THE SLIDE FROM "SELF-REGULATION" TO CORPORATE CENSORSHIP

THE SCALE AND SIGNIFICANCE OF MOVES TO ENTRUST INTERNET INTERMEDIARIES WITH A CORNERSTONE OF DEMOCRACY – OPEN ELECTRONIC COMMUNICATIONS NETWORKS

EXECUTIVE SUMMARY

Discussion Paper

Prepared by

Joe McNamee

EU Advocacy Coordinator

European Digital Rights

Rue Montoyer 39/9, B-1000 Brussels

E-Mail: joe.mcnamee@edri.org,

http://www.edri.org

01/2011

Introduction Self-regulation has traditionally been used in the Internet sector to permit companies in the fast-moving technology world to manage their networks efficiently in a way which gives flexible protection to their networks and protects consumers from problems like spam. Now, increasing coercion of Internet intermediaries to police and punish their own consumers is being implemented under the flag of "self-regulation" even though it is not regulation – it is policing – and it is not "self-" because it is their consumers and not themselves that are being policed.

Net neutrality and online policing
Large Internet access providers are requesting and, sometimes, demanding increased powers to interfere with traffic – to limit certain services or to demand payment from high-bandwidth services. Governments are demanding more voluntary measures from access providers in order to police the Internet for a variety of vested interests – blocking gambling websites to protect tax revenues and websites accused of facilitating intellectual property infringements, to protect media industries that have been unable to adapt to the digital age. This *quid pro quo* is made more interesting for access providers whose businesses are part of media groups or who have close cooperation with them. Two major European access providers are implementing highly invasive "deep packet inspection" technologies to fulfil their own and government demands.

Scale of demands Activities to encourage intermediaries to achieve various public policy initiatives exist at different levels: national (extra-judicial blocking of websites accused of containing illegal material), ad hoc international (the four-country -Netherlands with the UK, Germany and the Czech Republic -

GLOSSARY

Access provider

A company that provides connections to the Internet for individual consumers, organisations or companies.

Deep packet inspection

A technology which permits access providers to open each "packet" of Internet data sent or received on its network in order to assess where it is coming from, who it is going to and the nature of the file, if it is not encrypted.

Devolved enforcement

Where the state or public bodies devolve the responsibility for policing, judging and/or prosecuting alleged infringements of the law.

Hosting provider

A company which provides the facilities necessary to maintain a website or store other files on the Internet.

Internet hotline

A private or state facility which permits citizens to make (sometimes anonymous) reports of potentially illegal content and/or activities on the Internet.

Internet intermediary

This is a generic term referring to any company providing services on, or to connect to, the Internet.

IP address

Each device connected to the Internet has a unique number that allows it to communicate with other devices.

Net-minus effect

This is the term used in this paper to describe the situation where the limited action of a private company is used to deal with a problem which could be – and would be, without the involvement of the private company – more effectively and comprehensively dealt with by official public bodies. The net effect of the intervention by the private company is less than zero.

Newsgroup

This is a form of public noticeboard system.

Packet

Files sent over the Internet are split into "packets", to be assembled by the recipient computer.

Peer-to-peer

A technology which permits end-user computers to communicate directly with each other without relying on a single point of connection on the Internet. For example, Skype users find each other online using the Skype database, but then connect directly to each other, rather than using infrastructure provided by Skype.

initiative on illegal use of the Internet and ACTA), regional (various EU "self-regulation" dialogues with industry) and international (OSCE, OECD, CoE and UN).

Dangers The dangers of extra-judicial policing and punishment by private companies have not been assessed with regard to fundamental rights. Furthermore, they have not been assessed with regard to their effectiveness for fighting crime. There are already examples of punishments (such as website deletion) being used instead of real sanctions, even in cases of serious crimes such as child abuse – resulting in a "net-minus" effect. Ad hoc policing measures imposed by Internet intermediaries are resulting in less effective and less deterrent measures being taken by the state.

Conclusion A public debate is urgently needed in order to assess the scale of the policing measures being entrusted to Internet intermediaries, the cost for the rule of law and for fundamental rights as well as the cost for effective investigation and prosecution of serious crimes in the digital environment.

CONTENTS

INTRODUCTION

The largest and most developed Internet economies, including the European Union and the United States, are in the process of making a crucial and irreversible choice on the future of openness, democracy, transparency and innovation on the Internet. This choice is whether Internet intermediaries (access providers, website hosting companies, etc) should be allowed to manipulate Internet traffic for their own purposes or to police and punish the activities of their own consumers to achieve particular public policy goals. This decision is being made without any specific democratic policy decision or analysis of the consequences.

We are already reaching a "tipping point" in a gradual slide from the traditional sense of "self-regulation" (where intermediaries manage their own networks responsibly, as a more efficient approach than prescriptive legislation) to "devolved law enforcement", where, at the extreme, they become the police, judge, jury and executioner with regard to alleged infringements of either the law or of their own terms and conditions which may be stricter than the law.

Broadly speaking, online intermediaries have had little if any interest in adopting devolved law enforcement roles, but increasingly feel obliged to do so as a result of either government pressure or legal uncertainty created by weak or unclear legal protections ("safe harbours") offered to them in cases where their networks are used for illegal activities. For governments, the aim is obviously not to create a privatised police state. However, there is a general abandonment of the traditional concept of the rule of law and the role of the judiciary. The result is the "death by a thousand cuts" of traditional policing and judicial transparency. Each element of

Internet communication is being addressed in isolation with little coordination – leading to an overall detrimental effect. A list of such projects is included below in the section on devolved enforcement initiatives.

Some form of "cooperation" between Internet intermediaries for the achievement of public policy objectives has always been supported by the European Union (as in Article 16 of the E- Commerce Directive[1], for example). Now, however, a mixture of business interests and a conflation of the concepts of self-regulation, co-regulation and outsourcing of law enforcement to private companies have redefined this approach. This fundamental change in the concept of "self-regulation" represents a danger for the core values of the Internet and the benefits that these values provide to society.

The openness of the Internet enabled an avalanche of innovation over the past two decades. This innovation gave us services such as search engines, social networking, Internet telephony and digital libraries. It is also this openness that empowered citizens of oppressive regimes to distribute their message to the global public, to organise, to communicate and to build and develop democracy. This openness is now under threat.

