Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam

M +31(0)654386680
E ot.vandaalen@bof.nl
W www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

Aan de leden van de Vaste commissie voor Justitie van de Tweede Kamer

Betreft:
Kamerbrief Internetfiltering
"Verwijderen, niet verbergen"

Datum:
Amsterdam, 30 maart 2010

Geachte Kamerleden,

1. De stichting Bits of Freedom ("**Bits of Freedom**") heeft bezorgd kennis genomen van de recente ontwikkelingen rondom het instellen van een internetfilter ter bestrijding van kindermisbruik. Het aanpakken van deze ernstige vorm van criminaliteit staat natuurlijk niet ter discussie. Maar internetfilters zullen kindermisbruik onder het tapijt vegen, zonder het daadwerkelijk te bestrijden. Tegelijkertijd zal het internet door deze vorm van filtering verregaand gecensureerd kunnen worden. In het licht van het 'Algemeen Overleg Kinderporno' op 31 maart 2010, wil Bits of Freedom u ondersteunen internetfiltering zowel op Nederlands als Europees niveau een halt toe te roepen.

2. Deze Kamerbrief is mede gebaseerd op de standpunten van 'Verein MOGiS' ("**MOGiS**"), een Duitse belangengroepering opgericht door slachtoffers van kindermisbruik[1] Zelfs zij voeren actie tegen het filteren van websites, zowel in Duitsland als in Europa.

3. In deze brief komt Bits of Freedom tot de volgende conclusies:

   - **Filteren werkt niet:** het filteren van websites is een ineffectieve maatregel ter bestrijding van kindermisbruik. De overgrote meerderheid van het gewraakte materiaal wordt namelijk via andere kanalen verspreid, zoals post, peer-to-peer netwerken, nieuwsgroepen en chatprogramma's.[2]

1 De Nederlandse vertaling van de oproep van MOGiS – *"Verwijder, niet filteren! – Reageer, en kijk niet weg!"* – is te vinden via: http://mogis-verein.de/eu/nl/. Deze brief is als 'Bijlage I' bij deze kamerbrief opgenomen. Overigens mijdt MOGiS de term 'kinderporno', aangezien dit een onwenselijk en misleidende uitdrukking van het fenomeen is. Zij hanteren de term 'kindermisbruik', het betreft hier immers geen pornografie maar seksueel misbruik van kinderen.

2 Zie voor meer informatie de brief van MOGiS (Bijlage I) en de open brief van het European Digital Rights Initiative ("**EDRi**") aan EU-commissarissen Malmström, Reding en Kroes, te raadplegen via http://www.edri.org/edrigram/number8.5/edri-open-letter-internet-blocking. De brief van EDRi is als 'Bijlage II' opgenomen in deze kamerbrief.

- **De afbeeldingen blijven online**: door het filter wordt het gewraakte materiaal niet bij de wortel uitgeroeid, maar alleen verborgen. Met een filter blijven de online afbeeldingen van kindermisbruik bestaan, worden de daders niet vervolgd en de slachtoffers niet geïdentificeerd.[3]
- **Een instrumentarium voor internetcensuur:** het filter zal, als het er eenmaal is, ook ingezet kunnen om ander materiaal te blokkeren ("*function creep*"). Dit is geen theoretisch risico. Zo heeft het Australische internetfilter ertoe geleid dat websites over euthanasie en enkele pagina's van online encyclopedie Wikipedia werden geblokkeerd.[4] In Nederland is te verwachten dat de muziek- en filmindustrie websites als The Pirate Bay aan deze lijst zouden willen toevoegen.
- **Effectieve alternatieven, zonder censuur:** een veel betere manier om kindermisbruik te bestrijden, is het verwijderen van de websites en het opsporen vervolgen van daders. Dit kan onder andere bereikt worden door (i) verdere internationale samenwerking om afbeelding van kindermisbruik van het internet te verwijderen[5] en (ii) vaart te zetten achter het opzetten van de 'EU Financial Coalition against Child Pornography', zodat betalingen voor afbeeldingen van kindermisbruik in beeld komen van de opsporingsdiensten – een in de Verenigde Staten succesvol initiatief.[6]

