONVERSATION WITH CITIZEN LAB

Sharon Hom interviews Ron Deibert and Nart Villeneuve about their work investigating Internet censorship and surveillance, transparency debates and the uncharted waters of information warfare.

The general landscape of Internet censorship

HRIC: Let's begin at the beginning—can you give us a sense of the general landscape of Internet filtering and censorship? What are your key observations about trends and issues that have arisen?

Deibert: Through the research of the OpenNet Initiative (ONI), over the last six years we've observed an increase in terms of the scope, scale and sophistication of Internet filtering worldwide.

When we started our research, there were really only a handful of countries involved in filtering—Saudi Arabia, China and perhaps a few others. But in our next round of reports, we're examining as many as 30 countries. This is basically a phenomenon growing in every region of the world—though more intensely in some areas than others. Asia is of particular concern in the next round of research reports, and we will be focusing intensively on South Asia and Southeast Asia.

We've noticed that the scope of filtering has increased as well. By that we mean the type of content that has been targeted for filtering. It's gone from mostly pornography to a much more expansive spectrum of topics—including human rights information, dissident groups, information on anonymizing technologies, even translation services. A whole range of information is being targeted for filtering by countries around the world.

The sophistication of the censorship is growing as well. We've noticed that countries are focusing on local languages in addition to English. They're also using commercial technologies.

One of the main stories of ONI's research has been to identify corporate involvement in Internet censorship around the world. Countries have begun to use methods to isolate known circumvention technologies. For example, Google's

cache can be used as a method of circumvention. In China, however, the authorities recognize this is an easily accessible technique and block the URL path for Google cache at the backbone level. There are many other examples of that type of sophistication.

Generally speaking, this problem is growing worldwide. We're concerned with growing issues of accountability and transparency in Internet filtering, including the transparency of states regarding the type of filtering being conducted, and issues of accountability or redress available to citizens trying to remove content from blocked lists.

On transparency and accountability

HRIC: It's very interesting that you bring up the issue of accountability and transparency. We were recently involved in a consultation on these very issues.

One of the arguments made by industry was that increasing transparency could also hinder companies' anti-censorship efforts by making them public. Can you comment on that?

About Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk Centre for International Studies at the University of Toronto, Canada engaged in advanced research and development at the intersection of Information and Communication Technologies (ICTs) and Global Civic Networks.

A "hothouse" that brings together social scientists, filmmakers, computer scientists, activists and artists, the Citizen Lab sponsors projects that explore the cutting edge of hypermedia technologies and grassroots social movements, civic activism and democratic change within an emerging planetary polity.

For more information, visit Citizen Lab's Web site at <http://www.citizenlab.org>.

The OpenNet Initiative: Country reports on Internet filtering

The OpenNet Initiative (ONI) is a collaborative partnership between four leading academic institutions: the Citizen Lab at the Munk Centre for International Studies, University of Toronto; Berkman Center for Internet and Society at Harvard Law School; the Advanced Network Research Group at the Programme for Security in International Society (Centre for International Studies) at the University of Cambridge; and the Oxford Internet Institute, Oxford University.

The mission of ONI is to apply methodological rigor to investigate and challenge state filtration and surveillance practices, blending empirical case studies with sophisticated means of technical verification. ONI aims to generate a credible picture of these practices at a national, regional and corporate level, and to excavate their impact on state sovereignty, security, human rights, international law and global governance. ONI intends to uncover the potential pitfalls and unintended consequences of these practices, and thus help to inform better public policy and advocacy work in this area.

To achieve these aims, the ONI employs a unique multidisciplinary approach that includes advanced technical means, using a suite of sophisticated network interrogation tools and metrics; and local knowledge expertise through a global network of regionally-based researchers and experts.

For more information, visit the OpenNet Initiative's Web site at <http://www.opennet.net>.

Deibert: This rationale makes sense from a logical perspective, and at Citizen Lab we're very carefully deliberating over this very issue: if you publish a list of sites that are not being censored, are you giving the authorities a guidebook on how they can "improve" their system?

My personal impression is that you have to be careful in following the logic of this argument all the way down the road, because it can be used as a cover for corporations to hide what they have been and are doing, and how they're doing it.

In the case of Google and Chinese search engines, there's an ambiguity in the list that they're using. There's a certain amount of concern over the authentic intentions of corporations that are actively involved in supplying tools used for censorship and surveillance.

In reality, what the corporations might be trying to do is protect themselves from more embarrassing revelations beneath the surface.

