Internet Blocking

Crimes should be punished and not hidden

European Digital Rights
39 Rue Montoyer
B-1000 Brussels
tel: + 32 (0)2 550 4112
brussels@edri.org

European Digital Rights (EDRi)
is an association of
27 privacy and digital civil rights associations
from 17 Countries

Booklet written by

Joe McNamee
Advocacy Coordinator

Table of Contents

What is blocking?

Blocking involves leaving illegal websites online but simply making access somewhat more difficult. Access is *always* still possible, regardless of the blocking technology used.

By contrast, deletion or take-down of an illegal website involves removing it from the Internet and making access impossible.

Introduction and executive summary

The EU is considering a proposal to introduce filters for blocking of child abuse websites. European Digital Rights urges the Parliament and Council to rethink these plans. Child abuse and its portrayal on the Internet is a terrible crime that is sometimes of a severity that is scarcely believable. It must be treated seriously, with policies based on evidence and effectiveness and not on politics or gut reactions.

We must avoid policies which give Member States the opportunity to adopt cosmetic measures that we have already seen being used as a replacement for real action. Evidence from countries that have imposed blocking proves conclusively that this policy is employed as a replacement for real international action and is not applied as a complementary measure.

Creating a system to limit access to information brings with it huge risks:

- Weakening the political pressure on Member States to take real, effective, international action.
- Undermining the EU's credibility when addressing restrictions on communications in repressive regimes.
- Causing "mission creep" as the pressure inevitably grows – particularly in response to media headlines – to spread blocking measures into more and more areas.
- Bringing an end to the neutrality of the Internet as Internet Service Providers (ISPs) are forced to invest in technologies that can discriminate in increasingly invasive ways between different types of content.

We cannot simply launch a web blocking policy hoping that it might do some good – the benefits must be shown to outweigh the costs. The Commission's preparatory work did not treat the issue with the attention it deserves:

- Why has no evidence been presented to show that there is a perceptible benefit in the countries that have already introduced blocking?
- Why have the significant legal concerns raised by recent independent research[1] not been addressed by the Commission?
- Why has no research been carried out by the Commission regarding the scale and root causes of the problem of illegal sites being left online?

[1] http://www.aconite.com/blocking/study

EU approach on child abuse is weak and badly targeted

In order to protect certain business interests, extreme, disproportionate and potentially illegal measures are taken to remove or punish unauthorised activities. For child protection, the approach goes to the other extreme – measures that are both weak and directionless. *All* of our efforts must focus on ensuring that the police and judiciary have the resources to remove child abuse sites, prosecute criminals and identify victims. Anything else is a counterproductive distraction.

Business priorities	Child protection priorities
In 2004, IFPI's (International Federation of the Phonographic Industry) internet anti-piracy unit secured the take-down of 60,900 websites (Digital Music Report, 2004).	Some child abuse websites, hosted in countries with which the EU has excellent international contacts, allegedly remain online for months after being identified.
In the Anti-Counterfeiting Trade Agreement (ACTA), the United States demands removal of alleged copyright infringing sites.	EU "needs" to introduce blocking as it claims that these criminal websites are too difficult to address more effectively.
Bank phishing websites removed after an average of 4 hours.	Child abuse sites remain online for an average of 4 weeks.[2]
All international trade agreements signed by the EU contain binding obligations on protection of intellectual property.	There are no binding and enforceable international agreements that ensure rapid take-down of child abuse websites.
The European Commission invested 500,000 Euro in a project to investigate the impact of counterfeiting in the EU. It also paid one million Euro for a project on the impact of consumption of counterfeit goods.	European Commission policy on blocking is based on assumptions, due to a "lack of accurate and reliable statistics" (according to the Commission's "impact assessment").
Hollywood targets 50,000 peer-to-peer users with lawsuits (March 2010).	EU: No policy on peer-to-peer with regard to child abuse images.
The Commission supports a permanent secretariat for the Anti-Counterfeiting Trade Agreement.	The Commission stated in its impact assessment that it believes Member States will not implement the Council of Europe Convention adequately or fast enough. This is the justification given for proposing the Directive on Child Exploitation – more legislation rather than better enforcement.

[2]Tyler Moore and Richard Clayton: The Impact of Incentives on Notice and Take-down. Seventh Annual Workshop on Economics and Information Security (WEIS08), Dartmouth NH, USA, June 25-28 2008. In: M. Eric Johnson, editor: Managing Information Risk and the Economics of Security, pages 119-223, Springer, New York, 2008.

The issue is distorted by myths

"Internet blocking works"

Not only can end-users simply circumvent blocking, but criminals can easily evade it as well. The Canadian hotline observed[3] one website move 212 times in 48 hours – the introduction of blocking would encourage criminals to set up systems whereby they would move their site automatically when they detect that they have been added to a blocking list.