4. Om deze redenen roept Bits of Freedom de Nederlandse overheid op de verleiding van symboolpolitiek te weerstaan: **"verwijderen, niet verbergen"** dient haar credo te zijn. Zij moet afzien van de introductie van het internetfilter, en op Europees niveau bij de behandeling van de ontwerp-richtlijn 2010/0064/COD haar steun aan internetfiltering (artikel 21) ontzeggen.[7] Nederland zal daarin niet de enige zijn: ook Eurocommissaris Viviane Reding en de Duitse Minister van Justitie Sabine Schnarrenberger tonen zich tegenstander van internetfiltering.[8]

Over Bits of Freedom

Bits of Freedom verdedigt burgerrechten in de digitale wereld. Zij doet dat door constructieve campagnes te voeren en de overheid te informeren. Het belang van de burger staat daarbij centraal.

Bits of Freedom vertrouwt erop u hiermee voldoende te hebben geïnformeerd en houdt zich graag beschikbaar voor een nadere toelichting als daaraan behoefte bestaat.

Hoogachtend,

Ot van Daalen

---

3 Zie zowel Bijlage I als Bijlage II.

4 The Sunday Morning Herald, *Dentist, tuckshop cited on web blacklist* (19.03.2010): http://www.smh.com.au/articles/2009/03/19/1237054973414.html . Zie verder zowel zowel Bijlage I als Bijlage II.

5 Met name tussen de Verenigde Staten, Duitsland en Nederland – deze landen vormen de top drie als het gaat om het hosten van afbeeldingen van kindermisbruik. Zie bijlage II.

6 Zie bijlage II.

7 Te raadplegen via: http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=en&DosId=199159

8 Zie: http://tweakers.net/nieuws/66452/europa-wil-internetfilters-tegen-kinderporno-verplichten-update.html

MOGiS e.V. - Eine Stimme für Betroffene

Nederlands

The orginal appeal in English
Retweet aub deze pagina door hier te klikken
De Engelse Twitter pagina van MOGiS e.V. (@MOGiS_en)

Wij zijn MOGiS e.V. – een Duitse organisatie bestaande uit slachtoffers van seksueel misbruik. MOGiS is opgericht in April 2009 als"MissbrauchsOpfer Gegen InternetSperren" ("Misbruikslachtoffers tegen internetblokkade"). Wij verzetten ons tegen het blokkeren van webpagina's als middel om de verspreiding van seksueel kindermisbruik bevattend materiaal op het internet te voorkomen. Wij eisen internationale samenwerking op het gebied van de verwijdering van seksueel kindermisbruik bevattende afbeeldingen en video. Een goed voorbeeld van dit soort samenwerking is hetINHOPE internet hotlines netwerk.

Onze Slogan: "Verwijder, niet filteren! — Reageer, en kijk niet weg!"

We werden nogal verrast door het vervroegd uitlekken van het voorstel van de Raad van Ministers van de Europese Unie. Deze webpagina zal doorlopend worden bijgewerkt met referenties en feiten. Mocht u vragen en/of opmerkingen hebben of zelfs toegang hebben tot filterlijsten in andere landen, neem dan contact met ons op via "info.eu (at) mogis-verein.de".

COSPOL, CIRCAMP en de CSAADF

door Christian Bahls

Door de voorstellen van de Raad van Ministers van de Europese Unie staat het verplicht blokkeren van websites weer ter discussie. De EU lidstaten zullen binnenkort worden verplicht om de toegang tot bepaalde websites te blokkeren door gebruik te maken van een geheime blokkadelijst welke wordt uitgewisseld door de politie van de lidstaten zonder de rechtssysteemen van deze lidstaten erin te betrekken.

De EU-lidstaten zullen hun nationale providers verplichten de DNS-database te manipuleren op basis van deze geheime blokkadelijst. Om dit te implementeren moet de gehele nameserver infrastructuur van ISPs worden aangepast. Eenmaal geïmplementeerd kan dit mechanisme worden gebruikt om de toegang tot elke willekeurige website te blokkeren.