In the course of our research, which includes 10 country reports, we've never had a single instance where a URL or Web site that we identified as not being blocked became blocked after the report was published.

In fact, what we've seen is just the opposite. That is, releasing a country report puts pressure on those governments, and in some cases mistakes arising from filtering and unintended consequences (collateral blocking of Web sites) have been repaired and addressed.

Overall, we feel it's better to be more transparent about these things than less, and to push for transparency overall. It's the only way to gain accountability over Internet censorship.

If state authorities want to block content, they don't need help from research organizations. They're well aware of the landscape. What we're testing is not obscure, dissident sites. Rather, we're trying to get a snapshot of filtering.

HRIC: One of the ways HRIC has responded to this kind of argument is to draw an analogy with the differing strategies between individual groups. For example, the Dui Hua Foundation negotiates for individual releases based on *guanxi* (relationships) and behind closed doors. This strategy has been characterized as playing a hostage release game.

Of course, most of the individuals involved will prefer exile to dying in prison, but actions like these at the individual human level that are contingent on favors and relationships don't contribute to the systemic changes and reforms that are necessary for *real* protection for everyone. We need to move China towards a transparent and accountable rule of law and away from a discretionary and arbitrary process.

Deibert: Yes, the bottom line for us has always been the security of the people who do fieldwork on our reports, often at great personal risk. We're very sensitive to the protection of people we work with, and that of course extends to the issue of publishing data that might endanger people.

Pushing for transparency is the only way to gain accountability over Internet censorship.

We take the logic of the argument of transparency very seriously. But when this argument comes from western corporations involved in providing technology for censorship and surveillance, we find it very dubious, because what they may be doing is putting a shroud around their business practices in a way that prevents revelations on whether or not they are in bed with these repressive governments.

Looking beyond Google, Yahoo and Microsoft

HRIC: You've addressed the issue of the general role of foreign IT companies, especially U.S.-based IT companies. Can you say something about the role of Canadian companies and if they've been involved in exporting technology?

Deibert: Our research has not identified any specific Canadian corporation involved in supplying or maintaining filtering technology. But there has been some very good research done by Greg Walton in the *Golden Shield*¹ report involving the sale of

surveillance technology and infrastructure like fiber optic cables to China.

There's an interesting contrast that can be drawn between Canada and the United States. Canada often likes to take the moral high ground, but at least the United States has held congressional hearings about corporate involvement in Internet censorship. All we've seen in Canada are government support networks for trade missions to China that promote Canadian business, which as we know, includes surveillance and other technologies that help the Chinese censorship system. We would like to see more pressure put on the Canadian government and for companies to be held more accountable for their investment practices.

HRIC: In fairness to Canada, while the U.S. holds congressional hearings, there is still also strong government support for trade missions.

The question of the sale of technology and infrastructure materials is especially significant in light of the security infrastructure being built for the venues and border control for the 2008 Olympics. Looking ahead, how can we gain more traction in monitoring these issues and developments?

Deibert: It's absolutely correct that this issue is not confined to Internet censorship and surveillance. This has been and continues to be a long-standing concern among human rights groups about corporate practices in developing countries. I'm thinking mainly of the action of Canadian mining companies in Central America.

There are lessons to be learned in the experiences of the past, where human rights groups and other people concerned about justice and trade issues have put pressure on companies to be more open and transparent. Ultimately, we see three things that need to be done:

1. **Continue the research** that groups like the ONI and others are involved in, namely monitoring governments' practices that violate human rights. This research needs to go beyond rumors and hearsay; the goal of ONI is to present forensic, empirical evidence that cannot be denied.
2. The next step would be to **develop advocacy networks** that exert pressure to rein in these companies, which after all, are not inherently evil, but are simply operating within the boundaries available to them. There's a need to create laws and **develop legal frameworks** within the legal jurisdictions in their home base that will serve to restrain their practices.
3. The third step would be to **put pressure on these companies** to be more socially responsible and overcome their purely competitive instincts. We need to build norms on what is acceptable and what is not. We believe that these companies, while they do want to make money, instinctively wish to avoid violating human rights. This is especially true for companies like Google who presented themselves as not wanting to "do evil." With the proper framework and opportunity, there might be a chance for real progress.

Challenging the dominant economic paradigm

HRIC: A multi-pronged strategy of research and monitoring, legal regulation and pressure makes sense, but we also need to address head-on the concerns of competitive advantage and profitability that companies often invoke.

