GLOBAL INFORMATION SOCIETY WATCH 2011

INTERNET RIGHTS AND DEMOCRATISATION

Focus on freedom of expression and association online

Association for Progressive Communications (APC)
and Humanist Institute for Cooperation with Developing Countries (Hivos)

Internet intermediaries: The new cyber police?

Joe McNamee
European Digital Rights
www.edri.org

Introduction

The purpose of this report is to look at the increasing trend for internet intermediaries to be used to police and enforce the law on the internet and even to mete out punishments. As well as undermining the fundamental rights of freedom of communication, privacy and right to a fair trial, this approach is serving to create borders in the online world, undermining the very openness that gives the internet its value for democracy and, indeed, for the economy.

This issue is becoming increasingly important due to four different trends, which are developing simultaneously and synergetically. These are:

- The increased technical possibilities for online surveillance by internet access providers. The use of some of these possibilities is required by legal obligations such as the 2004 Communications and Law Enforcement Act (CALEA)[1] in the United States (US) and the European Union's (EU) Data Retention Directive.[2]
- The increased business interest that larger access providers see in blocking or limiting access to certain online content, as illustrated by recent discussions in both the US and Europe on "net neutrality".
- A concerted push at an intergovernmental level to legitimise and spread privatised enforcement measures.[3]
- Mergers of access providers and media companies, and distribution agreements between content providers and intermediaries where the contract includes obligations for the intermediary to undertake policing/punishment measures.[4]

1 en.wikipedia.org/wiki/Communications_Assistance_for_Law_Enforcement_Act

2 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

3 See, for example, article 5.3 of the Anti-Counterfeiting Trade Agreement at www.ustr.gov/webfm_send/2379

4 www.bof.nl/2011/01/04/vrije-internettoegang-ook-in-nederland-onder-vuur

Limitations of intermediary liability

The need for an open internet was recognised by both the US and the EU at the end of the 1990s. The US adopted the Digital Millennium Copyright Act (DMCA) in 1998, offering significant "safe harbours" to internet intermediaries for unauthorised content on their networks, while the EU adopted the E-Commerce Directive in 2000, which took a horizontal approach to safe harbours for all forms of illegal and unauthorised content. The public policy objectives on both sides of the Atlantic were clear, namely to maintain an open internet. This was seen as necessary to allow the economy to take full advantage of the internet and, as a collateral benefit, freedom of expression and almost unrestricted access to information. The benefits of such an approach can be seen in the economy[5] and in the effect of the internet in opening closed societies right around the world.

Nonetheless, despite this comparatively robust legal framework, weaknesses appeared almost from the start. This occurred particularly in Europe, where the wording of the E-Commerce Directive is too vague (due to the political compromises that were made during the adoption process) to allow intermediaries to feel completely secure, resulting in significant infringements of the right to communication. In 2004, a study by the Dutch NGO Bits of Freedom tested twelve hosting providers, nine of which deleted innocent material as a result of an obviously bogus "notice" sent from a Hotmail account set up solely for that purpose. This experience was duplicated by a team of United Kingdom (UK) academics,[6] also in 2004 (although it should be pointed out that this project did find the DMCA's process comparatively robust), and Dutch firm ICTRecht in 2009. Unilateral actions by internet providers have now effectively shifted their core activities from hosting providers to internet access providers, who have started "blocking" content, very often outside the rule of law. This started in the UK in 2004, supported by the Internet Watch Foundation, and spread to Denmark, Sweden and Finland in the ensuing years, as well as into the

5 eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

6 pcmlp.socleg.ox.ac.uk/sites/pcmlp.socleg.ox.ac.uk/files/liberty.pdf

mobile environment, thanks to an agreement brokered by the European Commission.[7] It is worth noting the heavy overlap between parts of the internet access market most opposed to net neutrality and the parts most favourable to voluntary internet blocking.

Operators that have been at the forefront of "voluntary" internet blocking – such as British Telecom, Telenor, Virgin and the mobile industry in general – have also been the loudest voices opposed to net neutrality. In January 2011, British Telecom announced plans to charge certain online video providers more for prioritised traffic,[8] as did Telenor,[9] while Virgin Media announced plans to launch a deep packet inspection of the traffic of 40% of its customers in 2010.[10] Similarly, there have been multiple examples of mobile industry efforts seeking to exploit and reinforce their control over access to their clients, such as the blocking of voice over internet protocol (VoIP) applications.[11] This creates a situation where these providers are eager to accept demands from regulators for so-called "self-regulatory" blocking measures as, in the long term, it will be difficult for regulators to sustainably argue that access providers should be voluntarily interfering in traffic for public policy reasons but not for business reasons.

The beginning of large-scale privatised enforcement

At the moment there appears to be a "tipping point", with governments apparently feeling that the openness that gives the internet its economic value is now so unbreakable that unfettered meddling by intermediaries for the protection of (mainly) intellectual property can be actively promoted.[12] They are not only promoting this approach internally, and not only in countries with strong democratic traditions, but across the globe, potentially blocking off markets and legitimising privatised surveillance and control on communication in totalitarian and highly controlled regimes. As a result, there has been a veritable rash of international-level measures which seek to encourage or coerce intermediaries – many with their own long-term vested interests in this – to filter, block and punish alleged online infringements.

