EVASION TACTICS

NART VILLENEUVE

GLOBAL ONLINE CENSORSHIP IS GROWING, BUT SO ARE THE MEANS TO CHALLENGE IT AND PROTECT PRIVACY

The number of countries that censor and monitor their citizens' use of the Internet is increasing. While it is no secret that China and Iran censor the Internet, at least 25 countries, including Pakistan, Ethiopia, Thailand and Uzbekistan, also have technical filtering regimes in place. Some of the technology is even exported by western companies: search engines, blog hosting providers and email providers have extended their existing filtering mechanisms – which usually target pornography and copyright infringement – to censor political content and gain access to lucrative markets in repressive countries.

Censorship and surveillance is not restricted to authoritarian regimes. The technology used to censor the Internet in entire countries in the Middle East and North Africa also filters access in schools and libraries in North America. An Internet service provider (ISP) in Canada blocked access to a website set up by members of its workers' union during a labour dispute. ISPs in the United States have implemented a sophisticated, and illegal, monitoring and data-mining programme, covering both Internet and telephone communications, at the behest of the National Security Agency. The problem is magnified when the concept of censorship is extended beyond just the technical aspects of filtering web content and Internet services.

There is, however, a growing resistance to Internet censorship and surveillance, although it is often characterised as a struggle confined to dissidents in a few select authoritarian regimes. There are a wide variety of awareness raising campaigns as well as academic research projects aimed at exposing and confronting censorship. Legal battles are being fought all over the globe, while the development and use of technologies that protect privacy and make it possible to circumvent censorship are rapidly increasing. The same tools helping dissidents to evade censorship in repressive countries are also being used by citizens in democratic countries – to protect themselves from unwarranted Internet surveillance.

There are three key factors to Internet censorship. First, there are formal and informal mechanisms, including laws, licensing and self-regulation, that act to create the legal, and often extra-legal, framework within which Internet censorship takes place. Second, there are a variety of technical methods

through which Internet filtering and blocking can be implemented to restrict access to content and services online. Third, Internet surveillance technologies are routinely deployed in order to monitor and track online communications. All countries use varying degrees of these to implement control, generating fear among Internet users and contributing to a climate of self-censorship that is creating alarming challenges to freedom of expression online.

The legal basis for technical filtering is murky and rarely explicit, and can vary significantly from country to country. It is often a combination of press law, telecommunications regulations and laws protecting state security.

Uzbekistan online
Credit: Sean Sprague/Panos, 2005

Regulation and oversight is most often conducted by the Telecommunication Ministry or by the often state-controlled telecommunications companies.

In South Korea, the Ministry of Information and Communication instructed Internet service providers to block access to content deemed to be 'North Korean propaganda' and thus illegal under the vague, and often abused, national security law. The Korean Internet Safety Commission (KISCOM) has also been set up to advise the government's Internet censorship policies and its logo is prominently featured, along with the National Police Agency's logo, on the 'block page' users see when they try to access censored websites. South Korea received a 'high' transparency rating from the OpenNet Initiative – a research project documenting

Internet censorship. This was based on the country's open acknowledgment of filtering, along with the presence of a 'block page' that informs users when attempts are made to access censored content.

In contrast, Uzbekistan received a 'low' transparency rating because the country's filtering regime is based on a combination of self-censorship by ISPs and pressure from the country's intelligence service – the National Security Service (SNB). In addition to occasionally ordering ISPs to block specific sites, the SNB monitoring also encourages them to self-censor or risk having their licences revoked. In a way, the practice is symbolic of the censorship regime as a whole. The ISPs attempt to conceal their filtering by redirecting users to innocuous sites when they try to access blocked content.

In some countries, there is no technical filtering in place; it is the legal system itself which acts as the primary mechanism of Internet censorship. Threatening ISPs, or content providers such as search engines, with 'takedown' requests is one of the most undocumented methods of censoring Internet content. In some cases these can be formal legal requests for removal due to copyright violation or claims of libel/defamation or informal requests due to allegations of supporting terrorism. ISPs are not required to report such 'takedowns' and most happen in complete silence. In these cases, ISPs act as judge, jury and enforcer at the same time and will act to remove content rather than fully investigate the claim, in order to avoid liability.