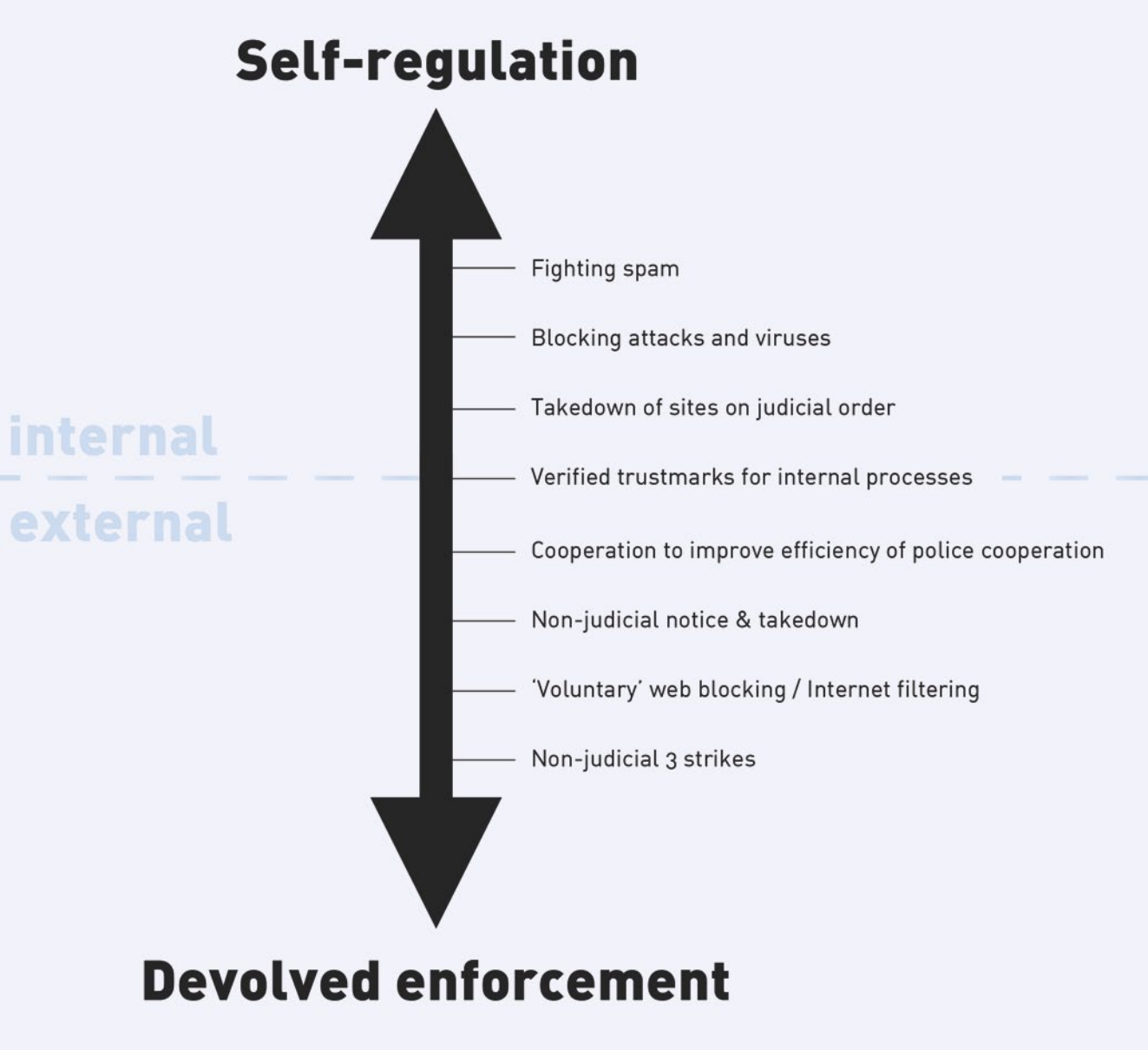
While the dangers to innovation (and the knock-on effects for the economy, for the take-up of Internet access and for investment) are very serious in their own right[2], this paper mainly addresses the fundamental rights aspects of the increasing interference of private companies in citizens' right to communicate. Very basic questions need to be asked about whether we should

"The openness of the Internet enabled an avalanche of innovation over the past two decades."

entrust enforcement of law in a core element of modern democracy – electronic communications – to private companies. More importantly, should we be entrusting this responsibility to an industry whose business priorities and technological capacities are changing rapidly and in unpredictable ways? Should we be entrusting private companies with the responsibility to undertake regulation of communication when they cannot reasonably be expected to provide the same level of impartiality, transparency and due process as traditional regulation of communications?

This paper looks at the growing role of delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of "self-regulation" or "cooperation". The first section provides an introduction to the experience of "self-regulation" and its slow slide from ISPs regulating their own systems (i.e. an entirely internal process) to the policing of customers based on data gathered outside their systems by third parties (i.e. an entirely external process which is, in fact, "devolved enforcement"). The second section then provides an introduction to the current market and technological developments which facilitate and encourage this slide and looks at some of the early examples of devolved regulation. The third section concludes with a brief overview of some of the fast-growing number of initiatives in this field.

In particular, this paper looks at the many unintended consequences that arise from governments taking the "easy" option



of abdicating responsibility for the achievement of public policy objectives by placing direct and indirect obligations on online intermediaries to police and regulate the Internet. It concludes by looking briefly at the flood of national and supra-national initiatives that are currently being discussed, which will have a profound impact on the openness, democracy and innovation that we have come to take for granted in the online environment.

This is a very brief overview of several key elements of this problem and describes the wide range of activities all currently understood under the broad concept of "self-regulation". The analysis demonstrates the changing roles of Internet intermediaries, provides case studies in enforcement measures undertaken by Internet intermediaries and summarises a non-exhaustive list of current international proposals to increase the enforcement activities of Internet intermediaries.

1 Directive 2000/31/EC of the European Parliament and of the Council, 8 June 2000.
2 See all responses to the European Commission consultation, including from Bits of Freedom/EDRi at: http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/net_neutrality/comments/index_en.htm

THE SLIDE FROM SELF-REGULATION TO VOLUNTARY POLICING

The concept of self-regulation is now being used in a way that extends far beyond its initial meaning to cover activities that are neither "self-" nor "regulation" but devolved enforcement, surveillance and extra-judicial punishment of allegedly illegal activities.

The European Union is pushing enthusiastically in favour of Internet "industry self-regulation"[3] without learning from the experience of the devolved enforcement initiatives that have been attempted in recent years. This experience has been subject to a range of detailed and cautionary industry, academic and civil society research. Part of the reason for this failure is that "cooperation" and "self-regulation" are used to describe activities which fall outside the scope of the normal definitions of these words. This leads to a lack of awareness among policy makers that successful "cooperation" in one field (the fight against unsolicited e-mail, for example) cannot be extrapolated to guarantee success in an entirely different one (policing of all consumers and punishing those found guilty by the online intermediary or by a third party of committing an offence, as suggested in one draft of the Anti-Counterfeiting Trade Agreement, for example)[4].

In most countries, an open and innovative Internet has been achieved in part by giving freedom from liability in clearly defined circumstances to Internet intermediaries that are in no way involved in the information they store or permit access to. However, there is now an increasing trend for Internet intermediaries to have investigative, monitoring, policing, judging and sanctioning powers delegated to them, occasionally through legislation but, far more frequently, by coercion or by weakening or redefining the protections that they have been able to avail of up until now. This activity is often mistakenly and misleadingly referred to as "self-regulation". However, it is obvious that intermediaries are not regulating themselves in these circumstances, they are regulating their consumers for the expected benefit of third parties.

The misnomer "self-regulation" stems from positive experience with Internet intermediaries undertaking real self-regulation in the past i.e. actively adapting internal functions for efficiency and/or for the benefit of their consumers. Even in this case, Internet intermediaries were often in favour of a regulatory underpinning[5]. Moving away from the

pure concept of "self-"regulation, some companies and associations also support or produce educational tools for Internet use – as a means of informing and enriching the experience of their users rather than "regulating" them[6]. Stepping a little further away from "self-"regulation and into the arena of deputised law enforcement support, Internet intermediaries are being asked, via "non-binding" guidelines, to establish procedures to maximise the efficiency of cooperation between themselves and law enforcement agencies.[7] Internet intermediaries have generally been very open to this kind of activity. This can improve efficiency of agreed, transparent, legal and uncontroversial procedures and does not inherently create fundamental rights problems – but they certainly create the potential and are also obviously outside the normal business activities of an intermediary.