The dominant neo-liberal economic model limits persuasive counter-economic arguments because of its focus on efficiency, short analytical time frames, externalized costs and narrow definition of communities impacted. Some progressive economists are developing more human-centered, intergenerational economic models of sustainable equitable development, but this has been largely applied to the environmental area, and has not been extended to IT. Ideally, what would a human rights IT "footprint" look like?

Deibert: The environmental movement has a long history, whereas the IT area is relatively new.

It was only five or six years ago that I can remember having gone to development units within the Canadian government to present the ONI concept as an important research project. We were basically laughed out of the building simply because they couldn't accept the idea that information technology might have components that violate human rights and enhance censorship and surveillance. This is a new issue, and there's a lot of work to be done in terms of raising awareness.

It really comes down to governance. That means, as you quite rightly point out, modifying the neo-liberal economic paradigm that erases the state from the equation and puts the emphasis entirely on market forces. That model is being questioned not only in the environmental sector but also in other areas, including, I hope, the IT sector.

Then we can begin talking about censorship and surveillance footprints in the same way as environmental footprints. And then it's a matter of holding corporations accountable for their actions, and framing laws and regulations that circumscribe what they can do. But this needs to happen in their own governments and eventually also at an international level, for example, at the World Trade Organization (WTO).

Apart from a strategy of research and monitoring, legal regulation and pressure, we need to address head-on the concerns of competitive advantage and profitability.

We don't want to underestimate the extent of real change that monitoring and advocacy can achieve. For example, Gap was once vilified around the world as an egregious violator of environmental practices, but now they've gone to great lengths to transform their practices and self-monitor. Their most recent Corporate Social Responsibility report² looks like it came from an environmental advocacy group rather than from a corporation. They've really taken themselves to task for violating environmental standards around the world. We can never

underestimate what advocacy and monitoring can do to bring about change.

HRIC: Before Gap released its report, they held a consultation that HRIC attended. Gap representatives appeared willing to look at the company's practices with respect to environmental and, to a more limited extent, labor rights issues. But there was a reluctance to address more structural issues, such as freedom of association and independent unions, which have more impact than outside monitoring and code compliance.

Creating pressure is useful, but ultimately it's important to look at how a company's activities undermine or enable greater social spaces within a host country.

Deibert: There are global political economic forces that create the environment within which all of this takes place. Hopefully that environment will change over time, but in the meantime we need to start taking small steps.

Citizen Lab on Internet Filtering

The number of states seeking to control the Internet has risen rapidly in recent years. Mustering powerful and at times compelling arguments—"securing intellectual property rights," "protecting national security," "preserving cultural norms and religious values" and "shielding children from pornography and exploitation"—extensive filtering and surveillance practices are being proposed and put in place to curb the perceived lawlessness of the medium.

While awareness-building and advocacy are important components of a strategy to elucidate the legal and practical consequences of censorship practices, these avenues are not always possible or effective in the regions most affected. Consequently, building awareness of technologies that make it possible to circumvent censorship and thus enhance the individual's right to communicate and access information is also an important means of challenging these practices.

To this end, the Citizen Lab has established an online clearinghouse of tools for assessing, archiving and testing anti-censorship, privacy/anonymity, security and encryption software called the Circumvention Technologies Clearinghouse. The Clearinghouse assesses the effectiveness of circumvention technologies from technological, usability and legal perspectives. Our own circumvention tools are developed at the Citizen Lab on the basis of experiences gathered through the analysis of national censorship strategies and existing circumvention technologies.

For more information, visit Citizen Lab's Web site at <http://www.citizenlab.org>.

Technology as agnostic?

HRIC: During the U.S. Congressional hearings into the repressive use of Internet technology,³ Cisco Systems took the position that technology is agnostic, and insisted that the routers they sell to China are the same routers they sell all over the world. Is technology really something completely neutral that takes on certain qualities only as it's deployed by humans? For example, NGOs can and have adapted technology from commercial applications for human rights work.

Villeneuve: It depends on the circumstances. It would be hard to argue the "agnostic" nature of technologies such as Secure Computing's SmartFilter,⁴ which has been sold to repressive countries where its only purpose is to filter.

With routers the case becomes different, because the main function of the technology is to route, not to block. Then it becomes an issue of what the use of that technology is going to be. It's the same idea as certain components that can be used for weapons. In that sense, it's very contextually dependent.

In terms of selling routers to China, in some cases this could very well be considered benign—but routers with special technology to censor would start raising red flags, because China has a long history of censoring Internet access. Any client technology that has those precise features would likely be used for that purpose, while generic routers might not be.