The questions surrounding the lack of transparency and accountability led Christian Ahlert, Chris Marsden and Chester Yung, from the Oxford Centre for Socio-Legal Studies, to investigate what they termed the 'privatisation of censorship'. In 2003, they conducted an experiment, known as 'Liberty', to test notice and takedown procedures in the US and Europe. They created a web page containing text that was clearly in the public domain and uploaded it to ISPs in the US and the UK. The uploaded text was an excerpt from Chapter 2 of J S Mill's *On Liberty*, which discusses freedom of the press and censorship. They then created an email account with a free service for a mythical organisation called the 'John Stuart Mill Heritage Foundation' and sent takedown notices to the ISPs claiming copyright infringement. In the UK, ISPs took the information down, but in the US, they asked for more details, including a declaration 'under penalty of perjury' that the claim was valid. At this point, the researchers terminated the experiment. However, they noted that if they had supplied the language required by the ISPs, the takedown process could have continued.

In 2004, the group 'Bits of Freedom' conducted a similar experiment using Dutch ISPs. They uploaded text that was clearly in the public domain – the text even stated that it was in the public domain – and then sent takedown notices

from free email accounts. Of the ten ISPs tested, only three did not remove the content. One provider even forwarded the account details of the customer to the complainant. 'Bits of Freedom' went further than the 'Liberty' experiment by filling out a form sent by the ISPs that asked for additional details including name and address and to 'indemnify the provider from any liability for acting upon the request to take down'. This led 'Bits of Freedom' to conclude that the 'penalty of perjury' test which worked in the 'Liberty' experiment was clearly not enough of a check against abuse.

These studies exposed the flawed process through which takedown and notice are being implemented. It is clearly being exploited to silence online critics. The Church of Scientology has used takedown notices alleging copyright violations with great success, even forcing Google to remove links from its search engine to particular sites. In addition to copyright, threats of law suits for defamation and libel are increasingly being used to stifle criticism. Singapore and Malaysia have often been accused of using such tactics. The new targets for libel and defamation cases are bloggers. While many blogs are about personal interests and read more like a diary, the blogging platform is also being used by citizen journalists, who publish without the filters of the traditional media.

While there have been documented cases where bloggers have been prosecuted for libel or defamation, many never make it to court. In August 2007, the website of the Iranian blogger Hossein Derakhshan was shut down. Derakhshan's blog has long been censored in Iran. Despite being filtered, it remained popular and Iranians used technology to bypass the filters and access the site. However, after criticising an Iranian intellectual, Mehdi Khalaji, for working for a conservative think-tank in Washington DC, Derakhshan, his web hosting company, Hosting Matters, and domain registrar, GoDaddy, were served with a takedown notice. The notice, alleging libel and defamation, led to the deletion of some of Derakhshan's blog posts by his hosting company and ultimately to the termination of his blog's hosting service. Exemplifying just how flawed the notice and takedown process is, the notice claimed that in addition to Derakhshan, both the domain registrar and the web hosting company were implicated in and/or liable for activities conducted on Derakhshan's blog. The notice implied that each of the three named in the notice (the registrar, the hosting company and Derakhshan) 'published' defamatory information and were therefore liable for damages.

The chilling effect of notice and takedown is well illustrated in this case. Faced with legal threats, Derakshan's web-hosting company ordered him to remove 'all' references to Mr Khalaji or they would remove his entire website, even though the company recognised that the claims fell into a 'grey area'. After taking down the offending posts, but refusing to remove all references to Mr Khalaji, Hosting Matters asked Mr Derakhshan to remove additional posts about Mr Khalaji.

> Please remove the latest post you have made referencing Mehdi Khalaji. This person continues to insist that everything and anything you post about him is defamatory. While we do not agree with the assessment as it relates to the latest post you have made, we do not have the time, interest, or resources to invest in continually dealing with his complaints and to review your site.
>
> (Source: http://hodertemp.blogspot.com/2007/08/accounts-and-billing-hosting-matters.html)

This exchange clearly shows why ISPs are not equipped or qualified to make judgments on content and will always default to the lowest common denominator, with serious repercussions for freedom of speech and expression.

Content removed for allegedly supporting terrorism is one of the least documented forms of takedown. With copyright and defamation there is at least some element of a legal procedure, however flawed, but when it comes to terrorism, individuals and groups simply contact ISPs and have content removed. The Internet Haganah, which calls for the removal of sites which allegedly support terrorism, had counted 600 successful takedowns by 2005. These include websites, groups hosted by Yahoo! and storefronts at Cafe Press. In 2005, the Toronto-based Friends of Simon Wiesenthal Center had several sites removed by their ISPs, one of which only contained a flag that carried the inscription, 'There is no other God but Allah'. There was no hateful text or material advocating suicide bombing. The issue, as noted in the press release, was that the flag appeared to be the same one used by Hizb-ut-Tahrir, a group that, at the time, was not on the US State Department's or Canada's list of terrorist organisations.