These activities have now spread to a stage where they are entirely outside the dictionary definitions of the words "self-" and "regulation". This is a new environment where Internet intermediaries take it upon themselves (as a result of coercion by governments and/or vested interests and, occasionally, their own business interests) to police private online communications, often in blatant disregard of legal safeguards and even to impose sanctions for alleged infringements.[8] For example, the European Commission proposed an agreement[9] to be signed between intermediaries on extra-judicial deletion of websites accused by various sources of containing illegal information. Interestingly, as this proposal is not a formal Commission position, nor one

"these activities are not 'self-regulation', but law enforcement by private companies."

that would be signed by the Commission, the institution's entire internal decision-making process is circumvented by this approach. Similar initiatives are underway or agreed regarding, for example, blocking of websites by mobile operators, filtering of peer-to-peer traffic by access providers, blocking of consumers accused of involvement in the trade in counterfeit goods, protection of children in social networks.

These initiatives are being proposed even when this has no proven benefit and where they contradict the Commission's own legal assessments and legal undertakings.

Such extra-judicial activities can create real dangers for society, as Internet intermediaries remove symptoms of crimes, reducing pressure on state authorities to take real action against the criminals involved. Access providers in several European countries have been persuaded to voluntarily block lists of domains that have been deemed (often without judicial intervention) to contain child abuse material. This appears, for all concerned, to be little more than a public relations strategy, the analysis having been made by the European Commission in 2007 that blocking of websites is pointless because inter alia "when a website is successfully removed from a host server, it reappears very easily under another name[14]." It seems simply reckless for industry to engage in an activity whose consequences are so important when the costs and benefits have not been assessed.

The current stage in this evolution further away from the original concept of "self-regulation" is where the intermediaries' own consumers are increasingly being treated

Examples

The European Commission persuaded the mobile phone industry to establish an extra-judicial web blocking system, despite the fact that:

it correctly points out in the impact assessment to a proposal in 2007[10] that "[blocking] can only be imposed by law, subject to the principle of proportionality",

in 2008,[11] it concluded that "such measures must indeed be subject to law, or they are illegal",

the Commission signed a binding agreement stipulating that "self-regulation" "will not be applicable where fundamental rights or important political options are at stake" and recognised in 2007 that "the adoption of blocking measures necessarily implies a restriction of human rights"[12]

Indeed, not only have these contradictions not stopped the Commission from facilitating extra-judicial blocking, they have not even stopped the Commission from proposing and funding just such activities under the umbrella of "self-regulation"[13].

as "the enemy". Their Internet access is being increasingly blocked, logged, spied upon, restricted and subjected to sanctions imposed by the intermediaries, who fear legal liability for the actions of their clients. Measures undertaken for the identification and sanctioning of potentially illegal activity are generally (and unsurprisingly) unable to replicate the procedural fairness or protection for fundamental rights that are expected from a judicial process. As one could imagine, such privatised enforcement systems – because this is not the task of private businesses – do not prioritise freedom of expression or privacy. It is logical, therefore, that academic research is increasingly reaching the conclusion that "the democratising potential of the Internet is indeed being constrained by measures imposed in an attempt to control the perceived dangers posed by the medium."[15]

Trustmarks This paper does not in any way seek to address the issue of corporate social responsibility, trustmarks or externally verified undertakings to respect, for example, fundamental rights. Initiatives such as the Global Network Initiative[16] establish a set of principles by which member companies agree to limit their own operations in a way that ensures that certain principles are respected. On the continuum between self-regulation and devolved enforcement, externally verified trustmarks are on the border between both concepts. Where such an initiative seeks only to regulate and limit the activities of the company itself, it does not contain any of the key disadvantages of devolved regulation and should not, therefore, be confused with such activities.

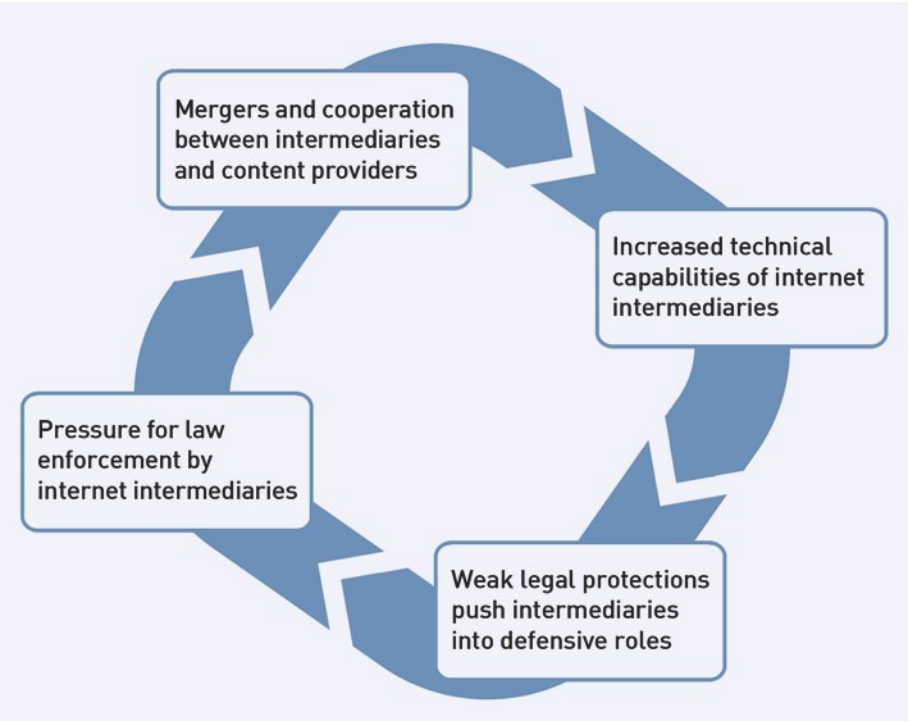
3 European Commission. "A Digital Agenda for Europe", p18
4 ACTA February 2010: footnote 6.
5 Richardson 2001.
6 Microsoft Corporation 2007.
7 Council of Europe Economic Crime Division, 2 April 2008.
8 Collins 2010.
9 http://www.edri.org/files/Draft_Recommendations.pdf
10 Proposal for a Council Framework Decision on combating terrorism. Impact Assessment, 2009, p29
11 Proposal for a Council Framework Decision on combating the sexual abuse, 2009. p38
12 Proposal for a Council Framework Decision on combating terrorism. Impact Assessment, 2009 p29
13 See, for example, the "COSPOL Internet Related Child Abusive Material Project" (www.circamp.eu)
14 See: Commission of the European Communities, 6 November 2006: 22.
Subsequently, in 2009, the Commission decided that it was a good idea to block websites anyway, even if it is ineffective.
15 Cooke 2007. Abstract
16 See http://www.globalnetworkinitiative.org (last visited 20 November) for more information.

DRIVERS FOR DEVOLVED REGULATION

We are at a particularly pivotal moment for the future of Internet freedoms as a result of three separate developments, all of which combined mean that the very character of the self-evidently democratic and open Internet is in question, with significant dangers for freedom of expression, innovation, competition and the rule of law. These developments are building on the long-standing pressure from law enforcement authorities and governments for intermediaries to become involved in policing activities

A: Weak legal protections are pushing Internet intermediaries into defensive policing roles. There are various measures being proposed and enacted (see below), which directly and indirectly place obligations on Internet intermediaries to "police" the Internet. Direct obligations are in the form of, for example, the French HADOPI law or the UK Digital Economy Act, which require or imply interference with consumers' personal data, blocking of online resources and cooperation with (or even complete responsibility

Weak legal protections are pushing Internet intermediaries into defensive policing roles



Increasing technical capabilities of Internet Access Providers

for) the implementation of sanctions. Indirect obligations can come from legal uncertainty or political pressure and lead to delegated enforcement where, as in the case of Eircom in Ireland, the company chooses to become police, judge, jury and executioner in relation to alleged infringements by consumers due to a fear of being held liable for such infringements. An increasing number of legal judgements (such as the 2007 Myspace and Dailymotion cases in France[17] and the Google/Vividown case in Italy[18]) continue to increase pressure for extra-judicial action by these private companies.