Laten we eerst een paar feiten op een rij zetten:

- *"Kinderpornografie"* als term is een een onwenselijke en misleidende simplificatie van waarover wij het over hebben. Het kind is immers geen prostituee (porneia) noch is er van illustratie (grapho) sprake. We hebben het in feite over de documentatie (afbeeldingen of films) van seksueel misbruik van kinderen. Het kan daarom aldus ons beter benoemd worden als "afbeeldingen van seksueel kindermisbruik" . Daarmee wordt ook een signaal naar degenen die deze plaatjes bekijken gestuurd: zij zijn geen pornografie maar afbeeldingen van seksueel misbruik van een kind aan het consumeren. De beschikbaarheid van dat soort materiaal bevordert alleen het lijden van de betrokken kinderen.
- Als we kijken naar Duitse politie-statistieken, kunnen wij vaststellen dat het misbruik van een op de honderd kinderen die seksueel misbruikt zijn, (voornamelijk door familieleden of aanverwanten) op camera wordt

vastgelegd (98 van de 15098 misbruikslachtoffers in 2008).
- Hoewel het grootste deel van deze inhoud waarschijnlijk via post of mobiele telefoons wordt verspreidt komt een deel van deze kindermisbruik bevattende afbeeldingen vervolgens op het internet terecht.
- On the Internet one of the redistribution channels is the Web (the other (far bigger) channels would be P2P and E-Mail). In 2008 the german INHOPE handled 2562 complaints about the distribution of abuse imagery on the Internet, of those 2562 complaints only 449 were about content to be found in the Web.
- Op het internet is overigens maar een gering aantal van de herdistributiekanalen aan het normale www-web toebedeeld. Andere, veel omvangrijkere, kanalen zijn P2P en E-mail. In 2009 heeft INHOPE contact "Internetbeschwerdestelle" 2562 klachten over de distributie van afbeeldingen van misbruik op internet behandeld. Van deze 2562 klachten gingen 449 over inhoud die op internet te vinden was.
- Een internetfilter is gericht op het web.

Dus laten we kijken naar wat wordt voorgesteld:

Actieplan:

• fase 1: introductie van technologie om websites te blokkeren met als doel de distributie van afbeeldingen van sexueel kindermisbruik tegen te gaan. Dit systeem heet CSAADF ('Child Sexual Abuse Anti Distribution Filter").
• Fase 2: Analyseer de websites en identificeer de juridische elementen in het bedrijfsmodel en ontneem de mogelijkheid om winst te maken.
• Fase 3: het opsporen van de mensen die financieel gewin hebben bij de commercieele distributie van kindermisbruik materiaal.

Dit plan lijkt ietwat ontoereikend, omdat men alleen in fase 3 achter de criminelen die dit soort materiaal verspreiden aangaat. Hetgeen compleet mist in dit actieplan is het bevrijden van kinderen die misbruikt worden, dit zou stap 1 moeten zijn. Als er echt nog steeds een betaalde markt is voor dit soort materiaal, zou dit makkelijk samengevoegd kunnen worden met "*het vangen van criminelen door het geld te volgen*".

Het is raar en eigenlijk verontrustend dat de EU-lidstaten meewerken aan het maken van een filterlijst (newspeak voor "*blokkeerlijst*") maar niet welwillend lijken te zijn om mee te werken aan het verwijderen van afbeeldingen van kindermisbruik. Het is vooral verontrustend dat het voor banken mogelijk is om phishing-websites in 4 tot 8 uur te verwijderen terwijl beelden van sexuele kindermishandeling pas na dertig dagen of langer gewist kunnen worden..