While content removal remains largely undocumented, it is possible to interrogate the technical infrastructure through which countries block access. There is a variety of methods through which content on the Internet can be blocked that falls into three general categories: domain name server (DNS) tampering, Internet protocol (IP) address blocking, uniform resource locator (URL) filtering and keyword filtering.

DNS is the system that translates a domain name into a numerical IP address. By tampering with their DNS server, ISPs can force domain names to resolve to invalid or 'spoofed' IP addresses. The South Korean ISP, Kornet, resolves censored domains to an IP address which displays a police block page, indicating to the user that illegal content is being accessed. One of India's leading ISPs, Videsh Sanchar Nigam Ltd, uses DNS tampering to block websites, forcing domains to resolve to the invalid address 1.2.3.4 India focuses its filtering on Hindu extremists and some American right-wing sites, as well as sites advocating

a Dalit homeland. DNS tampering is easy to circumvent, as a user can simply configure their computer to use an alternate DNS server, but it is often used by ISPs to avoid problems with over-blocking.

Countries new to filtering will generally start with blocking by IP address, before moving on to more expensive URL filtering solutions. Most ISPs do not have the capacity to filter by URL and the ones that do would need to purchase a significant amount of equipment to implement URL filtering without a significant drop in performance. ISPs must often respond quickly and effectively to blocking orders from the government or national security and intelligence services. So they block material in the cheapest way, using technology already integrated into their normal network environment. Blocking by IP is effective (the target site is blocked) and no new equipment needs to be purchased. It can be implemented in an instant, as all the required technology and expertise is readily available. Many ISPs already block IP addresses to combat spam and viruses.

But blocking by IP address comes with a significant cost: over-blocking. Many unrelated websites may be hosted on a single IP address, so, when blocked, all other content hosted on the server will also be inaccessible. Pakistan is an interesting case, because it is one of the few countries in which the blocking lists have become public. Internet traffic routes through a gateway operated by the Pakistan Telecommunications Company Limited. Officially, Pakistan only blocks 17 sites, although the list contains dead sites and typographical errors. The OpenNet Initiative tested 11 of these designated sites. It found that, in total, nearly 3.5 million are actually blocked. This total does not, however, include the hundreds of thousands of individual blogs hosted on Google's blogspot service. Pakistan has blocked access to the IP addresses of key hosting providers including GoDaddy and Yahoo! In the past, Pakistan has also blocked IP addresses associated with the mirroring company Akamai, causing hundreds of thousands of sites to become inaccessible.

This is the same technique that the Canadian ISP Telus used to block access to a union-affiliated site during a labour dispute. In the process, it blocked access to over 700 unrelated sites. This generated a considerable amount of criticism and clearly demonstrated the unintended consequences of filtering technologies.

Over-blocking tends to create a significant backlash, especially from non-activist Internet users. While people will often tolerate the blocking of extremist or offensive sites, when their own regular browsing and blogging is interrupted they quickly become aware of censorship's impact and campaign against it. An excellent example has been the 'Don't Block the Blog' campaign which was started after Pakistan blocked access to Blogspot; pkblogs.com now offers an alternate means of accessing Blogspot, bypassing Pakistan's filtering.

However, in response, the authorities will often seek to implement filtering techniques that better target the specific sites they want to block.

As the complexities of implementing an effective filtering system are recognised, countries are beginning to move towards the use of commercial filtering technology. In addition to the issue of over-blocking, filtering systems suffer from another inherent problem: under-blocking. Alongside the maintenance of blocking lists – which can be considerable for categories such as pornography – other forms of content need to be blocked in order to have a reasonably effective filtering system. This primarily involves finding and blocking sites that enable users to get around the filtering. Commercial technologies have enabled the expansion of Internet censorship, providing a fine-grain control over the filtering and monitoring process. They are equipped with easy-to-use graphical interfaces for management of the filtering system, as well as pre-configured blocking categories which include 'anonymisers' – sites that allow one to bypass censorship.

