The internet: Closing the frontier

Print

By Richard Waters and Joseph Menn
Published: March 28 2010 18:43 | Last updated: March 28 2010 18:43

China may be public enemy number one when it comes to internet censorship. But ask executives at Silicon Valley's leading companies about other countries that cause them concern and the first name that springs to many lips may seem surprising: Australia.

In the name of suppressing child pornography, the Labor government of Kevin Rudd, prime minister, has championed the imposition of some of the toughest internet filters proposed by any established democracy. Many internet companies fear that this is just the thin end of the wedge.

David Drummond, **Google**'s chief legal officer who fronted its showdown with the Chinese censors last week, warned recently that Mr Rudd's government has "designs perhaps on things that were offensive to Christianity", along with other content it deems harmful. The temptation to adopt filters such as this without strict controls "does seem like the slippery slope [in the west] unless we turn things around", he added.

Nor is the significance of what is happening in Australia lost on Beijing officials. China's State Council Information Office recently reported approvingly on its own website Canberra's efforts to wrest back control of the web on behalf of its citizens.

The situation in Australia highlights a fact that jars with the image of the internet as medium for free expression. Internet censorship has spread well beyond the usual culprits and predictable targets, such as political opponents. **Google**'s showdown with China has drawn fresh attention to the most conspicuous attempt to regulate the online medium but a knock-on effect will be to draw attention to creeping controls worldwide.

In popular consciousness, the internet still promises a borderless world, a place where the free flow of information threatens artificial barriers erected by nation states. But the web is fast being carved up by national laws and regulations, whether aimed at suppressing opinion, tackling pornography or identity theft, as countries around the world learn the techniques of control. Far from being a universal medium, the world wide web is becoming balkanised – as users are now learning.

"It's true of cyberspace as it is of real space – companies have to bow to the laws and customs of the countries they operate in," says Jack Goldsmith of Harvard law school.

The only way around this is to avoid the most restrictive countries, says Mr Drummond. Google, for example, has avoided operating its search engine in Vietnam to avoid a censorship regime as strict as China's, he says. But having set up shop in Turkey, it could do little to resist when a local court ordered it to block videos on its YouTube subsidiary deemed offensive to the memory of national patriarch Mustafa Kemal Atatürk.

This realpolitik has been brought home by Google's decision first to bow to Chinese censors, and then

Control list

The OpenNet Initiative lists 18 countries in which it has found evidence of actual or suspected **political censorship** online, ranging from "pervasive" in countries like China, Vietnam and Iran to "substantial" (Libya, Ethiopia and Saudi Arabia) and "selective" (Pakistan, Thailand and Azerbaijan.) More than 30 states filter for **social reasons**, blocking content related to things like sex, gambling and illegal drugs. Most Middle Eastern

last week to attempt to retain its Chinese search presence while dodging the effects of censorship.

“People will now see that there’s a global battle going on over the future of the internet,” says Ron Deibert of the University of Toronto and a founder of the OpenNet Initiative, which tracks global censorship.

More **than 40 countries** now apply some sort of barrier on the web, compared with a handful less than a decade ago, according to the ONI. The most severe censors are China, Iran, Vietnam, Syria, Burma and Tunisia. Even where electronic blocks have not been imposed, laws requiring higher levels of self-censorship are being enforced more aggressively.

countries are identified as “pervasive” social censors; China, Burma and Thailand are among the “substantial”. The US, the UK and many European states apply it “selectively”.

Google’s Mr Drummond, for instance, would probably want to avoid travelling to Italy right now. In a landmark case, a court there last month handed him and two other executives six-month suspended prison sentences. Their offence was to have failed to prevent YouTube from carrying a video showing the harassment of an autistic child.

As examples such as Italy and Australia show, internet censorship is not limited to repressive regimes. “Internet freedom is a bit of a Rorschach test: it means different things to different people,” says Rebecca MacKinnon of Princeton University’s Center for Information Technology Policy and an expert on Chinese censorship.

In this debate, Google’s decision to end compliance with Chinese censors is a watershed. Beijing’s strenuous efforts to filter the tide of online content washing ashore into the world’s largest internet market set a standard for other regimes. If it reacts aggressively to Google’s gambit of taking its search business offshore to Hong Kong, beyond the reach of mainland censors, the effects could be widely felt. “It could further embolden other authoritarian regimes and add to their legitimacy,” warns Mr Deibert.

Internet freedom advocates warn that China has exported its censorship technologies to other countries, and some of the country’s web security companies have boasted of expanding abroad, training police in markets such as Bangladesh. However, proof is hard to come by.

Even countries with elected governments and a stronger claim to following the rule of law have taken to flexing their muscles in the cause of protecting their citizens from online abuses. For Google, that has brought restrictions of one kind or another from no fewer than 25 governments, one company executive says.

Working out how to counter repressive and unwarranted attacks on internet freedom, while still leaving governments room to protect their citizens from online abuse, will not be easy. Google, whose role as gatekeeper for much of the world’s online information puts it at the centre of the debate, has apparently decided it is time to stake out a clearer line. “As they butt up against more governments, they are realising they need a consistent position,” Ms MacKinnon says. “This is not just about China – it’s about how the internet is going to be regulated globally.”

But while the search company has sent a signal that it intends to stand its ground, few others have been prepared to follow its lead, making it easier for repressive governments to continue with their current policies.

The lack of broad support for the **Global Network Initiative** is a case in point. Set up four years ago, it was meant to be a forum for companies and non-governmental organisations to devise a common practice for confronting online censorship and repression. However, it still counts only three companies – Google, **Microsoft** and **Yahoo** – as members. In a meeting at the US state department this month, undersecretary Robert Hormats castigated the technology and telecommunications executives from nearly 20 companies for not rallying around the initiative, according to one person present.