B: Increasing technical capabilities of Internet Access Providers

Internet Access Providers have traditionally been "mere conduits", who passively provide access to the Internet for their customers and have neither wanted to nor have been technologically able to interfere with communications. This suited governments, whose priority was to let the Internet develop and it suited businesses whose task was simply providing Internet access. Now that the Internet has grown hugely in developed countries and the business models of access providers are changing, the whole environment is different.

Internet Access Providers are increasingly able to exploit their growing ability to manage access to online resources. They are also increasingly motivated to do so, as the anticipated financial benefits of providing "non-neutral" access to the Internet become ever more tempting. If large access providers such as Telefonica[19] and Deutsche Telekom[20] are now calling for the right to interfere with their customers' data for commercial benefit, it follows that they will invest in technologies to make this happen. This process will be accelerated by "wire tapping"[21] and data retention[22] laws imposed by national and supranational organisations, which frequently require such interferences.

For the moment, more advanced interference remains somewhat expensive and complicated to implement. However, we are already seeing the first steps taken as this situation changes. For example, the Virgin Internet access provider in the UK has announced plans[23] to undertake "deep packet inspection" of 40% of its customers. We have also heard the demands of companies such as Telefonica and Deutsche Telekom who argue that they "need" to capitalise on their control of their own consumers, ostensibly to invest in faster networks. Deutsche Telekom's investment in its own VoIP service[24] while blocking the use of Skype[25] and Truphone[26] on its networks suggests motives of a more anti-competitive nature. Once these companies are interfering with communications for their own benefit and at the request of government, it is logical to assume the next step will be demands from every well-funded vested interest with a good public relations department to block, delete or investigate whatever subject is on the front page of the tabloid press from one week to the next[27].

C: Merging and/or cooperation of Internet access providers and media companies are creating incentives for more surveillance and interference with private communications In the past, Internet service providers were simply in the market of providing a range of Internet-related services such as Internet access, e-mail, website hosting, etc. These companies are increasingly involved in the provision of content services. An excellent example of this is Virgin Media. On the one hand, Virgin Media provides broadband Internet access while on the other, Virgin Media Entertainment provides audiovisual media content.

An access provider which is part of a group that contains a music or film company will undoubtedly be more motivated to undertake more proactive interference in their networks, particularly for the enforcement of intellectual property legislation. The devolved

Merging and/or cooperation of Internet access providers and media companies are creating incentives for more surveillance and interference with private communications

enforcement systems being proposed by government and the content industry thereby become (or at least appear to become) more economically advantageous.

Such companies have been required by law to gather personal data for law enforcement purposes (such as the EU Data Retention Directive, 2006/24/EC) and have been encouraged to retain additional data (such as browsing history) through voluntary agreements with governments.

In an environment where any large access provider is

- already paying for data collection measures such as retention of communications data
- already obscuring government inadequacy through the blocking of alleged child abuse material,
- already paying for technology such as deep packet inspection for "wire tapping" by the police and following its new (if adopted) obligations under the "Anti-Counterfeiting Trade Agreement" to promote "cooperation between service providers and rights holders",the companies have the means, the motive and the opportunity not only to interfere with the fundamental rights of their consumers by excessive policing of their networks when searching for possible intellectual property infringements (with government encouragement to do so), but also to block innovative new services to ensure that no "first mover advantage" can be gained if an online provider develops a compelling product. Such an environment is also ripe for abuse and corruption[28].

17 Edwards, 2007
18 D'Alessandro, 2010
19 Daly 2010.
20 Schneibel, Farivar 2010.
21 Geere 2010.
22 Directive 2006/24/EC of the European Parliament and of the Council, 15 March 2006.
23 Williams 2009.
24 Gonzalez 2008.
25 Gardner 2009.
26 Ray 2007.
27 Flynn 2010.
28 Spiegel Online 2008.

DEVOLVED ENFORCEMENT - MISTAKES MADE BUT NO LESSONS LEARNT

Experience of devolved regulation activities is not being assessed by governments in order to avoid past mistakes and to ensure adequate respect for democratic principles and the rule of law.

Almost from the beginnings of the Internet, governments and law enforcement authorities have – deliberately or unintentionally – misunderstood the concept of ("self-") regulation and have presented Internet service providers a choice between "hard" regulation or "soft" "self-" regulation. In the "self-regulation" that is, in fact, devolved law enforcement responsibility, it is not the Internet intermediary that is regulating itself, it is the intermediary regulating the behaviour of its consumers on behalf of various unrelated stakeholders. The absence of a democratic and public decision-making process and transparency regarding how this enforcement is undertaken leads to situations where private companies and their priorities establish which aspects of the law are enforced, how they are enforced and what sanctions are imposed in the event that a private company considers that a given action is illegal.

CASE #1

Internet blocking in the UK

Case Study 1: Internet blocking in the UK In the mid 1990s, the fact that illegal content was available online led to "knee-jerk" reactions in the press, among law enforcement authorities and among politicians. Public perception is often used to coerce Internet providers to "self-"regulate. The London Metropolitan Police chief inspector took it upon himself to send an open letter to all UK ISPs demanding that they monitor, identify and take "necessary action" against newsgroups containing allegedly illegal material[29]. It should be pointed out that, as newsgroups are public forums, any newsgroup can contain illegal material at any given moment. This gentle arm-twisting was accompanied with the threat that this would the necessity "to move to an enforcement strategy".

Subsequently, the UK hotline, which has now become the Internet Watch Foundation (IWF), was established. This non-judicial body, after receiving reports from the general pubic, makes an extra-judicial ruling on what is illegal and what is not. When sites hosted in the UK are deemed to be illegal, Internet providers remove them and reports are given to the police. Keith Mitchell, head of the London Internet Exchange at the time, is quoted as saying that "[a]t first, the Home Office just seemed to be glad this problem was being taken care of for them."[30] This was the first hint of a major and entirely ignored problem of the "net-minus effect" associated with this devolved enforcement approach. It is a clear example of where essentially cosmetic measures (blocking or, somewhat better, deletion of the sites) replace effective law enforcement investigation of the crimes depicted on the sites, reducing overall effectiveness of the fight against the illegal content in question.

In 2004, the IWF introduced a "blacklist" of "potentially illegal"[31] foreign websites that it puts at the disposal of the UK Home Office, which it passes to Internet access providers.

The risks and disadvantages of this system are very clear:

- Lack of transparency
- Lack of judicial oversight
- Mission creep: (The IWF now covers "violent pornography" (depictions of legal activity))[32] and the Digital Economy Act now provides a legal framework to require Internet access providers to block websites judged to facilitate breaches of intellectual

property rights.

- Mistakes: Known problems include the technical disruption of both the Wikipedia[33] and the Internet archive site called "the Wayback Machine"[34]. As the sites are always abroad and Internet users are presented with a "not found" error message, there is no way of guessing how many mistakes are made involving smaller sites.