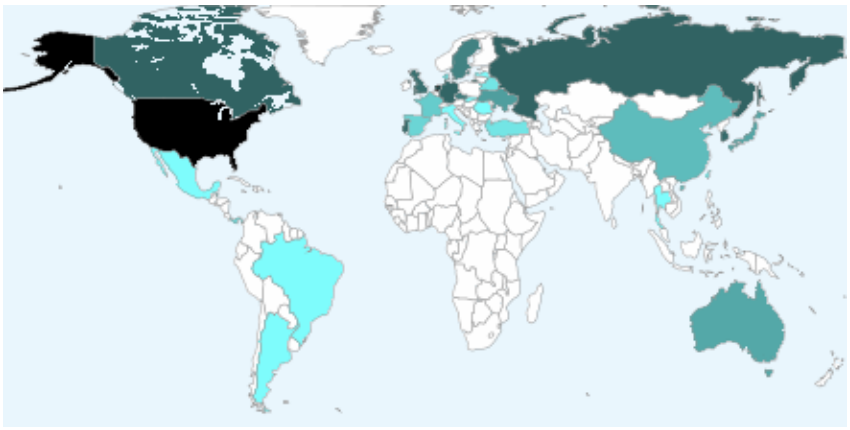
Voor de duidelijkheid: beelden die van internet zijn verwijderd hoeven niet op een zwarte lijst te worden geplaast. In plaats van het blokkeren van de documenten van sexueel misbruik van kinderen hoeven deze afbeeldingen alleen verwijderd te worden door een van de lidstaten. Er moet dus meer worden samengewerkt.

Dus laten we kijken wie werkt aan CIRCAMP:

- De motor achter het proces: Noorwegen
- Mede initiator: het Verenigd Koninkrijk
- Landen die voorop lopen: Denemarken, Belgie, Frankrijk, Finland, Ierland, Italie, Malta, Polen, Zweden, Nederland, Spanje, Duitsland
- Ondersteuning: Europol and Interpol

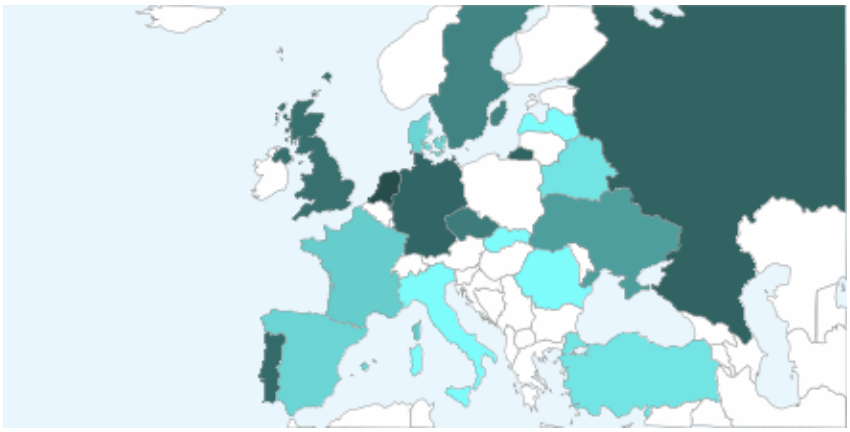
Dus laten we iets beter kijken, naar de statistieken.

Vanuit welke landen worden de websites op de Noorse zwarte lijst gehost?
like:



Origin of entries on Norwegian blocking list (world)

A closeup of Europe:



Origin of entries on Norwegian blocking list (Europe)

VS:1292, NL:146, CA:79, RU:75, DE:69, KR:62, PT:61, GB:54, CZ:37, SE:32, UA:15, JP:12, AU:11, HK:8, BZ:8, CN:6, BS:5, FR:4, PA:3, ES:3, DK:3, TW:2, BY:2, TR:1, TH:1, SK:1, RO:1, NO:1, MX:1, LV:1, IT:1, BR:1, AR:1; the server in .no (Noorwegen) is een test-server van de Noorse politie.

Tot zover de internationale samenwerking voor het verwijderen van afbeeldingen van sexueel kindermisbruik op het internet. De VS en Canada zijn niet, wat we normaal gesproken een onbetrouwbare staat ("failed state") zouden noemen. Juist interessant is het te zien, dat Canada zelf technology gebruikt om enigszins te blokkeren.