The bottom line is that we don't even know precisely what technology China is using for its filtering capacity. We have a good sense of it, but until someone comes forward from within companies like Cisco, we won't know for sure.

Integrating human rights into the information business

HRIC: HRIC commented at the U.S. Congressional hearings that Cisco shouldn't get off the hook by arguing that it was only selling routers. First, Cisco is a very active trading partner with China and produces a lot of its equipment there. The number of Cisco engineers being trained and certified in China is also striking—China is currently home to the third largest concentration of Cisco certified engineers, behind Germany and the United States.⁵

On the question of human rights training and awareness, since IT companies are in the information business, shouldn't their training include awareness of international human rights standards that apply to their work? Shouldn't they at least know about the relevant human rights laws and norms about freedom of expression, and the right to access and disseminate information?

Villeneuve: Absolutely, we think that that is a great suggestion. Sometimes when people are dealing with issues at a purely technical level, they lose sight of the broader context in which technology is deployed. The impact that technology has on freedom of expression would be a great component to add to training. Having said that, we don't think companies are integrating that into training.

HRIC: We're looking at it as a triangulated possibility. For example, the Global Compact⁶ has adopted a "learning" model approach where companies can share creative approaches for promoting environment, human rights, labor rights and governance.

If a company could exercise some leadership and vision on developing an approach to promote greater respect for the rights provision in international and domestic Chinese law, it might encourage others and help build the necessary critical mass.

During the U.S. Congressional hearings, companies repeatedly invoked cultural relativism and referred to the need to comply with domestic law. When the Committee asked what they would do if domestic law required them to discriminate against women, the company representatives were unable to respond clearly. If any of them had been briefed on the basics of human rights law and Chinese law beyond the narrow IT regulation area, they could have persuasively demonstrated that such discrimination is illegal under domestic Chinese law, as well as under the international conventions by which China is bound. The failure to engage in a comprehensive review of the regulatory environment results in poor policy formulation and business practices that impact on human rights.

Villeneuve: Yes, our sense is that an understanding of specific applications of laws to exact content and specific sites is extremely blurry.

For example, the *New York Times* recently reported that when Google went into China, they actually made their own list of sites to remove from their search engine in China. There was no list handed to them by the government; they had made it up themselves. This speaks volumes as to what happens when companies are left to anticipate what they think the government wants them to censor.

The emergence of information warfare

HRIC: Has Citizen Lab ever received direct or indirect pressure from countries as a result of its country reports?

Deibert: No, not really; at least, not anything that we're aware of. I'm hesitating on this question because our people in the field very surely face personal threats in the course of their research and in their activities outside of ONI work. It comes with the territory of being a human rights activist.

In terms of Citizen Lab itself, we've been visited by intelligence organizations looking to find out more about our work, and we're happy to describe what we're doing. But we've never been threatened or intimidated in any way.

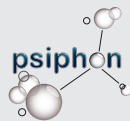
The norms and principles surrounding information warfare are at present very poorly defined.

But with that said, we do take security very seriously, and would not be surprised if something along those lines did happen in the future, not so much in connection with the

Psiphon FAQ

Psiphon is part of the CiviSec Project run by the Citizen Lab at the Munk Centre for International Studies at the University of Toronto.

What is Psiphon?



Psiphon is a censorship circumvention solution allowing users to access blocked sites in countries where the Internet is censored. Psiphon turns a regular home computer into a personal encrypted server capable of retrieving and displaying Web pages anywhere.

Who will use Psiphon?

Psiphon operates through networks of trust. There are Psiphon providers who install and run the server in an uncensored country, and Psiphon users who log in and access the server from a country that censors the Internet.

For more information on Psiphon, see <http://psiphon.civisec.org>.

research around the ONI, but because of other activities—particularly Psiphon.

Countries such as China and Iran could see Psiphon as a form of information warfare, and the norms and principles surrounding information warfare are at present very poorly defined. The existing definition is based on practices that states are currently engaged in. Curiously, one of the leading proponents of information warfare is the United States.

It's kind of like the wild west frontier, with no clear boundaries on what is and is not acceptable. When we put something out there that directly challenges government control over information, we shouldn't be surprised if we face a certain amount of pressure.

HRIC: When we were lobbying at the UN, they didn't know about the ONI report—and neither did the Chinese delegation. But experts on the committee became really interested in it and raised questions about it, and we were pleased to see the committee include the right to access the Internet in its final recommendations to China. This shows how the OpenNet Initiative provides groups like HRIC with legitimate and empirical analysis for use in our arguments. At the same time, our use of this analysis also raises the profile of the OpenNet Initiative, for better or for worse.