- Abuse: Richard Clayton has shown how some blocking mechanisms could be used as an "oracle"[35] to discover the locations of substantial amounts of abuse material, turning a system for combating child abuse into one that would actively facilitate it.

- Net-minus effect: Six months after the first blacklist was produced, the UK Home Office Minister Bill Rammell was asked in a parliamentary question which countries he had had discussions with to request the removal of child pornography websites and how many such request were agreed upon. The response was that "no such requests have been made by the Foreign and Commonwealth Office" [36].

On the other hand, the possible benefits that could be used to justify these costs have never been clearly assessed:

- Is the blacklist meant to stop accidental access, deliberate access, both or neither?

- What evidence exists that any of the assumed benefits are, in fact, achieved through the implementation of the blocking system?

"the presumed benefits of this system have never been measured against the known costs"

- How does the evolution of statistics on complaints to the IWF compare with complaints to analogous hotlines in countries where blocking is not undertaken?

- As illegal sites are rapidly and increasingly moving their location and using hacked servers (and the IWF produces statistics to confirm this) and both phenomena significantly reduce the possible usefulness of blocking, at what stage will the negative impacts of blocking outweigh the diminishing benefits?

The problem is, of course, that nobody has both the interest and the resources to ask these questions. The British government is happy with a system where it can show activity in this important policy area without necessarily having to devote significant resources to the problem. Similarly, the ISPs that have signed up to the system get good publicity without having to invest significantly in terms of either time or money.

One could almost be forgiven for forgetting that the websites depict real and horrific crimes against children, for forgetting that this policy is removing pressure for those children to be identified and rescued, removing pressure to have the criminals behind the sites brought to justice, for forgetting that the "blocked" sites remain online and accessible to anyone who wants to see them in Britain and without restriction for any Internet user who wants to see them around the world.

It is ironic to note, however, that, for all of its shortcomings and the lack of analysis of its impact, the blocking system facilitated and promoted by the IWF is probably the

least bad of all similar initiatives. The system most widely used in the UK is far more targeted than in other countries, resulting in fewer legal resources being blocked. In addition, the list is updated more frequently in the UK than in other countries, increasing the likelihood that some currently active illegal sites are on the list. That said, the proportion of static websites that are not hosted in hacked servers or free web hosting sites is getting smaller and smaller, making blocking an increasingly pointless endeavour.

The overall negative impact of this blocking system has generally been static since it was established. Now, however, new technological developments, the trend towards devolved enforcement and the expansion of such schemes internationally gives it a whole new meaning:

- The use of deep packet inspection by Virgin Media to check for potential intellectual property infringements will inevitably lead to demands for this technology to be used for other purposes. Having implemented the technology for its own perceived business interests, it will have few legitimate excuses not to use it to attempt to fight intellectual property infringements, alleged child abuse material and any other material deemed unacceptable either by the British government or the media. This technology is hugely invasive and damaging for fundamental rights and risks being implemented on a wide scale "voluntarily" before a proper democratic analysis of its acceptability can be undertaken.

- Legally mandated requirements for more invasive/efficient blocking technologies will oblige Internet access providers to develop the capability for provision of "non-neutral" access (where the access provider can block specific services if they are in competition with their own, such as Internet telephony, or can demand payment for better access to its customers from competing third party services such as search engines or online video services). It is difficult to imagine that access providers, having invested in the technology ostensibly for the benefit of society – and in an environment where they are expected to interfere with communications for the benefit of others - will not exploit it for its own commercial advantage – to the detriment of choice, freedom of expression, innovation and competition in the online environment.

The European Commission has now proposed the introduction of EU-wide Internet blocking, without having done a thorough impact assessment, without identifying the goals of this blocking, without assessing the impact of blocking in those countries that have implemented it so far and having deliberately changed a previous version of the legislation with the specific intention of facilitating a "self-regulatory" approach – despite this being in clear breach of the Inter-Institutional Agreement reached in the EU in 2003.

A response to a Parliamentary question on the evidence for blocking suggests that the Commission's preparatory work may not have been as thorough as one would expect. Commissioner Malmström explained, after reasserting her support for "evidence-based decision-making" that there are some general positive developments and that these "**give an indication** that, to a **certain extent** and **at least partly**, this may follow also from action taken, **including** action to block access to websites in some countries[37]." (emphasis added)

CASE
#2

Notice and Takedown

Case study 2: Notice and Takedown

The incentives for hosting providers (companies that "host" websites on behalf of customers) to either delete or leave websites online after receiving complaints are extremely important. If hosting providers feel legally more secure to delete websites that are the subject of complaints, this will lead (and has led) to privatised censorship and extra-judicial punishments meted out by private companies based on business interests. As more and more communications happen online, on social networks, for example, failure to ensure an adequate balance will result in restrictions on freedom of expression.

In a small-scale study, Ahlert, Marsden and Yung[38] compared the responses of one British and one American Internet hosting provider, upon receipt of an invalid takedown request from a non-existent organisation. The British and American hosting providers work in very different legal environments:

US: The US legal framework provides a patchwork of legal protections for Internet intermediaries, depending on the type of illegal activity in question. Despite being more complex[39], it appears that the overall impact is to provide greater legal certainty than the EU framework. With regard to intellectual property, the United States has a distinct "notice and takedown" regime specific for intellectual property infringements created by the Digital Millennium Copyright Act. This provides protection for hosting providers that host unauthorised copyrighted material, on condition that they react to complaints that must follow a clearly defined structure. When the prescribed procedure has been followed, the hosting provider must delete the website (based on the simple fact that a complaint has been made). This deletion takes place in the absence of a judicial order. The Electronic Frontier Foundation[40] in particular has been critical of the chilling effect on free speech which is created by the deletion of content in the absence of a judicial ruling.

EU: In the European Union, the environment is far less clear. Hosting providers will not be held liable in cases where they unknowingly host illegal material, provided they act in an (undefined) expeditious way after having received (undefined) actual knowledge of the infringement. Whether "actual knowledge" refers to knowledge of the

allegedly infringing material or actual knowledge of the illegality of the material is unclear, as is what authority or authorities would be considered competent to provide the "actual" knowledge. Ten years after the adoption of the legislation, for example, it is not clear whether in practice or in law a notification or formal legal order for removal of the website would be considered adequate.

In the USA, in response to the incorrect notification from the non-existent organisation claiming ownership of the public domain material in question, the US hosting provider sent information to the complainant explaining the procedures that needed to be followed and that the website could only be taken down "under penalty of perjury" if the complainant provided inaccurate information. The website was not deleted at this stage and the researchers decided not to pursue the complaint any further.

In the EU (a UK provider was used), the website was deleted the day after the bogus complaint was made.