There are a growing number of countries that use commercial filtering technology. However it is often difficult to determine the exact technology being used. To date, the OpenNet Initiative has identified the use of SmartFilter, produced by the US company Secure Computing, in Saudi Arabia, Tunisia, Oman, Sudan, United Arab Emirates, and possibly in Iran, while Websense and Fortinet are being used in Yemen and Burma respectively.

Commercial filtering technologies can be configured to block very specific content as well. In Saudi Arabia, for example, the websites of the Arab Human Rights Information Network and Humum are mostly accessible. Only specific pages about Saudi Arabia are blocked. They can also be used to avoid network degradation associated with other methods of filtering. Saudi Arabia claims that its system actually improves performance.

But commercial filtering technologies introduce additional concerns. The way in which these companies categorise websites affects access to the Internet more widely. SmartFilter, for example, is configured to block predefined categories of content: anonymisers, nudity, pornography, and sexual materials. Recently, the video-sharing website dailymotion.com was blocked in Tunisia. SmartFilter had temporarily categorised the site as pornography, and, since Tunisia blocks the pornography category, the website was blocked. Several days later, SmartFilter removed dailymotion.com from the pornography category and it became accessible.

In effect, governments are ceding the decision on what precisely to filter to unaccountable commercial entities. Due to the categorisation choices made by these companies, content may become inaccessible to entire populations, even if the government never intended to block the content. This situation is exacerbated by the intellectual property protections afforded to the companies. The block lists

used by commercial filtering software are secret; decrypting and analysing them is considered to be illegal.

The chilling effect of legislation, such as the United States' Digital Millennium Copyright Act (DMCA), has resulted in researchers stopping work on the impact of commercial filtering software. This is especially relevant because the software is increasingly turning up in undemocratic countries and is being used to filter all sorts of content – including political speech.

The work of two high-profile researchers was cut short in this field due to mounting legal risks. Ben Edelman sought to obtain a court judgment in order to protect himself from liability for decrypting the blocking lists of commercial filtering technologies, but his case was dismissed. Seth Finkelstein was forced to abandon work decrypting the blocking lists of filtering software products because of the associated legal risks.

Despite the obstacles, there are growing efforts to resist and challenge the spread of Internet censorship. These range from research projects designed to document and expose current censorship practices, to legal challenges to the development and use of technologies. Combined, these efforts seek to challenge the norms surrounding the practice of filtering, change the policies of governments and ISPs and empower users to protect their privacy and exercise the right of free expression online.

There are numerous human rights organisations investigating and highlighting egregious cases of Internet censorship, including Amnesty International, Reporters Without Borders and Human Rights Watch. These groups collect and analyse reports of blocked content, as well as create campaigns to highlight egregious cases of censorship and make that information available to a wide audience. They also seek to influence public policy and engage in lobbying and advocacy, targeting governments and corporations. Amnesty International started the irrepressible.info campaign that seeks to highlight Internet censorship by allowing website owners to display fragments of text taken from censored sites around the world. More than 70,000 people have signed the pledge calling for an end to 'unwarranted restriction of freedom of expression on the Internet'. The signatures from this pledge were delivered at the 2006 Internet Governance Forum before an audience of governments and companies involved in censoring the Internet.

Reporters Without Borders maintains a list of imprisoned cyberdissidents and has also created the *Handbook for Bloggers and Cyber-dissidents* which provides information on how to secure one's communications and bypass Internet censorship. Human Rights Watch has released detailed reports that not only document the technical aspects of filtering, but also the cases of individuals who have been directly affected by state censorship. The reports contain detailed

recommendations for governments, corporations and activists to promote policies that enhance freedom of expression online.

In addition to major international organisations, there are coalitions such as the Global Voices Advocacy project and the Society Against Internet Censorship in Pakistan that seek to build alliances among bloggers and free expression advocates worldwide. There are also numerous grass-roots campaigns to free imprisoned bloggers around the world. The groups not only raise awareness about violations of freedom of expression, but also provide information on how to bypass Internet censorship and on strategies to maintain anonymity online.

While advocacy is an extremely important component in challenging censorship, there also exists the need to technically uncover exactly the methods and targets of state censorship. Research projects have been pivotal in establishing a body of credible evidence, exposing practices that are most often secretive and forcing governments and corporations to account for their censorship practices. Faced with accurate, empirical evidence, it becomes increasingly difficult for states to continue denying the fact that they are censoring the Internet.

The chillingeffects.org project, a collaboration between leading law schools and universities across the US, tracks notice and takedown requests. The majority of complaints relate to copyright and trademark infringement, but increasingly also cover libel and defamation. The project has tracked over 2,000 such notices. It also provides 'weather reports', which are a great resource for investigating the use of the law to remove content.