Het Verenigd Koninkrijk met steun en hulp van de Internet Watch Foundation (IWF) stelt een blokadelijst samen voor de "Cleanfeed" die door Britse ISPs geimplementeerd is. De IWF werd bekend nadat het in December 2008 een Wikipedia artikel op de blokkadelijst zette omdat het een cover afbeelding van het scorpions muziek album "virgin killer" bevatte.

Hoewel Nederland ook plannen heeft op het gebied van het blokkeren van websites, zijn zij altijd in de top 5 van landen die geblokkeerde sites bevaten. En wat in het bijzonder zorgwekkend is, is dat de Nederlandse zwarte lijst een Nederlandse website blokkeerde. Dit laat echt fase 1 van CIRCAMP zien. Het hoofddoel is enkel de uitwisseling van addressen die moeten worden geblokkeerd. Men voelde vervolgens niet de plicht om die websites ook offline te halen.

Een ander voorbeeld is Finland, die de finse beveiligingsonderzoeker Matti Nikki blokkeert, die tegenstand biedt aan het blokkeren van internet in zijn land door het analyseren van de zweeds/finse blokkingslijst en het publiceren van de details van die analyse. De analyse toont aan dat maar 37 van de 1047 websites op de uitgelekte blokkingslijst inderdaad afbeeldingen bevatten van sexuele kindermisbruik. (9 [rood] + 28 [oranje] van Matti Nikkis' analyse)

Over Duitslands buurland Denemarken: zij blokkeerden 200 Duitse websites, onder andere een islamitisch videoforum.

In het document dat boven gelinkt is staat Duitsland genoemd als voorlopend, maar dankzij de sterke [grass roots movement] van de *AK Zensur*(werkgroep tegen internetblokkeren en censuur) en andere civiele vrijheidsgroeperingen

zoals *AK Vorat* (werkgroep tegen het bewaren van data [data retention]), *FoeBuD* e.V". en organisaties van [abuse survivors] zoals *Trotz Allem* e.V"., gegen-missbrauch e.V". en *MOGiS* e.V".In Duitsland lijkt men op de goede weg te zijn uit dit gekkenwerk.

De implementatie van de DNS manipulatie is gestopt – sommige veranderingen zijn al terug gedraaid. Op dit moment discussieert het Duitse parlement de afschaffing van "***filteren***" ten voordele van "***verwijderen***". Dit kan zelfs een van de redenen zijn waarom blokkeren op een europese schaal wordt voorgesteld door het Spaanse EU-presidentschap.

Omdat wegkijken precies datgene is dat gebeurt in familie's (of organisaties) als kindermisbruik wordt blootgelegd is MOGiS's slogan:

"Verwijder, niet filteren! — Reageer, en kijk niet weg!"

Dat is wat we het afgelopen jaar consequent en inmiddels al behoorlijk succesvol hebben lopen communiceren in Duitsland.

Het is nu tijd om het probleem van web-blocking op een internationaal (op zijn minst Europees) niveau te brengen. We moeten ons verenigen tegen de verregaande beperking van burgervrijheden over de hele wereld.

Christian Bahls; MOGiS e.V.
abuse survivors against internet blocking

Retweet aub deze pagina door hier te klikken

Open Letter to Commissioner Malmström
and Commission Vice-Presidents Reding and Kroes

Dear Commissioners,

European Digital Rights is an association of 27 privacy and digital rights organisations in 17 European countries.

We would like to congratulate you on your nominations and approval as members of the new Commission, led by President Barroso.

Our association warmly welcomes the statements made during your hearings on the need to place the citizen at the centre of decision-making, to ensure a "zero-tolerance policy as regards violations of the Charter" and to ensure that policy-making is "evidence-based". In this context, Commissioner Reding's comments on the Data Retention Directive were particularly welcome.

If the new Commission is able to maintain its independence and deliver citizen-centred and evidence-based policy, this will not alone serve to revitalise civil rights in Europe but it will serve to re-establish the EU as a leader for democracy and civil rights in the world.

Testing the new approach

One of the first decisions that will be taken by the new Commission will be a direct test of whether such an approach will survive political realities. That decision will be the re-launch of the "Proposal for a Council Framework Decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA". EDRi strongly supports the aims of that legislation and hopes that the new instrument will be an effective tool in fighting child exploitation. We do, however, have serious concerns about the draft which which was published last year (prior to being withdrawn due to the entry into force of the Lisbon Treaty).