While this sample is quite clearly very limited, the hosting providers in both cases reacted in the way that appears most conducive to their commercial interest – i.e. both took what seemed to be the least costly and most legally secure option. Furthermore, the arbitrary and censorious approach based on the E-Commerce Directive was duplicated in research undertaken by Dutch EDRi member Bits of Freedom in 2004. In that research, three free ISPs, three paid access providers, three hosting providers and one cable provider were selected. A viciously allegorical text was uploaded from the famous author Multatuli (Eduard Douwes Dekker). The text tells the story of a flock of sheep who chase away a tyrant, only to find themselves in need of specialists to represent them and, in the end, inviting the same tyrant back in the guise of a "Specialist". The text on the website clearly stated in the opening line that the work dates from 1871, and was reprinted in 1981. Obviously invalid complaints were made using an invented name and a Hotmail e-mail address. As a result of the complaint:

"Innocent websites are frequently deleted due to legal uncertainty"

- Tiscali (access provider) deleted the website, referring to its terms and conditions and without giving the uploader of the site full details of the complaints.
- Access provider Wanadoo contacted the consumer, giving 24 hours to remove the website, without sharing the full complaint. Ten days after the initial complaint and after receiving a second one, the website was deleted.
- Hosting provider Yourhosting assumed the accuracy of the complaint, called and e-mailed the uploader of the website and removed the website within three hours of receiving the initial complaint.
- Hosting provider LaDot/Active24, upon receiving a second complaint (having lost the first one) gave the uploader of the site 28 hours to remove the website or provide evidence of permission to upload the material (which contained a prominent statement that it was public domain). After three days, the website was deleted.
- Hosting provider iFast sent full personal data (including irrelevant data such as date of birth) of the uploader of the website to the complainant. After the complainant insisted that iFast take action, they complied and deleted the website the next day.

- Access providers Planet Internet and Demon responded to the complaints by asking for specific further information and indemnification. However, in response to a filled out questionnaire containing fake personal details and no additional relevant information, they gave the uploader of the website 48 hours to delete it.

- Three providers did not respond to the bogus complaint – XS4All, Freeler and UPC.

The research comes to the stark conclusion that it only takes a Hotmail account to bring a website down, and freedom of speech stands no chance in the face of a devolved enforcement structure based on commercial imperatives rather than anything resembling due process.

The European Commission appears far from perturbed by the dangers for fundamental rights of this approach and appears keen to export the approach through ACTA (the Anti-Counterfeiting Trade Agreement) which aims to reduce legal certainty of Internet intermediaries and incentivise them to engage in such vigilante justice. It is also promoting non-judicial methods for deletion of websites in the DG HOME Dialogue on public-private cooperation to counter the dissemination of illegal content in the European Union.

29 Davies 2009.
30 Idem
31 Idem
32 It should be recognised that these types of content remain very exceptional in the IWF's work, but they are nonetheless examples of mission creep.
33 Metz 2008.
34 Metz 2009.
35 Clayton, 2005, p9
36 United Kingdom Parliament, 14 December 2004.
37 Response to parliamentary question E-7865/2010. **http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2010-7865&language=EN** (last consulted 20 November 2010)
38 Ahlert, Marsden, Yung 2002.
39 Lemy, 2007
40 Electronic Frontier Foundation 2010.

CURRENT DEVOLVED ENFORCEMENT INITIATIVES

In the interest of an informed public debate, which is not yet happening, it is crucial to appreciate the scale of devolved regulation initiatives in the EU and globally.

Current EU initiatives It is important to note that "cooperation" / "self-regulation" agreements orchestrated, encouraged and drafted by the European Commission are not only free from the democratic scrutiny of traditional legislative measures, they are also not subject to the approval of the European Commission itself. Individual units of the Commission take the initiative (often on the basis of non-specific statements adopted in documents of the other EU institutions) to invite industry representatives to meetings and, under the unspoken or unofficial assumption that a voluntary agreement is the only alternative to strict regulation, draft industry agreements[41] are proposed and negotiated. As the Commission is not formally a party to the agreement, there is no process whereby the unit responsible is subject to any internal scrutiny.

This creates the unfortunate situation which the unit responsible has all of the power of the European Commission behind it, but none of the responsibility.

It is also worth remembering the final text of the Telecom Package adopted in 2009 by the European Institutions:

Article 1.3a. of the revised Framework Directive

Any of these measures regarding **end-user's access to or use of services** and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may **only** be imposed if they are appropriate, proportionate and necessary within a democratic society, **and their implementation shall be subject to adequate procedural safeguards** in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, **including effective judicial protection and due process**. (emphasis added)

Further safeguards are clear from the 2003 Interinstitutional Agreement:

> The Commission will ensure that any use of co-regulation or self-regulation is always consistent with Community law and that it meets the criteria of transparency (in particular the publicising of agreements) and representativeness of the parties involved. It must also represent added value for the general interest. **These mechanisms will not be applicable where fundamental rights or important political options are at stake.** (emphasis added)

#1 DG Internal Market

Dialogue on illegal uploading and downloading

Aim: To encourage self-regulatory filtering/ surveillance of peer-to-peer networks

In 2009, the European Commission Directorate General for Internal Market and Services established a working group involving Internet access providers and the content (music and film) industry, in order to explore ways in which access providers could undertake measures to police their networks and punish possible infringements. Items discussed include surveillance of peer-to-peer networks involving the unauthorised collection and the processing of personally identifiable data and the further use of this data to identify, contact and, possibly, sanction consumers accused of unauthorised use of copyrighted material.

Due to what it considered the anti-consumer bias of the discussions, the European Consumer Bureau (BEUC) chose not to participate. For the first year of operation of the initiative, data protection representatives were actively prohibited from participating. Now that the process has developed to a stage at which the unit responsible deems appropriate, data protection bodies are permitted to take part.

#2 DG HOME

Dialogue on public-private cooperation to counter the dissemination of illegal content in the European Union

Aim: To encourage Internet hosting providers to delete websites on the basis of accusations of illegality

Also in 2009, the European Commission's Directorate General for Justice, Liberty and Security (the relevant unit is now part of the DG for Home Affairs) launched a dialogue with Internet hosting providers in order to agree on a code of conduct for dealing with allegations of illegal websites being hosted in the European Union (initially restricted to sites containing alleged child abuse, racism or terrorism). The European Commission's original proposal[44] was for hosting providers to unquestioningly and indefinitely delete websites that were accused of being illegal by bodies "authorised or tasked under national law to monitor Internet content" and to delete websites that they (the hosting provider) felt were illegal if they received a complaint from a member of the public. Child abuse hotlines report that approximately 75% of calls refer to sites that were not, in fact, illegal. As a result, one can reasonably assume that up to three quarters of sites deleted based on the intermediary's own assessment would be sites that were legal.

Strangely, for a document ostensibly about creating a framework for "public-private partnership", the document makes no proposals for actions on the part of public authorities other than making extra-judicial rulings of illegality. There is no suggestion that public authorities should undertake prosecutions or investigations or take any other action that citizens in a society based on the rule of law would assume to be self-evident in cases of material that is of such a serious nature. This raises yet again the serious danger of a net-minus effect, which has not been assessed in any detail in this context.

Furthermore, this initiative wholly ignores the conclusion of the European Commission-funded "Rightswatch" project in 2001 on precisely this subject, which concluded that "any self-regulatory regime within the context of NTD[45] procedures cannot be truly effective without some form of legislative underpinning"[46]. If a legislative underpinning is needed for restrictions in the area of economic interests, it appears self-evident that this need is all the greater in relation to serious crimes against individuals, whether child abuse or terrorism.

#3 DG HOME

Project creating the "Financial Coalition against Child Pornography"

Aim: To recruit financial services companies to undertake proactive policing activities online

In the United States, a coalition of financial services companies, together with a small number of Internet service providers, have worked together with the National Center for Missing and Exploited Children since 2006 to investigate commercial child abuse websites and shut down any revenue streams they were receiving. This initiative was set up as a result of inaction on the part of government authorities and receives no public funding.