In November 2010, the negotiating parties published the final text of the Anti-Counterfeiting Trade Agreement (ACTA). Although significantly improved from earlier versions, the section of the agreement on intellectual property enforcement circuitously talks about maintaining an internet service provider (ISP) liability regime which preserves "the legitimate interests of rights holders" and obliges parties to "endeavor to promote cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement"[13] – a footnote in a leaked draft explaining that "an example of such a policy is providing for the termination in appropriate circumstances of subscriptions and accounts in the service provider's system or network of repeat [alleged, presumably] infringers."

In February 2011, the World Intellectual Property Organization (WIPO) tried and failed[14] to launch a discussion[15] on internet intermediary liability for trademark infringements. This was followed in June 2011 by a side-event at a WIPO event in Geneva on the "role and responsibility of internet intermediaries in the field of copyright" which, interestingly, included no internet intermediaries at all! WIPO has also recently commissioned and published two independent studies on intermediary liability.[16] It has successfully tabled a workshop proposal for the Internet Governance Forum in Nairobi in September 2011 to discuss "thought-provoking ideas" such as in ACTA, the US Combating Online Infringements and Counterfeits Act (COICA) (which requires "blocking" by internet intermediaries) and the EU Intellectual Property Rights Enforcement Directive (whose use for mandatory internet blocking and surveillance is currently being assessed by the European Court of Justice).[17]

In June 2011, the Organisation for Economic Co-operation and Development (OECD) adopted its Communiqué on Principles for Internet Policy Making.[18] Under the heading "limit internet intermediary liability" it calls for states to undertake multi-stakeholder processes to "identify the

7 ec.europa.eu/information_society/newsroom/cf/itemlongdetail.cfm?item_id=3153

8 www.wired.com/epicenter/2011/01/bt-rejects-accusations-of-net-neutrality-breach-sort-of

9 www.dn.no/forsiden/etterBors/article2067200.ece

10 technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article6989510.ece

11 www.ft.com/cms/s/0/1ce4e1c8-1fd7-11de-a1df-00144feabdc0.html#axzz1STK17d9n

12 The draft PROTECT IP Act in the US was accused of allowing "the government to break the Internet addressing system" and "breaking the Internet's infrastructure" by a group of 108 professors in a recent public letter on this proposed legislation. blogs.law.stanford.edu/newsfeed/files/2011/07/PROTECT-IP-letter-final.pdf

13 www.ustr.gov/webfm_send/2379

14 www.ccianet.org/index.asp%3Fsid=5%26artid=213%26evtflg=False

15 www.wipo.int/edocs/mdocs/sct/en/sct_25/sct_25_3.pdf

16 www.wipo.int/copyright/en/internet_intermediaries/index.html

17 European Court of Justice Case C70/10

18 www.oecd.org/dataoecd/40/21/48289796.pdf

appropriate circumstances under which internet intermediaries could take steps to educate users, assist rights holders in enforcing their rights or reduce illegal content" (this communiqué itself was the subject of a multi-stakeholder process that civil society rejected).[19] The text avoids supporting network neutrality and instead meaninglessly refers to maintaining "appropriate" quality. It also pointedly avoids even a single reference to "due process", opting for the less restrictive and legally meaningless "fair process" instead.

Privatised policing in practice

So what does all of this mean on a practical level? As this approach is generally outside the rule of law, implementations tend to be very ad hoc. Across Europe, internet hosting providers and social networks delete material which they fear could result in them being liable, based on random criteria. As seen in the 2004 Bits of Freedom study, the same content will be deleted or left online depending on the unpredictable internal practices of the companies in question. Dutch social networking site Hyves will automatically delete anything if users with ten different IP addresses click the "report material" button. Remarkably, the European Commission has actively encouraged hosting providers to change their terms of service to give them an unfettered ability to delete anything they want.[20] Similarly, internet providers who started "blocking" websites accused of containing child abuse material are now being asked and sometimes required to introduce blocking measures for other content.

In Ireland, the former monopoly internet provider Eircom has agreed to become judge, jury and executioner on accusations of illegal downloading – cutting off consumers repeatedly accused of infringements[21] and blocking websites[22] accused by music industry interests of facilitating infringements. The Spanish "Sinde" law offers an interesting mix of rule of law and extra-judicial coercion. Under that approach, the plaintiff requests extra-judicial action from the internet provider first and, afterwards, if the internet provider wants to incur the expense of pursuing a court case, a judicial procedure is foreseen. In the US, the large ISPs that have been lobbying hard for the right to throttle bandwidth for their own commercial benefit have kindly offered to throttle bandwidth to users who have been repeatedly accused of copyright violations.

In addition to their business interest in this anti-net neutrality approach, the changing nature of the business (demonstrated *inter alia* by Comcast's purchase of NBC and Verizon's recent move to movie distribution)[23] creates new incentives for this approach. Smaller access providers will be increasingly "squeezed" – they are obliged to incur the cost of implementing technologies to be able to interfere with internet traffic in the absence of the economies of scale that would permit this to be done in a cost-effective way, or in a way which could be used for non-net neutral purposes.