"Opponents of blocking believe that child abuse is a free speech issue"

Nobody has ever suggested that child abuse is an issue of freedom of speech or is the expression of an opinion. Free speech and freedom of communication will be the inevitable collateral damage of the building of the censorship infrastructure necessary for Internet blocking.

"The sites are in 'rogue states' where cooperation is impossible"

The material in question is almost exclusively based in western countries with high levels of Internet infrastructure. Although it appears this problem is now being addressed, EU hotlines have consistently said that the USA is home to the largest proportion of the illegal material.[4]

"We are talking about 'child pornography' so free speech laws prevent effective international action"

The most important of these sites are the ones containing depictions of sexual violence and abuse against children. This is universally illegal. We are morally (and under international law legally) obliged to take all possible action to ensure that the sites are deleted, the victims are identified and rescued, and the criminals involved are prosecuted.

"Is it not better to do *something?"*

Every legislative intervention has costs for society. In the absence of any clear benefits for blocking, it is bad practice to propose a wide-reaching measure with such substantial costs in terms of "mission creep" (the inevitable spread of blocking to other types of content), "technology creep" (the inevitable development of more and more invasive blocking technologies), damage to the EU's reputation for defence of free speech and the risk of providing an "early warning system" for owners of illegal sites.

[3] http://www.cybertip.ca/app/en/research
[4] http://www.hotline.ie/annualreport/2008-analysis/trends.html

Deleting instead of blocking sites is the only effective approach

Tackling the problem and not the symptom

Most child pornography material is not on freely available websites. Other, less obvious methods such as peer-to-peer networks and chat rooms are more amenable to hiding such illegal activity. Organised crime is clearly never going to be tackled by weak technology and weaker investigations. Real human beings with real resources are needed to tackle real crime.

Deletion of the material is possible

The Cambridge University study[5] comparing the take-down of financial fraud websites and child abuse pages shows that we can do better. Without a proper impact assessment identifying the current procedural and legal problems and which jurisdictions are the most problematic and why, effective policy-making is rendered much more difficult than it should be.

The blacklist will not be restricted to abuse sites

British ISPs were promised that government demands would be limited to "voluntary" blocking of child abuse sites. In April 2010, legislation was passed that creates a framework for blocking websites associated with civil offences of the unlawful sharing of intellectual property.

Danish ISPs were promised that government demands would be limited to "voluntary" blocking of child abuse websites. This was followed in early 2010 with a proposal to make ISPs criminally liable for providing access to gambling websites.

In the Frankfurter Allgemeine Zeitung on 13 April, 2010, Commissioner Malmström both talked about other subjects that could be blocked and more invasive technologies for blocking.

Blocking lists cannot be published, yet not publishing them means that proper transparency and safeguards are virtually impossible.

Did you know that in February 2010 a European Parliament resolution "strongly criticised" companies providing the Iranian authorities with censorship tools? Web blocking in Europe will increase the market for research, development and selling of such tools.

[5] Supra note 2 See: http://www.cl.cam.ac.uk/~rnc1/takedown.pdf

Blocking attempts to address yesterday's problem

Data from EU hotlines shows that blocking aims to solve yesterday's problems – static sites exclusively hosting illegal material. Figures from the UK's Internet Watch Foundation[6] show that the number of domains hosting illegal material has dropped by around half in the past four years.

Web-based material is now increasingly hosted on legitimate free web space, image hosting sites or hacked websites. Such sites are obviously eager to remove illegal material as quickly as possible – rendering blocking irrelevant. The misuse of legitimate image hosting sites to spread illegal material has grown from 0% in 2004 to 10% in 2006 and 40% in 2009.

Through its failure to adequately identify, let alone address, these trends, the European Commission is proposing a "solution" which is inadequate and counterproductive in order to solve the problem as it existed in 2004. The proposal also does nothing to address the bigger problem of peer to peer trafficking of abuse images.

Is the cost of creating this blocking infrastructure, the cost of mission creep, the cost of technology creep and the human cost of not spending these resources on victim identification worth the "benefit" of addressing an ever-smaller part of the problem with deficient technology?

Accessing blocked material is not "only for experts"

The European Commission and certain lobby groups have been propagating the myth that blocking is so difficult to work around that only someone "motivated" or an "expert" could manage to do it.

Websites exist, such as www.proxyforall.com or www.zend2.com, where a user can simply input the "blocked" page and they will receive immediate access.

Alternatively, people who access the Internet using privacy enhancing technologies (the development of which is funded by the Commission), are likely to find themselves accidentally circumventing blocking systems.

Finally, you can search for one of the many instructional videos online which explain to you in five minutes or less how to bypass your Internet provider's equipment and therefore any blocking that it has installed.