This apparent[47] success of the US Financial Coalition prompted the European Commission to bring together stakeholders to try to achieve the same impact. However, it invited a far wider range of organisations – mainly Internet Service Providers and child rights organisations – which are unrelated to the problem that the European Commission was trying to solve. At the end of a one-year pilot project, the EU financial coalition has produced no results, despite having received substantial funding from the European Commission. It has, however, produced a report on the scale of the problem[48], which was urgently needed, bearing in mind that the Commission launched a proposal for a Directive on Child Exploitation[49] without having carried out such research. The report shows that many of the assumptions on which the Commission based Internet-related elements of that Directive are inaccurate.

#4 DG Internal Market

Dialogue on "sale of counterfeit goods on the Internet"

Aim: To encourage private companies to identify, disrupt and punish activities of alleged sellers of counterfeit goods online

In 2009, the European Commission Directorate General for the Internal Market and Services also launched a dialogue with online service providers in order to create a "memorandum of understanding" between online companies that trade or facilitate trade in goods and services online. In the current[42] draft text, rights owners commit to inform Internet Platforms about who they believe to be repeat infringers and commit to provide feedback to Internet Platforms on the effectiveness of their schemes regarding repeat infringers (e.g. if rights owners feel that there has been a failure to take measures against a repeat infringer) with online platforms committing to "**to ensure that valid [i.e. following the agreed procedure] notifications of Offers of Counterfeit Goods lead to a swift removal or disabling of the notified Offer (take-down) and to take deterrent measures in relation to such sellers**"[43]. As is typical in such agreements, none of the parties will have a particular interest in demanding that the transparency obligation would be enforced, while the rights holder will clearly have a business interest in demanding that the extra-judicial sanctions are implemented as comprehensively as possible. "Obligations" for transparency, etc, in such agreements are therefore of very little practical value.

Update: The process has now been completed. The final text is available from:
http://ec.europa.eu/internal_market/iprenforcement/docs/memorandum_04052011_en.pdf

#5 DG HOME

Funding for "self-regulatory" Internet blocking

Aim: To persuade ISPs to limit access to online resources accused of being illegal

In June, 2010, the European Commission launched a funding proposal in relation to "illegal use of the Internet" which includes a proposal for "facilitating the taking down of illegal Internet content through public-private cooperation or blocking access to child pornography or blocking the access to illegal Internet content through public-private cooperation"[50]. Despite the fact that a legislative process is underway to decide whether Internet blocking should be introduced for the purpose of restricting access to child abuse material, the European Commission has made it clear that it will incentivise the development of projects to block "illegal" (it is worth noting that "illegal" in the context of the DG HOME exercise on "public-private cooperation to counter the dissemination of illegal content in the European Union" described above means "accused of being illegal.") sites in general.

This initiative appears to breach Article 17 of the Interinstitutional Agreement, the European Commission's assessment of the legal context, as described in the impact assessment on the Child Exploitation Directive[51] and the public statements of the Commissioner responsible who, contrary to the broad aims of this funding proposal, promised that she would "personally strongly oppose" any suggestion that blocking be extended beyond child abuse material[52].

#6 DG Information Society

Social networking principles

Aim: To create a safer environment for children using social networking

The European Commission DG Information Society proposed and had adopted a set of principles by various providers of social network services in 2009[53]. Some of the principles overlap measures proposed elsewhere (such as "community reports" of allegedly inappropriate behaviour) while some establish questionable standards on privacy. Very little effort is made to ensure due process when the social networking provider acts to, for example, delete an account or delete content in cases of "community" reports – reinforcing the lack of data protection and acceptance of unilateral punishments/sanctions being imposed by the service provider.

Principle 6 establishes that "providers should provide a range of privacy setting options with supporting information," which is, in fact, a standard for all data collection. The text adopted only goes as far as long-standing Article 29 Working Group recommendations[54] and, by raising these as a special case for children, suggests that default protections are lower than they actually are. Furthermore, the guidelines fail to provide extra protection – such as age appropriate information display – to the minors using the services in question.

The implementation of these principles are now being reviewed by the Commission.

INTERNATIONAL "SELF-REGULATORY" INITIATIVES

In addition to the sample list of current international activities identified below, it is worth noting that the scale of the move towards "self-regulation" has been recognised and encouraged by international organisations such as the United Nations. For example, the Tunis Agenda for the Information Society[55] called for "self-regulatory and other effective policies and frameworks to protect children and young people from abuse and exploitation through ICTs into national plans of action and e-strategies." In this context, it could be argued that the biggest problem is the failure to properly implement the UN Child Rights Convention and its Optional Protocol (not mentioned in the Agenda) by states. On the other hand interventions by intermediaries in this field have generally been cosmetic (such as web blocking), inadequately addressing the crimes being perpetuated.

#7 Council of Europe

"Reflection" on the legal status of certain stakeholders with regard to compliance

Aim: To open discussions on how Internet intermediaries can take part in policing of private communications

The Council of Europe has traditionally maintained a positive position with regard to self-regulation. In particular, its work focused on real self-regulation, where providers managed their own networks to the benefit of their own consumers. Recommendation R(2001)8[56], for example, established guidelines on the use of content descriptors, content selection tools, hotlines and user information and awareness. This was reinforced by the "Declaration on freedom of communication on the Internet"[57] which made the clear statement that the Assembly was "convinced also that it is necessary to limit the liability of service providers when they act as mere transmitters" and restated its opposition to prior state control of data.

However, in 2010, the Parliamentary Assembly took a very different view[58], arguing that the Committee of Ministers should initiate reflection on the legal status of Internet intermediaries (specifying access providers and search engines as examples) with regard to compliance. This approach is contrary both to the letter and the spirit of the 2003 Declaration on freedom of communication on the Internet, as the intention appears to be to increase the legal obligations of intermediaries. Consequently, the text by the Parliamentary Assembly brings with it a danger for the fundamental rights that the Council of Europe seeks to protect. In particular, increased legal uncertainty will push intermediaries into "self-regulatory" policing tasks, while the European Convention on Human Rights explicitly requires interferences with private life or communications to have a legal basis.

#8 OECD

The role of Internet intermediaries in advancing public policy objectives

Aim: A broad initiative to establish ways in which Internet intermediaries can receive devolved responsibilities to implement public policy objectives

As part of wider deliberations on the role of Internet intermediaries, the OECD organised a conference in Paris in June 2010 to discuss the role of Internet intermediaries in advancing "public policy objectives". The three main topics discussed at the event were cybersecurity, the protection of consumers from fraud by Internet service providers and the role of Internet intermediaries in protecting intellectual property rights.

The framing of the debate on intellectual property is worth noting. The first question on the agenda was "do ISPs have a role?" and the second question, assuming an affirmative answer to that question, asked what are the "respective roles of technological or market innovation, awareness-building, and notice regimes? What particular issues are raised by notice regimes that entail a sanction?"

The preliminary draft text from the OECD raises some profound questions about the role of Internet intermediaries in policing content which they have little commercial reason to be aware of. Additionally, it explores the extent to which they should be involved in not only policing the Internet but also interfering with consumers' communications, encouraging a role in preventing infringements. The preliminary

conclusions from the OECD[59] ask to what extent should Internet intermediaries be responsible for this content, or inversely, how far should responsibility remain with the original content author or provider? If the intermediary is deemed even partially responsible for the dissemination of the content or how it is being used, what requirements should be imposed on the intermediary to remove this content, or perhaps even to prevent it being made available in the first place? In defence of the OECD, it should be pointed out that they are consulting and researching these questions rather than simply imposing obligations directly or through indirect coercion. However the scale of the project and the size of the economic interests involved means that the balance of the discussions is far from optimal.