The original draft of that revised Framework Decision (COM(2009)135) made a proposal for the mandatory blocking of websites deemed to contain illegal images of child abuse ("child pornography"). That measure, which may not be in the best interests of the abused children is, as proven by the remarkably poor accompanying "impact assessment" (SEC(2009)355), an example of legislation proposed without evidence and without due regard for human rights. Unfortunately, as a measure which superficially sounds like a positive move, it is also an attractive option politically, which creates the temptation to legislate based on impulse rather than on evidence, legality and effectiveness.

The proposal is flawed on the basis of law, flawed on the basis of possible effectiveness, flawed on the basis of unintended consequences for the fight against online child abuse and flawed on the basis of inevitable damage for freedom of communication and privacy in the online world.

Elements of an effective and proportionate strategy

In order to deal with the issue of websites portraying child abuse in an effective way, the following issues must be analysed and addressed based on the evidence available:

- The nature of the problem being tackled
- The legality of the measure being proposed
- The scope, scale and nature of possible unintended consequences
- The availability of less intrusive measures

The nature of the problem being tackled

As repeatedly and consistently shown by figures produced by EU hotlines[1], the websites that are targeted by blocking measures are not in some distant "rogue states" that the EU has no influence over – they are hosted on the territories of our major trading partners.

What is needed is comprehensive international law enforcement cooperation – the last thing that is needed is a policy which does nothing to address the actual problem but reduces the political pressure for effective action. Blocking leaves the material online, leaves criminals free and unprosecuted and victims unidentified and unprotected. As a society, we cannot simply accept that the European Union is unable to export its best practice on hotlines, investigation and "notice and takedown" of sites containing material that is universally condemned.

The legality of the measure being proposed

The recent research undertaken on behalf of the Organisation for Security and Cooperation in Europe on Freedom of the Internet in Turkey[2] evaluates the legality of Internet blocking in that country. The report analyses some issues which are particular to that country, but its assessment regarding the core issues of (in)compatibility of Internet blocking with the European Convention on Human Rights would also hold true for every country that is bound that instrument. That analysis leads to the same conclusions as an independent study[3] prepared in 2009 by four leading cybercrime experts on "Internet blocking – balancing cybercrime responses in democratic societies". That research also raised a variety of serious practical and legal questions about the issue of blocking.

Even if one looks narrowly just at the central criteria used by the European Court of Human Rights, one can see the fundamental legal problems of Internet blocking:

- **Suitability**. This criterion is not met as all current blocking technologies are comparatively easy to circumvent.
- **Necessity**. Based on the "impact assessment" accompanying the original proposal, the actual purpose for the blocking measure is unclear. We can guess that its purpose is to address:
  - accidental access, which is an invalid justification as this rarely happens
  - deliberate access, which is an invalid justification as blocking measures are easy to circumvent

1 See http://www.iwf.org.uk/media/news.archive-2007.196.htm for example.
2 http://www.osce.org/documents/rfm/2010/01/42294_en.pdf
3 Executive summary: http://www.aconite.com/sites/default/files/Internet_Blocking_and_Democracy_Exec_Summary.pdf
Full report: http://www.aconite.com/sites/default/files/Internet_blocking_and_Democracy.pdf

- disruption of commercial sites, which is an invalid justification as other solutions are proving more effective (see information on the “financial coalition” below)

– **Proportionality**. This criterion is not met due to overblocking (where innocent sites are blocked) and underblocking (where illegal material is not blocked). Proportionality is also undermined by the inevitability of “mission creep” (the blocking of more and more types of content)

The scope and nature of possible unintended consequences

Currently, all but one EU country that implements blocking does so using “DNS blocking”. This technology is cheap and easy to circumvent. As blocking is a political measure used to create the appearance of action, while no effective measures are really being taken, the ineffectiveness of the technology has never been a particular concern for its political supporters.