In addition to the threats to citizens' ability to access the internet at all, to access an open and neutral internet, and to access material "voluntarily" or accidentally blocked by their ISP, there are also increasing efforts to use the structure of the internet itself as a law enforcement tool. The EU and the US, for example, have an ongoing project to discuss the revocation of domain names (on which the US claims wide-ranging jurisdiction)[24] and IP addresses[25] (the regional registry for Europe, the Middle East and parts of central Asia is located in the Netherlands). While the US approach is partly based on law, with COICA and the PROTECT IP (Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property) Act[26] planned to regulate the blocking and revocation of domain names, a non-legislative approach is also followed in some circumstances, such as regarding unlicensed online pharmacies. In the EU, blocking is regulated by law in some countries (France and Italy, for example), without law in others (the UK and Sweden) and with and without law in others, depending on the subject (such as in Denmark and, possibly in the future, the UK). Revocation of domain names, on the other hand, is generally without a legal framework.[27]

Conclusion

The promotion of a closed internet regulated outside the rule of law undermines efforts of Western governments to support the democratising potential of the internet in closed and totalitarian regimes. The

19 www.edri.org/files/CSISAC_Press_Release%20_0628011_FINAL.pdf
20 www.edri.org/edrigram/number8.15/edri-euroispa-notice-takedown-comission
21 www.theregister.co.uk/2009/02/03/eircom_agrees_to_three_strikes_enforcement
22 www.theregister.co.uk/2009/02/23/irma_demands_irish_isps_block_access_to_piracy_sites
23 www.nytimes.com/2011/07/17/opinion/sunday/17sun3.html?partner=rssnyt&emc=rss
24 digitizor.com/2011/07/06/us-jurisdiction-com-net-websites
25 www.theregister.co.uk/2010/04/27/eu_cybercrime
26 en.wikipedia.org/wiki/Protect_IP_Act
27 www.theregister.co.uk/2011/05/18/nominet_wrestles_with_net_cop_role

imposition of unreasonable jurisdiction claims over parts or all of the IP address allocation and domain name systems creates dangers for the integrity of the global internet. The outsourcing of policing of the internet and imposition of punishments by internet intermediaries contradicts basic democratic values and our democratic societies' view of the rule of law. The outsourcing of these activities to large corporations who have a publicly stated vested interest in the development and imposition of a non-neutral internet creates an online environment which is diametrically opposed to the openness of the internet. This openness gives us the democratic – and the economic – value of the internet and is too important for governments to simply take for granted and to experiment with as if it were insignificant. Our social interaction is increasingly online and freedoms which were previously unquestioned are now increasingly at the whim of private companies: our freedom of expression, our freedom of assembly, our privacy and our right to due process and presumption of innocence.

Next steps

- Activists should demand that the spirit and the letter of constitutional[28] and human rights[29] be respected
- The dangers of pushing world regions or individual countries into developing "splinternets" to avoid EU/US jurisdiction should be recognised.
- Positive positions of international organisations should be publicised as much as possible.[30]
- Positive political statements on the need to keep the internet open should be publicised and promoted.[31]
- The contradictions between calls for an open internet in certain countries and support for a privately regulated and closed internet domestically should be highlighted.
- More attention should be given to the economic damage of moving from an innovative, competitive and open internet to a closed non-neutral internet. ■

28 Such as the US First Amendment.

29 Such as Articles 8 and 10 of the European Convention on Human Rights and Article 19 of the International Covenant on Civil and Political Rights.

30 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

31 www.physorg.com/news/2011-02-clinton-renews-internet-access.html

GLOBAL INFORMATION SOCIETY WATCH 2011

In the year of the Arab uprisings **GLOBAL INFORMATION SOCIETY WATCH 2011** investigates how governments and internet and mobile phone companies are trying to restrict freedom online – and how citizens are responding to this using the very same technologies.

Everyone is familiar with the stories of Egypt and Tunisia. **GISWATCH** authors tell these and other lesser-known stories from more than 60 countries. Stories about:

PRISON CONDITIONS IN ARGENTINA Prisoners are using the internet to protest living conditions and demand respect for their rights.

TORTURE IN INDONESIA The torture of two West Papuan farmers was recorded on a mobile phone and leaked to the internet. The video spread to well-known human rights sites sparking public outrage and a formal investigation by the authorities.

THE TSUNAMI IN JAPAN Citizens used social media to share actionable information during the devastating tsunami, and in the aftermath online discussions contradicted misleading reports coming from state authorities.

GISWATCH also includes thematic reports and an introduction from Frank La Rue, UN special rapporteur.

GISWATCH 2011 is the fifth in a series of yearly reports that critically cover the state of the information society from the perspectives of civil society organisations across the world.

GISWATCH is a joint initiative of the Association for Progressive Communications (APC) and the Humanist Institute for Cooperation with Developing Countries (Hivos).

GLOBAL INFORMATION SOCIETY WATCH
2011 Report
www.GISWatch.org

ISBN 978-92-95096-13-4
9 789295 096134

APC

HIVOS