[6] IWF annual reports 2006 and 2009 (http://www.iwf.org.uk) and BBC news site: http://news.bbc.co.uk/2/hi/technology/10108720.stm

States hide behind empty gestures

Historically, EU Member States have preferred making noises about child protection to real international action. Repeated failures to respect international agreements demanding action on child abuse show the dangers of allowing Member States to hide behind blocking policies.

1990 UN Convention on the Rights of the Child and 2000 Optional Protocol on child pornography

Article 34: “Take all appropriate national, bilateral and multilateral measures to prevent the exploitative use of children in prostitution or other unlawful sexual practices.”

1996 Stockholm Declaration

“Concerted action is needed at the local, national, regional and international levels to bring an end to the phenomena.”

1999: ILO Convention on the worst forms of child labour

“Each Member shall [...] take effective and time-bound measures to provide the necessary and appropriate direct assistance for the removal of children from the worst forms of child labour.”

2000 UN Optional Protocol on sale of children, child prostitution and child pornography

The 22 EU Member States that have ratified this Protocol are obliged to take “all necessary steps to strengthen international cooperation by multilateral, regional and bilateral arrangements for the prevention, detection, investigation, prosecution and punishment of those responsible for acts involving the sale of children, child prostitution, child pornography.”

2001 Yokohama Global Commitment

“We reaffirm, as our primary considerations [...] enhanced actions against child prostitution, child pornography and trafficking of children for sexual purposes, including national and international agendas.”

The time to take effective, proportionate and durable action is now. States must not be given another media-friendly non-action to hide behind.

Leading experts say “no” to blocking

“Blocking websites has little long term impact on distribution.”

Grant Agreement signed by the European Commission and the European Financial Coalition Against Child Pornography (January, 2010)

“Our blocking measures are unfortunately not leading to a reduction in web-based pornography.”

Björn Sellström
Head of Swedish Police Investigation Group on Child Pornography and Child Abuse

“Sweden’s Prime Minister Fredrik Reinfeldt says he has stressed the merits of uncensored Internet access in a meeting with Chinese Vice President Xi Jinping. Reinfeldt says they discussed human rights, democracy and the freedom of expression ‘and I especially emphasized ... the significance of the Internet in that context.’ ”

Business Week (30 March 2010)

“Technically, it is difficult. Legally, it is problematic. Above all, it represents a real threat to the free transfer of information and conflicts with basic democratic principles.”

Cormac Callanan, co-author of Council of Europe report on cooperation between Internet service providers and law enforcement authorities

“According to the ECtHR, ‘necessity’ within the meaning of Article 10(2) implies the existence of a ‘pressing social need’ [...] it is undoubtedly more difficult to satisfy the necessity test for Internet content, because users seldom encounter illegal content accidentally.”

Report of the OSCE Representative on Freedom of the Media on Turkey and Internet Censorship

“Blocking clearly is disproportionate, as the infrastructure implementing this measure will spread into other technologies and topics completely unrelated to child abuse images.”

Christian Bahls
Chairman of the Association of Abuse Victims against Internet blocking

Did you know?
On her blog, Commissioner Malmström has accused the United States of leaving child abuse websites online for over a year in some cases. If this is true, the lack of effective engagement with the USA on this issue means that all EU Member States have failed to respect their obligations under both the European Convention on Human Rights and the UN Convention on the Rights of the Child to take positive international action to ensure child protection.

The Commission's policy-making is incoherent

Why was no external expertise requested?

Why does the explanatory memorandum of the proposed Directive explain that there was "no need for external expertise" while the Commission is paying for external expertise with regard to policy (including the feasibility of blocking) on terrorist use of the Internet?

Why is internal Commission information not public?

The European Commission requires the hotlines that it funds to provide statistical data regarding the reports that they receive. This information could have been used to demonstrate the impact of blocking. Why, after paying for these statistics, is the Commission hiding them?

Why give the Member States a smokescreen if they can't be trusted?

The Commission's impact assessment on the proposed Directive on child exploitation says, in essence, that the Member States cannot be trusted to implement the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse. Why then allow Member States to hide their own inactivity by putting the emphasis on blocking rather than taking real action?

What specifically is blocking supposed to achieve?

The Commission says that blocking will limit accidental access to illegal sites. Where is the evidence that this is a major problem that means that resources should be spent on blocking rather than, for example, victim identification?

To what does the European Commission attribute its total failure in its international cooperation?

How has it been possible for both the EU and individual Member States to achieve so little for so long, with so little hope of improvement, that blocking is seen as the only option?

Did you know?
Blocking is an approach – not a technology. As technologies change, the implications of mandatory blocking will change without any democratic intervention as to whether the latest innovation respects privacy or human rights.