Even those companies that have taken a public stand can appear ambivalent. Microsoft, which still offers a censored search service in China and stands to benefit from Google’s change of stance there, recently drew criticism from Human Rights Watch, a New York-based advocacy, after Steve Ballmer, chief executive, and Bill Gates, chairman, made public comments appearing to side with Beijing in its row with Google. Mr Ballmer later published a blog post reiterating his company’s support for internet freedom.

Governments have also been slow to take up the running, though political momentum in the US has picked up this year. Google’s heavy emphasis on the cyberattacks that it said led to its change of heart in China helped to fan the flames in Washington, where cyberwarfare is a growing concern.

In January Hillary Clinton, US secretary of state, proclaimed it part of her country’s mission to foster **global internet freedom**. While it is unclear how much diplomatic firepower will underpin such words, she has at least made this an item for bilateral discussions, according to supporters.

Congress has also joined in. “Most people for some reason think the free press is on the march, but actually it’s the opposite,” says Senator Ted Kaufman, a Democrat who last week formed a Global Internet Freedom caucus with nine other senators, five of them Republicans.

Yet such efforts have yet to be echoed elsewhere; industry executives, for example, bemoan lukewarm support from Europe. That is partly due to suspicions about the motives of some in the US who have jumped on the bandwagon. “The cold war warriors are seizing on it to revive their agenda,” says Ms MacKinnon.

Also, the US devotion to its First Amendment right of free speech does not resonate as strongly elsewhere, where different privacy and

other social expectations can often take a higher priority, warns Mr Goldsmith – as Australia's filtering plans show.

Perhaps most importantly, government attempts to promote internet freedom also clash directly with a rival priority: the fight against cybercrime in all its guises, from identity theft and file-sharing of copyrighted movies to government-sponsored attempts to extract corporate and military secrets.

One obvious way to combat web crime has been to try to increase official monitoring of the internet – though that also raises concerns.

For example, security advocates have long criticised the loose patchwork of rules allowing web addresses to be awarded to people using bogus identification. Domain names ending in .ru for Russia and .cn for China have been so riddled with criminality that many western companies and software services prevent browsers from visiting them. Recently both countries issued rules requiring positive identification for anyone wishing to register domain names. That should help to limit criminality but it will also give those governments a clearer view of dissident activity.

In response, GoDaddy, the world's largest domain name registrar, said last week that it would stop selling .cn addresses, making it the first technology company to follow Google's lead – though its business in China is very small.

The battle against censorship also clashes with the fight against internet piracy. Ms MacKinnon cites the UK's planned digital economy bill, which would increase government powers to monitor and regulate networks by applying many of the same techniques used in censorship.

The US, meanwhile, is developing its own master plan for copyright enforcement in the internet era: the music and movie associations said last week that internet access providers should be forced to monitor traffic for copyrighted material. Most critically, the US now sees cybertheft of digitised commercial property as a threat to national security.

Ultimately, in distinguishing what are reasonable government attempts to regulating internet behaviour from intrusive and unwarranted incursions, lies in the eye of the beholder.

The setting of standards for how internet companies respond can at least help to guide those companies' decisions and limit abuse. Pushing for greater transparency, for instance, reduces the opportunity for entrenched governments to wield their power of censorship behind closed doors.

Google executives hope that the transfer of their China search business to Hong Kong will help in this regard, by forcing the authorities to be more explicit in future about which search results they block.

As the world wide web becomes increasingly fragmented by national laws, deciding how to respond in cases like this looks set to get increasingly challenging.

"It took a generation for companies to recognise their responsibilities in terms of labour practices, and another generation for them to recognise their environmental obligations," says Ms MacKinnon. Developing ethical rules for the web, she adds, is likely to take just as long.

.....

Washington promotes social networking as key to pro-democracy protests

Tools for internet communications, notably some that did not exist a few years ago, have opened the door for both public rallying and clandestine collaboration among opposition groups in countries that have until recently seen little of either, **writes Joseph Menn**.

This was displayed most dramatically during street protests in Iran last year. The US state department saw the Twitter messaging service as so critical that it asked the Silicon Valley company created in 2006 to **delay downtime for a service upgrade** to allow democracy advocates to continue using it to co-ordinate their moves.

"The early round went to the protesters," says Jonathan Zittrain of Harvard's Berkman Center for Internet & Society. "The [Iranian] government was a little bit clueless about Twitter and what it meant, and had its hands filled with what was going on in the streets."

America's executive branch and Congress now see such technology as essential to encouraging global democratic movements. With the support of leading diplomats, the Treasury department this month excepted blogging, e-mail, instant messaging and social networking services from longstanding blocks on trade with Cuba, Iran and Sudan.

Last Wednesday, 10 senators from both parties formed a Global Internet Freedom Caucus to further the drive. Republican senator Sam Brownback, co-chair, has secured $50m (€37m, £33m) in federal funding to develop and promote technology such as open proxy servers that let internet users disguise their location.

"With resolutions, hearings and legislation, we are going to highlight the bad things people do, the individual countries that are engaged in [censorship]," says the group's other leader, Democratic senator Ted Kaufman. "We're going to promote the idea of how important it is to keep the net free." The technology race, he told the Financial Times, always "favours the offence" – in this case, those seeking to dodge central control.

But governments are wising up. Iran used mobile phone tracking to monitor Twitter posts, hunted down open proxy servers and blocked them. It is believed governments also use “honey pots” to trick people into giving identifying information to fake protest groups.

Because of such disinformation, the Iranian opposition has become more cautious, Mr Zittrain says. Crackdowns “may inspire a round of innovation on reputation and trust among protesters, giving them the generic tools where you can build around friends and family. It may go underground”.