However, as “mission creep” moves blocking into other areas, such as gambling (as currently either in force or planned in Italy, Belgium, Denmark, Poland and France), effectiveness will become more significant – national gambling monopolies will demand blocking that actually works rather than blocking that can be used for public relations purposes. As a result, it is easy to envisage more invasive technologies, such as BT's Cleanfeed, (currently deployed in the UK) and, ultimately, “deep packet inspection” being demanded and mandated.

With blocking already creeping into other policy areas, from the protection of national gambling monopolies in the above-mentioned countries to IPR infringements (based on the initial ruling in the Scarlet/Sabam case in Belgium and envisioned by the French HADOPI law), the EU's credibility in condemning restrictions to communication freedom in Iran, China and elsewhere will be eroded to the point of simple farce. Worse still, the work done to develop ever more effective blocking measures will serve to support imposition of these restrictions in such countries. In February 2010, the European Parliament adopted a resolution criticising companies for “providing the Iranian authorities with the necessary censorship and surveillance technologies”. In this context, it would be very unfortunate if the Commission were now to make a proposal in favour of Internet blocking which would have the unintended consequence of increasing the market for such technologies.

Indeed, the European Commission's credibility with regard to human rights is already being put under pressure by Internet blocking. While the EU will shortly accede to the European Convention on Human Rights, which provides that freedom of communication “may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law”, the European Commission currently funds the CIRCAMP project, which supports extra-judicial Internet blocking via industry “self-regulation” in several EU Member States. To quote the Commission's own impact assessment “such measures must indeed be subject to law, or they are illegal”.

The availability of less intrusive measures

A bad policy should not be implemented simply because nobody can think of anything better to do. However, there are some obvious steps that could be taken. We have had an unending list of International Treaties from the International Labour Organisation, the United Nations, the Council of Europe and others over the last twenty years on the issue of child abuse images. What is needed is focussed, evidence-based actions that deal with the crime as a crime and not as a nuisance that can be somehow “switched off”. The following points should be considered in this regard:

- The EU's system of hotlines and “notice and takedown”, based on the safe harbour protections for Internet access and hosting providers (Directive 2000/31/EC) is an effective measure that has been in place for most of the history of the world wide web. The country identified as hosting most of the illegal websites is the United States – it seems incomprehensible that the USA proposed “notice and takedown” for websites infringing intellectual property within the context of the ACTA negotiations, yet the EU is unable to persuade the USA to implement such a policy as regards child abuse websites that are, in effect, crime scenes.
- Secondly, the time has come to fully implement the UN Convention on the Rights of the Child. This calls for “*all* appropriate national, bilateral and multilateral measures to prevent the exploitative use of children in pornographic performances and materials.” Commissioner Frattini's call on Russia to take action against sites hosted in that country is a rare, laudable and, above all, successful example of the UN Convention's obligations being respected. Other examples are very hard, if not impossible, to find.
- The delays in setting up of an effective “EU Financial Coalition against Child Pornography” are entirely unacceptable. The US model already exists, is already effective, does not use public funds and is already successfully leading to prosecutions. Why has it taken over two years of discussions and one year of funding by EU taxpayers to produce fewer results, less focus and more costs in the EU – despite the fact that many of the same companies are involved? We ask Commissioner Malmström to become personally involved to ensure that this initiative narrow its focus to that of the US coalition and start operations without any further needless delay. The tools are available to ensure that no EU citizen can feel secure when paying for child abuse images online – it is time to put them in place. Finally, we wish to stress that industry “self-regulation” should never be used in a way which circumvents legal protections, democratic decision-making or places private business priorities ahead of those established by democratically-elected governments.[4]

Conclusion

We remain hopeful that the undertakings made during the hearings in the European Parliament will be effectively implemented and that new Commission will make an evidence-based proposal on this issue. The first test is a politically difficult one – we hope that it will be passed with success.

EDRi remains at your disposal for any support that we can give you in achieving your goals.

Thank you for your consideration of our views.

Yours sincerely,
Andreas Krisch

EDRi President

4 http://www.guardian.co.uk/business/2008/nov/09/child-porn-money-trials