The Commission facilitates illegal action by Member States

When the Commission launched its original proposal, the blocking measures would have required laws to be introduced in the Member States. This is necessary to be in compliance with Article 10 of the European Convention on Human Rights – "the exercise of these freedoms [...] may be subject to such formalities [...] as are prescribed by law."

This need for a legal basis was confirmed in the otherwise rather empty impact assessment. "Such measures must indeed be subject to law, or they are illegal."

In the Council, Member States such as the United Kingdom, that already have "voluntary" blocking, opposed this measure as they did not want to introduce legislation.

As a result, the European Commission amended its proposal to simply require "measures" to be taken to bring about blocking instead – thereby avoiding the opposition of the countries that carry out blocking without a legal basis.

It is clearly inappropriate for the Commission to actively, consciously and deliberately alter its proposal for the sole reason of facilitating an activity that it believes is in contravention of the European Convention on Human Rights.

The proposal abandons basic principles of better regulation

According to the European Commission, the purpose of an "impact assessment" is "to help in structuring and developing policies. It identifies and assesses the problem at stake and the objectives pursued."[7]

The Commission's "impact assessment" does not address the limitations of current blocking technologies, the implications of possible future blocking technologies, the societal dangers of the inevitable blocking of innocent sites, the impact of the likely spread of blocking to other types of content, the nature of the problems that lead to criminal websites remaining online for extended periods, the possible impact of less intrusive measures nor the impact of blocking in countries where it has been imposed.

[7] http://ec.europa.eu/governance/better_regulation/impact_en.htm

Blocking by self-regulation – the beginning of the end of the open Internet

The European Commission's proposal was amended before publication in order to ensure that blocking via "self regulation" would be possible.

This "self-regulatory" approach is part of a much wider strategy of using Internet Service Providers (ISPs) to police the Internet, in a less predictable, less democratic and more pervasive way than regulation undertaken by the state. Some current initiatives include:

- The draft Anti-Counterfeiting Trade Agreement (ACTA) suggests limiting ISP legal protection from liability unless unspecified policing "policies" are put in place by ISPs.[8]
- The Council of the European Union in its resolution on IPR enforcement calls for "the Commission, the Member States and the relevant stakeholders to pursue ongoing dialogues and to resolutely seek agreements on voluntary practical measures."[9]
- Discussions on Internet blocking among the Member States are reportedly leaning towards "self-regulatory" measures rather than them having a legal basis, as required by Article 10 of the European Convention on Human Rights.
- The European Commission's dialogue on "notice and take-down of illegal content" and "stakeholder dialogue on illegal up/downloading" aim to achieve extra-judicial policing activities by Internet providers.
- UK ISP Virgin Media has indicated that it will start wide scale surveillance of its customers, while Irish ISP Eircom has undertaken to carry out both "three strikes" policies and website blocking in response to *allegations* of intellectual property infringements.

Did you know?
Criminals will be able to check if their sites are on blocking lists and move them to other locations automatically, if necessary. As a result, blocking risks becoming a useful tool for protecting criminal activities rather than an effective measure to fight cybercrime.

[8] http://blog.die-linke.de/digitalelinke/wp-content/uploads/674b-09.pdf
[9] http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/113098.pdf

Case study: Italy

In Italy, blocking is undertaken for multiple purposes, by multiple agencies and with and without the protections required by the European Convention on Human Rights.

Italian Monopoly Administration Authority (AAMS)

The Italian Monopoly Administration Authority has drawn up a blacklist of approximately 1750 websites that provide various gambling services. This list is public and ISPs are obliged by law to block all of the sites.

Italian police

Building on the secret CIRCAMP international blocking list, the Italian police have added further sites without judicial intervention. This makes a total of between 600 and 900 sites which they claim contain child abuse images. Internet providers are legally obliged to block all of these sites.

Judiciary

Court orders are also used to add to the list of sites to be blocked by ISPs in Italy. Sites blocked include an anti-mafia website (accadeinsicilia.net[10]) for being an unauthorised press publication, a consumer organisation, for defamation (aduc.it), a free online advertising website for facilitating prostitution (bakeca.it) and a file sharing site (thepiratebay.com).

Other types of blocked content

Sites facilitating the purchase of cigarettes abroad, a website containing information about steroid use, a Korean university website, for reasons that are not immediately obvious, and a gay website have also been added to blocking lists.

Mission creep

The next steps to limit the right to communication in Italy include the Pecorella-Costa bill to impose press obligations on ordinary websites, the Carlucci law (written by the audiovisual lobby) to ban anonymity online, the Alfano law imposing a "right to reply" to anyone who says their interests were undermined by a blog, the Pisanu law to log (with personal identification) all Internet connections including via WiFi, etc.

[10] No longer online.


STOP
Stop believing that hiding
a problem will somehow
help to solve it

With the expert support of:

Dutch Online Parents Association
http://www.ouders.nl

http://www.archrights.org.uk