Bart Cammaerts, Nick Anstead and Ruth Garland

How Private Actors Engage the Duties of States

Monica Horten

Other dissertations of the series are available online here:
http://www.lse.ac.uk/collections/media@lse/mediaWorkingPapers/

How Private Actors Engage the Duties of States

Monica Horten

The development of online technologies, services and applications presents challenges for policy-making with regard to the protection of free speech rights. Those technologies, services and applications are enablers of free speech, but conversely they also contain powerful functionality to restrict it. It is this restrictive functionality that is the subject of this paper. The issue considered here is how to interpret the duty of States with regard to private actors, acting on behalf of States, in the context of Internet restrictions (network-level blocking and filtering) and the right to freedom of expression. In a human rights context, does it matter whether the private actor is applying content restrictions in response to a government request or doing so of its own accord?

To answer this question, the way in which restrictions placed on the Internet engage free speech rights from a legal and policy perspective is addressed. In particular, the ways in which the underlying network technology may restrict access to content and interfere with free speech rights is of relevance,. Besides this, the duties of States in this context will be

However, those underlying technologies present policy challenges in the form of ongoing developments that take the Internet from a neutral platform to one that has a sophisticated built-in intelligence. Notably, those technologies contain powerful functionality, such as

an automated block (Ofcom, 2011) as well as to intercept the users' traffic when they try to view specific content, or alter the access speed to make it difficult for users to get certain types of content. This vast and sophisticated blocking capability has placed the broadband providers at the centre of the political debate about Internet content, and what should and should not be permitted. They have become a target for many third parties who have desires to prevent or stop content, and are seeking the means to do so.

Applying Lessig's (2006: 121-32) ideas of 'code is law', what is happening is that norms and markets are being disrupted to such an extent that the affected stakeholder interests are clamouring to policy-makers for legal changes to amend the 'code' of the network. For example, norms of acceptable behaviour are changing as a result of a series of technology developments. The camera in the mobile phone, and the platforms such as Instagram, have generated a new norm where people take photographs and publish them not just to friends and family but also to the world. Those images could be embarrassing or invasive of privacy. Social media platforms provide a new mechanism that transfers a quiet grudge spoken to a friend into a published comment that is potentially defamatory (House of Lords, House of Commons, 2011, S.92-107)[4] The potential for abuse in terms of breach of privacy and defamation, led to a judicial procedure for content take-

over children's access to content, stalking, harassment, as well as copyright enforcement. All of these demands present a policy challenge. States are seeking the co-operation of broadband providers to take action which may conflict with their duty to protect free speech rights.

Central to policy measures proposed in this context is the obligation being placed onto the broadband providers to take action. Broadband providers are the gateways to the Internet, and they fall within the jurisdiction of nation States and so they can be governed by law, contrary to the popular perception of the Internet as an ungoverned space.[7]

a whole website or platform, results in over-blocking. This happened in the case of Yildirim vs. Turkey, where the Turkish government sought to block a website that had allegedly insulted the memory of Atatürk, the father of the Turkish state. The offending content was only on one particular website, but the entire platform of Google Sites – http://sites.google.com – was blocked[8]

blocking criteria. In some countries, such as Russia, the list is compiled centrally by the State (Weaver and Clover, 2012; Tselikov, 2014: 10). There are four registries that are maintained by the Russian telecoms regulatory authority, Roskomnadzor. The data for the lists is supplied by other government agencies. The broadband providers are obligated to check the lists and implement the blocks within 24 hours. In Britain, the broadband providers obtain a

A network-level blocking system requires Internet service providers to systematically examine all of a user's communica

intended.[21] Upstream filtering is where a network provider is filtering content according to rules in one jurisdiction and providing services for citizens in another. Those citizens in the second jurisdiction may find themselves unable to view content that is legitimate in their country but not in the one whose filtering rules are being applied. In other words, 'upstream filtering' by private actors could which could entail a violation of the rights of the 'downstream' citizens. States may have a duty to of due diligence in this regard, which, under international law, implies that they should do all that they reasonably can to avoid or minimise harm across national borders[22].

The central issue for policy-makers is the notion of 'interference', and notably to establish what constitutes 'interference' in the Internet space. The ECHR was drafted at a period in time just after World War II, when it was assumed that the interferer would be the State. The nature of the interference was assumed to physical, such as visits fro (m) -7 0 0 (s1f [(0.2 0.24 0 0 0Tm 2 (

criminally pornographic, the company would have to be absolutely certain that it had the remit to remove that content.

The ECtHR has said that 'any restriction imposed on access to content *'necessarily interferes with the right to receive and impart information*'[23]. This means that whenever blocking or filtering measures are considered, the right to freedom of expression is engaged and the measures must be evaluated against human rights law.