The OpenNet Initiative (ONI) has developed a set of tests that interrogate the Internet to identify filtered content. To date, ONI has tested in over 40 countries worldwide and has uncovered the techniques employed by states, usually at the ISP level, to filter the Internet. Moreover, ONI has begun to develop methods to monitor Internet access during key time periods, such as elections, in order to collect evidence of the temporary tampering with Internet access and in some cases denial of service to opposition websites. ONI has also identified technologies created by American companies, which are used to censor political speech in repressive countries. This work has informed a US Congressional committee that brought representatives from leading companies to explain their actions. ONI work has also been widely cited and used by human rights and press freedom groups around the world.

But while ONI has done excellent work in interrogating systems of Internet filtering, surveillance has proven to be much more elusive: it can be conducted in a passive manner and is thus extremely difficult, if not impossible, to document technically. Therefore, the majority of the work done in uncovering systems

of surveillance has been through leaks, freedom of information requests and legal process.

The United States maintains the most sophisticated surveillance programme in the world. The American Civil Liberties Union (ACLU) created the 'Surveillance Society Clock', modelled after the doomsday clock, to symbolise just how much of a threat the current levels of surveillance in the US are to a free society. The clock is currently at six minutes to midnight.

Surveillance practices in the US are being challenged in the courts. The Electronic Frontier Foundation (EFF) and the Electronic Privacy Information Center (EPIC) have been extremely active in bringing legal challenges to uncover the vast surveillance programme. The EFF filed a lawsuit on behalf of AT&T customers to challenge the company's participation in the National Security Agency's (NSA) illegal domestic surveillance. The challenge was made after it was revealed that the NSA had been data-mining Internet and telephone logs from various telecommunications companies in the US without the proper legal authority. In response, the Bush administration is seeking to shield participating companies behind vaguely worded 'state secrets' protection. The Department of Homeland Security (DHS) and the Pentagon also maintain surveillance programmes. As a result of investigative reporting and the threat of legal challenges, two of these programmes have been suspended. The DHS suspended ADVISE (Analysis, Dissemination, Visualisation, Insight and Semantic Enhancement) after it was found to violate privacy laws. The Pentagon suspended its TALON database – which monitored peace activists amongst others – and the infamous Total Information Awareness project after similar concerns were mounted.

Legal challenges against Internet censorship are also being mounted worldwide. In Iran, the conservative website Baztab was filtered after several articles critical of President Ahmadinejad were published, but access to the site was restored following a successful legal challenge. The unblocking of one website – run by well-connected people – is a small victory, but it could be very significant. If the procedures for blocking content become transparent, if there is an appeals process and some level of accountability, it then becomes increasingly difficult for governments to justify censorship. Human rights groups have long called for a legally transparent process through which censorship can be challenged.

China has also been the site of a legal challenge – once largely thought to be impossible. A Chinese blogger known as Yetaai [see pp161–164] brought a case against China Telecom for blocking his website. It is seen as a landmark case because it may force the company or the government to admit that Internet censorship actually takes place. Although many believe that Yetaai will not be successful, his case has inspired others to use the legal system to

Internet cafe, China
Credit: Gemma Kate Thorpe

challenge Internet censorship in China. Another blogger, Liu Xiaoyuan, has attempted to sue the Chinese company Sohu for censoring several posts on his blog, while a website, www.bullog.cn, is calling for public hearings to protect it from being shut down.

In another case that is emblematic of the global resistance to censorship, the family of Wang Xiaoning, an activist who was arrested and tortured in China, is suing Yahoo! in an American court because Yahoo! provided information to the Chinese government that was used in the prosecution. Yahoo! has filed a motion to dismiss the case.

This is not the first case in which Yahoo! has provided evidence to the Chinese government resulting in the conviction of dissidents. Chinese journalist Shi Tao was sentenced to ten years in prison in China, after distributing the Chinese government's instructions to domestic journalists on how to cover the anniversary of the Tiananmen Square massacre. Shi Tao sent the information to a foreign-hosted dissident website from his Yahoo! email account. The Chinese government asked Yahoo! to provide information on the account details and this information was used in the case against Shi Tao.

The case illustrates that while many people assume that there is anonymity online, users have to protect themselves to keep their identity hidden. Technologies that make it possible to circumvent censorship and enhance the individual's right to communicate and access information are also an important means for challenging censorship and surveillance. Filtering and monitoring communications online make it possible for hostile actors to find identifying information that may be used to arrest and imprison political dissidents.

