The fight for control of the internet has become critical

John Kampfner

If plans to put cyberspace under a secretive UN agency go through, states' censoring of the web will be globally enshrined

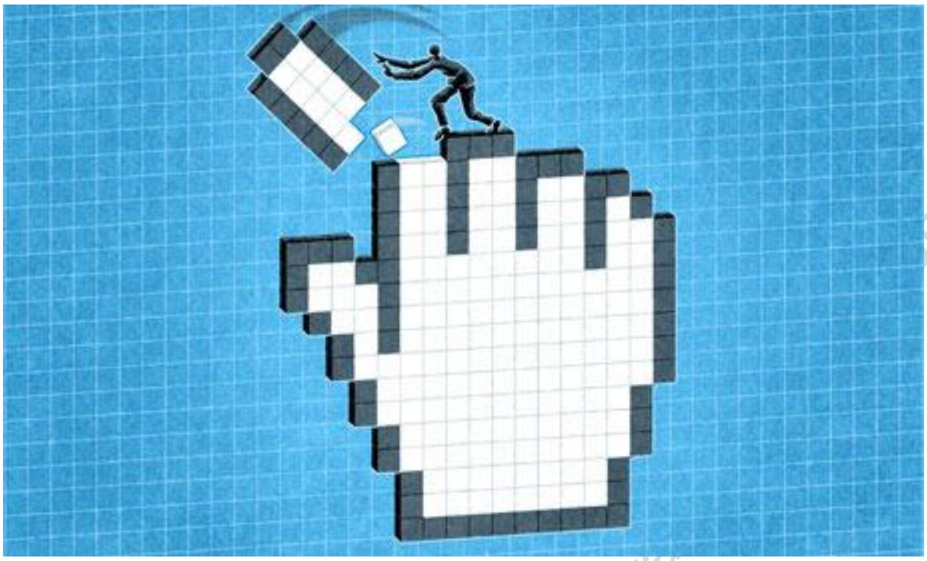

Illustration by Matt Kenyon

In horror movies, the scariest moments usually come from the monster you can't see. So the same goes for real life, or at least online life. Over the past few years, largely out of sight, governments have been clawing back freedoms on the internet, turning an invention that was designed to emancipate the individual into a tool for surveillance and control. In the next few months, this process is set to be enshrined internationally, amid plans to put cyberspace under the authority of a largely secretive and obscure UN agency.

If this succeeds, this will be an important boost to states' plans to censor the web and to use it to monitor citizens. Virtually all governments are at it. Some are much worse than others. The introduction last month of a law in Russia creating a blacklist of websites that contain "extremist" content was merely the latest example of an alarming trend. Authoritarian states have long seen cyberspace as the ultimate threat to their source of power.

They are given succour by self-styled democracies who seek to introduce legislation enhancing the rights of authorities and security agencies to snoop. The British government's current draft communications bill would produce a system of blanket collection and retention of all online data. As the group Privacy International pointed out in its submission to parliament: "The technology that will be used is only currently deployed in Kazakhstan, China and Iran … subjecting citizens to the near certainty of ongoing and unremitting interference in their private lives."

All governments, whatever their hue, cite similar threats: terrorism and organised crime, child pornography and intellectual property are the ones most commonly used. Unsurprisingly these, and local variants, are used by dictatorships, who need merely to point to precedents set in the west to counter any criticism with the charge of hypocrisy.

The internet, as originally envisaged, was borderless. In theory, anyone could – if they had access to the bandwidth – find out information anywhere and communicate with anyone. The demarcation between free expression and data and identify privacy on the one hand, and the state's right to security on the other, is continually debated and recalibrated, partly due to technological advances.

One of the most vigorous places for debate has been the Internet Governance Forum, which since its founding in 2005 has brought together governments, private sector firms large and small, academics and members of civil society. This year's meeting in November takes place incongruously and intriguingly in Baku, capital of Azerbaijan, a country with a particularly poor record on free expression and suppression of dissent.

What matters, as the lines are drawn, is transparency and inclusivity. If the internet is to be governed more cohesively, and on a less ad hoc basis than now, then it should not be left to governments alone. There has never been a central authority, and the internet has flourished in spite of (or perhaps because of) its decentralised governance model.

The reverse is now in prospect. In December in Dubai, a body that has existed for 150 years but few outside narrow industry circles have heard of, is seeking to take control of the internet. The International Telecommunications Union (ITU), a UN organisation that counts 193 countries as its members, aims to add the internet to its existing regulatory roles. Its strongest supporters include regimes such as China, Russia, Tajikistan and Uzbekistan, who submitted a proposal last September to the UN general assembly for an "international code of conduct for information security". Its goal is to establish government-led "international norms and rules standardising the behaviour of countries concerning information and cyberspace".

These countries, and others of their ilk, have three main goals for the Dubai summit and beyond: an assertion of national sovereignty over cyber communication; a clampdown on anonymity and encryption; and a change in global governance. Not that many readers would know as much. Official preparations for the ITU are clouded in secrecy, as is the organisation's standard practice, but information has been coming out via WCITleaks.org, a website created by two techies to publish leaked documents for the meeting. The ITU describes itself as a "multi-stakeholder" organisation, but the claim is spurious. All the big decisions are taken in meetings in which only governments can take part.

Lobbying (from all sides) has been taking place for months, but almost completely behind the scenes. Netizens have been shut out from this process.

Other cultural and political messages are in play too. Some developing nations and emerging powers are galvanised by the prospect of prising jurisdiction away from the US. This is the most seductive part of their message. Since its inception, the internet has been dominated by the US, both government, corporations, civil society groups and users. This is changing fast. Access to high-speed internet via mobile will transform access to information in developing countries in coming years.

The internationalisation of the internet is inevitable, and good. The question is not which countries are in charge, but where the power resides within countries. Control is always the first instinct of the state. The ITU summit in December marks just the start of the battle between those who wish to keep the internet (relatively) free and those who will do everything in their power to reverse the process.

Fonte:The Guardian, 22 Aug. 2012. [Portal] Disponível em: <http://www.guardian.co.uk/commentisfree/2012/aug/22/fight-control-internet-become-critical>. Acesso em: 22 Aug. 2012.