Deibert: And that's the thing. You can't engage in this type of research without facing the kind of risk that it implies. This is something that everyone involved in human rights work needs to be cognizant of; otherwise they're just being naive. This is not a surprise for human rights activists, but for academics, it may be more difficult to grasp and accept.

After the *Globe and Mail* article on Psiphon came out, we received many interesting inquiries from many different people—and some of them were, frankly, creepy.

HRIC: What you said about the norms of information warfare is very provocative. I'm really struck by how there are norms for war, for example, the Geneva Convention. It would be interesting to think about if we move that idea to information warfare. Where would the ethical center be? I can see it being tied to human rights and saying, does the information being exchanged contribute to enslaving people or does it contribute to greater protections for human dignity?

A lot of money and effort is being put into information warfare in Iraq, Afghanistan and elsewhere that is having a major impact on the nature of Internet communications, and will have even more impact in the future.

Deibert: Unlike the rules of conventional warfare, the principles and norms in this area are not widely understood, and there is very little normative restraint. The U.S. is taking a very active and aggressive lead, which creates reciprocal actions on the part of other states.

There is an international relations theory called the "security dilemma situation." In an attempt to enhance its own security, the U.S. is making others feel less secure and more threatened, so that they end up effectively mimicking what the U.S. is taking the lead on. This is an area that is generally poorly understood, in part because it is shrouded in so much secrecy.

Challenging the myths of the Internet

HRIC: Looking ahead, as states become more sophisticated and as Citizen Lab itself becomes more visible and prominent, how do you see your role evolving? Implementing Internet censorship and challenging it is such a cat-and-mouse game. Is it possible to break this cycle, or does it just go with the territory?

Deibert: We think of it more in terms of the latter. Citizen Lab was set up to create a space within a university where people with an interest in computer science and Internet communication could interact with each other and do research alongside people with an interest in political science and human rights.

This stems from our belief that you can't just take the Internet for granted. There needs to be a continuous and conscientious effort made by individuals around the world to maintain the Internet as an open communication environment.

What happened, quite unfortunately, in the past, was that there was a myth surrounding the Internet that it had mysterious, magical properties that made it biased towards access to information and freedom of speech. That may have been true in the past, but it certainly is not in today's world, where states and corporations are shaping the Internet in ways that suit their own commercial and military interests. In the same way,

citizens around the world must also actively work to shape the Internet.

We see Citizen Lab as part of that effort, but based in a university environment. We will continue to do this type of research, which has three components to it:

1. **Monitoring and watching the watchers:** Doing empirical and technical interrogation of the Internet to determine what is being censored and how surveillance is being conducted, to open the lid on what is happening;
2. **Raising awareness** of censorship and surveillance through publications and mass media campaigns; and
3. **Building software** to enhance freedom of speech, access to information and privacy, and in doing so, to help tilt the balance of Internet architecture away from control and proprietary concerns, and more towards openness and freedom of speech worldwide.

HRIC: Do you think there's a way to develop a topography of the expanding and evolving content that is being targeted? It seems to us that dissident and opposition groups are being targeted for what they are saying, but translated information is targeted more for the function provided, which is basically that of enabling access.

Deibert: Absolutely, and the same goes for anonymizing and circumvention tools, when those are filtered. We've also increasingly found that VoIP services are being targeted in certain countries—not for political reasons, but in attempts to protect domestic telecom companies.

NOTES

1. Rights and Democracy, *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China*, 2001, available at <http://www.dd-rd.ca/english/commdoc/publications/globalization/goldenShieldEng.html>.
2. Gap Inc.'s 2004 Corporate Social Responsibility report can be found online at http://www.gapinc.com/public/documents/CSR_Report_04.pdf.
3. Testimony of Mark Chandler, Senior Vice President, General Counsel, Cisco Systems, Inc., "The Internet in China: A Tool for Freedom or Suppression?" Committee on International Relations, Subcommittee on Global Human Rights, Africa and International Operations, February 15, 2006, available at <http://www.cdt.org/international/china>.
4. For more information on SmartFilter, see <http://www.securecomputing.com/index.cfm?sk=85>.
5. As of May 2006, there were 1,848 Cisco Certified Internetwork Experts (CCIE) in China, with 5,440 in Germany and 4,275 in the United States. For more information, see http://www.cisco.com/web/learning/le3/ccie/certified_ccies/worldwide.html.
6. For more information, see United Nations Global Compact, <http://www.unglobalcompact.org>.