It begs the question as to whether *without interference*

platform' would not be legal, and 'blocking orders imposed on sites and platforms which remain valid indefinitely or for long periods are tantamount to inadmissible forms of prior restraint, in other words, to pure censorship.' [26]

Filtering of traffic on the network may also constitute interference. The European Court of Justice (ECJ) said that a filtering system engages the right to freedom of expression because it may not be able to accurately distinguish between lawful and unlawful content. It would also engage the right to privacy since it would have to systematically examine all content and identify the IP addresses of the individual users.

The right to privacy is a necessary corollary to freedom of expression because it guarantees confidentiality of communications, notably that the State will not intercept private correspondence. The large-scale monitoring of individual behaviour and of their communications has been condemned by European data protection experts, who argue that these rights should not be surrendered 'through neglect' (EDPS, 2014).

In that regard, EU law does not permit an injunction ordering a network provider to filter all traffic 'indiscriminately, to all its customers, as a preventative measure, exclusively at its expense, and for an unlimited period'[27]. Effectively, this means that anything involving continuous monitoring, of all content, for unlimited period of time, would comprise a general obligation to monitor, and

democratic society:[28] The State must be pursuing a policy aim that clearly justifies the need to implement restrictions, and must provide that justification (House of Lords, House of Commons, 2010, S.1.37). Legal experts point out that the requirement for narrow and targeted measures is especially important where the justification for the restriction concerns public order, national security or public morals (Rundle and Birding, 2008): restrictive

It is now generally considered that in copyright enforcement cases, policy-makers and courts should balance the right to freedom of expression against the right to property. Copyright is a private right and would usually be addressed under civil law (Matthews, 2008: 30). It is generally argued that copyright is a property right under the ECHR Protocol 1, Article 1, which mandates the 'peaceful enjoyment of possessions'[36]. The European Union Charter of Fundamental Rights[37], adds a right to intellectual property, as a subset of the more general right to property, in Article 17.2[38]. According to a British Parliamentary committee, policy-

_____

or not that was its intended purpose, but if that status is altered, then it will pose issues for policy-makers.

The notion of 'general monitoring' is another important legal distinction. EU law says that telecoms providers may not be given a 'general obligation to monitor'[48]. Blocking and filtering systems will fall foul of any net neutrality law, and notably the proposed law in the EU[49] would mean that measures undertaken by the broadband providers without statutory backing would be illegal.

If making laws to restrict the Internet, policy-makers have to weigh up the rights of the intermediary to conduct business, enshrined under the EU Charter of Fundamental Rights [50] along with freedom of expression and any other rights such as copyright. They have to find the most appropriate balance between the conflicting rights and interests involved. Within this context, there are tensions (Angelopoulos, 2014: 5) between the freedom of expression rights of the individual Internet user, as well as the rights of others (where others could be children in this context, or they could be copyright holders). Hence, when a government is considering restrictive measures, for example to protec 45 0 76.11-4 (te) -2 (c 45 0 533.80.24 0 (i) 3(n) -3 (

According to the U.N. guidelines, States should enforce laws aimed at guarantees for human rights, support businesses on how to respect human rights, and encourage business to communicate how they address human rights impacts (United Nations, 2011a: I.B.3 & B.5). This would suggest a requirement for regulatory safeguards. States will be under an obligation to ensure that restrictive measures such as blocking and filtering are not implemented in an arbitrary or over-broad manner (Rundle and Birding, 2008: 85). There should be a rigorous justification process, evaluating the proposed blocking measures against a legitimate aim, ensuring that they are necessary to achieve that aim and proportionate to it.

(

dependency mitigates in favour of a 'state-promoted private ordering' with non-disclosure and non-transparent regulation, 'insulated from public scrutiny and that can be tailored, by virtue of that insulation, to serve corporate interests at the public's expense' (Bridy, 2011: 577).

However, if a voluntary agreement is put in place, the UN guidelines call for private actors to avoid causing adverse impacts to freedom of expression, and seek to mitigate them if they

interference is created by the network infrastructure technology, which, by means of surveillance, monitoring and interception, makes it possible to bar requests and hide content from view – not actually destroying it, but as good as doing so from the user's or publisher's perspective. The balance of rights turns on the level of *interference*. Content restrictions lack the dramatic impact of piles of burning books, but in terms of their potential to effect censorship on a wide scale, the harm they could generate is much deeper. Leaving them in the hands of private actors without adequate safeguards would seem to entail inherent risks

Matthews, D. (2008) The Fight Against Counterfeiting And Piracy In The Bilateral Trade Agreements Of The EU, Brussels: European Parliament.

Mueller, M., Kuehn, A. and Stephanie S. (2012) Policing the Network: Using DPI for Copyright Enforcement, *Surveillance & Society* 9(4): 348-64.

Ofcom

Media@LSE Working Paper Series will:

- Present high quality research and writing (including research in-progress) to a wide audience of academics, policy-makers and commercial/media organisations.
- Set the agenda in the broad field of media and communication studies.

1474-1938/1946