Shifting Borders

Steven J. Murdoch & Ross Anderson

The Internet once promised a brave new borderless world, but the reality is more complex

In *A Declaration of the Independence of Cyberspace*, John Perry Barlow called for communities built around the Internet to be independent of national governments and borders: a Utopian ideal that has failed to materialise. The Internet does have borders, for similar reasons that national boundaries exist: they ease administration, permit collective defence and can be founded in culture.

While it is true that Internet borders do not have to be the same as political boundaries, the two have naturally mirrored each other. This is hardly a surprise since the Internet was built on the infrastructure of telecommunications companies, often controlled or regulated by nation states.

Even during the early 1980s, during the infancy of public networks and before what we now call the Internet had left the laboratory, this pattern was established. Although bulletin board services were run by enthusiasts rather than commercial interests, and driven by ideals similar to Barlow's, locality mattered. Since the communication hubs were accessed by telephone, each was popular only within the local call area.

Communication across borders was possible, but initially limited. Later, as the Internet became commonplace, global communication was seen as the norm, but international traffic was still charged at a higher rate and so discouraged. Nonetheless, the Internet has changed the nature of borders, and particularly their power to control the flow of ideas. The traditional censorship methodologies that nations built over centuries do not work particularly well on the Internet.

National borders are becoming more porous to information. Organisations previously had to publish through posters, leaflets or radio within their home country, risking material being banned. Now they can host their material overseas. Even where there is no initial concern about censorship, a lot of hosting is done for cost and efficiency reasons in the US. When a dispute arises, it is judged by the more liberal values there.

Since this has become apparent, many countries have implemented measures to restrict access to content that they declare to be illegal or immoral,

Originally published in: *Index on Censorship*, Volume 36, Issue 4, pages 156–159, November 2007. DOI: 10.1080/03064220701740525

despite being acceptable in the country where it is hosted. The common mechanism is to block communications with the computer on which the content is stored. Information coming from or going to a banned Internet address is misdirected or dropped entirely. The technology for performing the blocking varies by country, as does the nature of the material filtered, but the overall concept remains the same.

This type of blocking is fairly easy to circumvent for those with enough persistence or technical knowledge, but censors are not aiming for the unattainable goal of completely censoring forbidden information. Instead, it is sufficient to block most of the banned content from most of the people. Combined with surveillance and threats of punishment, this is felt sufficient to encourage self-censorship, and thus to halt or slow the social changes the censor fears.

The strengths and vulnerabilities of this style of blocking largely follow from the 'end-to-end principle', one of the central tenets in the design of the Internet. This calls for the intelligence of the network to be moved to the edges, rather than being distributed within it. The idea was that by constructing a dumb network, with clever endpoints, new Internet applications could be developed without altering the core of the network.

When information is pushed to the edges, blocking based on the address of the endpoints is fairly effective. However, while the end-to-end principle has been maintained in the technical details of how computers communicate over the Internet, when it comes to content, the end-to-end principle is increasingly breaking down, requiring the methods of blocking to become more complex. Community-based sites, known as Web 2.0, are one example of applications that shift the intelligence away from the end-user's computer. The code and data are kept on central servers, and the user requires only a web browser. This idea is not new: Geocities, founded in 1994, allowed people to publish content without requiring them to manage their own server. What has changed is the popularity and diversity of applications that are available.

Social networking sites like Facebook, blogging platforms like Blogger, and other community publishing venues like Wikipedia can all have their addresses blocked, rendering them inaccessible within a country. But censors are faced with the choice of blocking all of the site or none of it. All the disparate communities sharing the same site are behind the same address, and probably only a tiny fraction are the target of censorship. This is a very different situation from German ISPs blocking a handful of websites dedicated to promoting neo-Nazism.

The 'collateral damage' of blocking a huge website is significant. For example in 2006, when Google's Blogger and Yahoo Geocities were blocked in India, large online protests were organised. The Chinese blocking of Wikipedia was unpopular; the site was often unblocked only to be later blocked again. Even users of the sites who had no interest in the material

the censors disliked were frustrated by the censorship. Indeed, blocking a major service like Google or Skype can do actual economic damage to a developing country.

The tensions surrounding censorship of community sites are unlikely to change, since 'network effects' lead to popular sites becoming even more popular. This phenomenon was described in Metcalfe's law, which states that the value of a network grows with the square of the number of members. Network effects lead to industry consolidation, as with Google buying their video product's competitor YouTube, and Yahoo! buying Flickr. It also leads to 'winner takes all' behaviour-people will want to join the most popular community while the second-best languishes in obscurity.

But if address-based blocking is no longer feasible, what are the alternatives? One is to block by keyword, as is already done by China. Here, regardless of the address of a site, if a banned word is used the material is blocked. However, this approach requires more expensive equipment and is not reliable. Websites can also prevent this blocking, whether intentionally or unintentionally, by obscuring the information as it is transmitted. Then the censor is back in the previous situation: faced with a large site containing a small amount of offensive material, he has to block it all, or not at all.

That leaves countries with the option of asking the site operator to remove the offending content. Even if the content is legal in the country where it is hosted, the country in which the content is delivered still has leverage. Thailand has on occasion blocked all of YouTube.

Countries can also censor content if the provider has a physical presence there, regardless of where the content is actually hosted. In 2000, the US-based company Yahoo! lost a court case in France over whether they were required to prevent the sale of Nazi memorabilia, and earlier this year a Brazilian court ordered YouTube to remove an unauthorised video of a celebrity.

Even if the provider does not have a base in the offended country, a censor can move against the provider's suppliers, and in particular those who purchase advertising. This was the UK government's strategy in the 1960s to close down pirate radio stations that operated from ships outside Britain's territorial waters. This is an interesting case as the censor's goal was not an issue of faith or morals, but simply maintaining a level of state control of broadcast media that is nowadays considered excessive almost everywhere.

As community-based sites grow, network effects will cause their value to increase and so countries will be more hesitant in blocking them. However, this trend might not continue indefinitely. Industry consolidation means that a country could 'punish' an operator not by blocking the offending site-if that would cause too much collateral damage-but by blocking a different site owned by the same company. YouTube might be the dominant video-sharing site, but it is owned by Google, which plays in the more competitive search-engine advertising market. Even in countries where YouTube does

not have a legal presence, Google might be forced to remove its videos by threats to block its advertising.

All of a sudden, computer industry structures matter when it comes to censorship, where previously we had to worry about governments, and (to a much lesser extent) about the media industry. Important factors include whether controversial matter is hosted on a dominant site or niche interest. Corporate boundaries, rather than national ones, define how information will be restricted.

While John Perry Barlow's ideals of a borderless Internet have not come to pass, the barriers that have been created are different. Hopefully they are lower; it's a lot easier to set up companies than nation states. And change is particularly rapid in the computer business – so we shall see where these borders will move next.

Steven J. Murdoch is a researcher at the University of Cambridge. He is currently developing censorship resistant technologies for the Tor Project

Ross Anderson is Professor of Security Engineering at Cambridge. He was a pioneer of peer-to-peer systems and of security economics, and chairs the Foundation for Information Policy Research