In order to combat these growing threats, technologies are being developed to evade censorship and protect privacy. These same technologies are used by dissidents in politically repressive countries as well as activists in democratic countries. Peacefire, for example, is an organisation that develops and provides technology to evade censorship. It was formed to advocate on behalf of children who were being subjected to filtering in schools and libraries throughout the US. Peacefire now also focuses on providing these same censorship circumvention methods to users in China and Iran.

The technology allows a user in a censored location to connect to an unblocked, intermediary computer, in an uncensored location, to access content through the computer's Internet connection. The user in the censored country does not directly access a blocked website, but asks the intermediary computer to do so. The intermediary computer retrieves the requested website and displays it back to the user.

While there are a variety of technologies available that can be used to circumvent censorship, there is a fundamental challenge: how to disclose the location of the uncensored intermediary to users who want to bypass censorship, while keeping it secret from agents who seek to find and censor these intermediaries. There are two main approaches to this problem: public and private. The public approach is to create numerous intermediary locations, through which users can

bypass censorship and simply reveal more, through email lists, instant messaging and so on, as each becomes blocked. Censors who are slow to act will find more and more people using these circumvention systems. However, since many countries now use commercial filtering applications, the list of 'proxy and anonymiser' sites that these companies maintain are updated frequently, resulting in a situation where the lifetime of a new circumvention intermediary can last between one day and one week before being blocked.

Private circumvention solutions focus on distributing the location of the intermediary computer to people who know and trust one another. By leveraging these relationships of trust, a circumvention provider can slowly develop a network and provide stable circumvention services to a few – with a greatly reduced risk of being blocked by censors. Psiphon is a personal circumvention system that was designed and developed by the Citizen Lab at the University of Toronto. It allows users in uncensored locations to turn their own home computer into a circumvention server and allow their friends and family members in censored locations to surf freely. One of the goals of the project was to make the software extremely simple, so that those with limited technical abilities could make use of the technology.

There is an important distinction to be made between circumvention and anonymity technologies. Circumvention technologies focus, with varying degrees of security, on allowing users to bypass censorship, while anonymity technologies focus on protecting the users' identity from outside observers, such as government surveillance, as well as from the anonymity system itself. Circumvention systems that use encryption can protect users in some surveillance scenarios, but are not anonymous because owners of the circumvention system can see everything that the user does. They also cannot protect users from traffic analysis attacks in the same way that anonymity systems can. Anonymity systems protect privacy by shielding the identity of the requesting user from the content provider. In addition, they employ routing techniques to ensure that the user's identity is shielded from the anonymous communications system itself. In addition to providing anonymity, these technologies are also used in many countries to bypass Internet censorship. Anonymity systems are increasingly being recommended by privacy advocates. The Privacy Commissioner of Canada, for example, recommends that Internet users protect themselves online by using anonymity technologies, as well as anonymous remailers.

The most widely known anonymity system is Tor (see p143). It is promoted by the Electronic Frontier Foundation as software to protect privacy and civil liberties online and is used by bloggers who want anonymity, as well as by government embassies around the world. Tor works by routing a user's request through at least three Tor servers. As the request hops from one Tor

server to another, a layer of encryption is removed, so no individual server knows both the original source and destination of the request. The last server in the chain of hops, known as a circuit, actually connects to the requested content and then sends that information back through the circuit to the user. However, anonymity technologies are currently not difficult to block. Tor's developers are working on building in blocking resistance to the anonymity system.

The Internet is a tool, like any other, that can be both used and abused. We know that governments around the world, much like companies, schools, libraries, and parents, restrict access to Internet content they do not want their citizens, employees, students, patrons and children to see. However, there is a failure to recognise Internet censorship and surveillance as a growing global concern. There is a tendency instead to criticise the most infamous offenders – notably China and Iran – and to overlook repressive practices elsewhere. Focusing on the global character of both the practice of Internet censorship and surveillance, as well as the resistance to it, provides for both a better understanding of this important trend as well as for the possibility of creating global alliances to combat its spread. ❑

Nart Villeneuve *is a PhD student in Political Science at the University of Toronto. As Director of Technical Research for the Citizen Lab he has developed and conducted censorship testing in over 40 countries worldwide as part of the OpenNet Initiative and participated in the Psiphon circumvention project*