#9 OSCE

The role of the Internet industry in dealing with hate speech on the Internet

Aim: To find ways of using Internet service providers to regulate legal or illegal "hate speech" online

In May 2010, the OSCE and its Office for Democratic Institutions and Human Rights held a consultation meeting on the role of the Internet industry with regard to online hate speech[60]. Based on the meeting report, the participants were broadly sensitive to fundamental rights. Nonetheless, the question of what Internet intermediaries would be prepared to do inevitably arose. In particular, the meeting summary suggests that "experience shows that the approach taken by some Internet companies to remove hate-inciting material on the basis of breaches of their terms of service agreements is much more effective than using the criminal justice system to identify **and prosecute** the authors of such material". (emphasis added)

The analysis suggests that obtaining judicial rulings would be too difficult and, therefore, the most appropriate sanction for the owner of a hate-speech website would be the deletion of the site, on the basis of an extra-judicial ruling by the Internet intermediary hosting the site. The cost in terms of fundamental rights and the rule of law of demanding that such powers be used by private companies appears disproportionate to the achievement of the imposition of an exceptionally limited sanction – namely, creating the inconvenience for the site owner of uploading his/her site to a new server.

Another example given as "best practice" is the "robust and efficient" system implemented by a social networking site called Hyves in the Netherlands. Ten complaints from different sources (different IP addresses) is sufficient to have a resource removed from the service, at least temporarily. This approach creates a secondary danger of "mob justice" as well as the possibility of comparatively small-scale campaigns being used to remove sites/blogs/social network pages of political opponents.

AD HOC INTERNATIONAL MEASURES AIMED AT "SELF-REGULATION"

#10

Anti Counterfeiting Trade Agreement (ACTA)

Aim: "To provide an improved framework for countries committed to intellectual property protection".

The Anti-Counterfeiting Trade Agreement (ACTA) is a draft plurilaterial agreement, ostensibly to address large-scale trade in counterfeit goods. Despite its stated purpose, the draft agreement also contains provisions on Internet service provider liability. If we accept the European Commission's assertion that the purpose of ACTA is "to more effectively combat trade in counterfeit and pirated goods," then the only purpose of the ISP liability provisions would be to aid in achieving this goal. Following on from this, the only way that ISP liability could achieve this goal is by ensuring that they are incentivised or coerced into both policing their networks and enforcing extra-judicial sanctions, where they deem it to be appropriate. Proof that this is the intent behind the provisions on ISP liability can be seen from the leak that appeared in March 2010:

> *Footnote 29: An example of such a policy is providing for the termination in appropriate circumstances of subscriptions [US: and] [AU: or] accounts on the service provider's system or network of repeat infringers*[61].

This approach is mirrored in the July 2010 leak[62], which contains the proposal in chapter 4, article 2.18, section 3 quarter:

> *"the development of mutually supportive relationships between online service providers and right holders to deal effectively with patent, industrial design, trademark and copyright or relater [sic] rights infringement which takes place by means of the Internet, including the encouragement of establishing guidelines for the actions which should be taken".*

The almost final version (at time of writing) now contains in its preamble a reference to **"desiring"** to promote cooperation between service providers and rights holders with respect to relevant infringements in the digital environment, and an obligation on parties to "promote cooperative efforts within the business community to effectively address **at least trademark and copyright or related rights infringement** while preserving legitimate competition and consistent with each Party's law, preserving fundamental principles such as freedom of expression, fair process, and privacy" (emphasis added). As all parties will believe that their law with regard to freedom of expression, due process and privacy are adequate, they will clearly not be moved to improve it as a result of ACTA. It is therefore difficult to see any practical value in these safeguards.

#11 EU/Korea & EU/India

Aim: Small but important change to the EU acquis on intermediary liability.

The European Union is currently working on bilateral free trade agreements with various partners around the world. The EU/Korea deal[63] is awaiting signature while the EU/India agreement is currently under discussion. Both the published EU/Korea deal and the leaked draft EU/India deal[64] share one interesting characteristic. Both texts copy almost the entire text of the E-Commerce Directive (2000/31/EC) with regard to the liability of online intermediaries and both leave out the same short but crucial piece of text. While both texts explain that limitations on liability are only available for intermediaries that are "in no way involved" in the information they transmit, they both fail to include the crucial explanation that this does not cover manipulations of a purely technical nature. Omitting the same text twice in two different trade agreements leads one to believe that the European Commission is undermining the legal certainty of intermediaries. In a policy briefing prepared by the services of the European Parliament on the EU/Korea deal, this issue was not mentioned, indicating the lack of political visibility of ISP liability in this context.[65].

#12

Four-country initiative on "illegal use of the Internet"

Aim: To find new ways of policing of the Internet by Internet intermediaries

The Netherlands, supported by the Czech Republic, Germany and Great Britain, is in the process of preparing the next step in a project involving public authorities and ISPs in order to ensure more efficient policing of their networks by Internet intermediaries. The gap which the previous stage in the project claims to have identified in existing practice is that the E-Commerce Directive does not regulate in concrete steps how to act in case of illegal use of the Internet and does not define in which way "public and private parties can shoulder their common responsibility to keep the Internet clean from criminal and terrorist activities"[66]. While the project focuses on terrorism, the project also considers the ISPs' involvement in creating a "cleaner Internet" that would be equally useful in relation to other forms of cybercrime or abuse, like fraud, illegal trade and sexual exploitation of children.

The project does not start with a particular problem to solve, but rather from the perspective that Internet access providers **could** be pro-actively policing their networks. The next planned steps are to address the scope of the proactive policing measures foreseen and to identify such measures in individual countries within and outside the group of four countries to establish if and how they can be exported.

41 For an example of such a draft text proposed by the European Commission see: http://www.edri.org/files/Draft_Recommendations.pdf
42 July 2010
43 Unpublished draft agreement
44 United Kingdom Parliament, 14 December 2004.
45 Notice and takedown
46 Williams 2009: p26
47 Statistics produced by the Coalition indicates success in disrupting the trade in child abuse material. However, the possible "net-minus effect", where this action could have reduced pressure on state authorities to prosecute the criminals and identify the abused children, has never been analysed or acknowledged.
48 European Financial Coalition 2010.
49 Proposal Repealing Framework Decision 2004/68/JHA, 29 March 2010.
50 European Commission 2010.
51 Proposal Repealing Framework Decision 2004/68/JHA, 29 March 2010.
52 Commissioner Malmström 2010.
53 "Safer Social Networking Principles for the EU" 2009.
54 See, for example, Article 29 – Data Protection Working Party 2000.
55 Tunis Agenda for the Information Society, Paragraph 40p, last visited 8 November 2010 http://www.itu.int/wsis/docs2/tunis/off/6rev1.html
56 Council of Europe 2001.
57 Committee of Ministers 2003.
58 Committee on Culture, Science and Education 2010.
59 http://www.oecd.org/dataoecd/18/44/46013181.pdf - last visited 24 January, 2011
60 Report of OSCE-ODIHR Meeting 2010.
61 Consolidated Text: ACTA, January 2010.
62 Consolidated Text: ACTA, July 2010.
63 See: http://trade.ec.europa.eu/doclib/press/index.cfm?id=443&serie=273&langId=en
64 European Commission, 24 February 2010.
65 See http://www.europarl.europa.eu/meetdocs/2009_2014/documents/inta/dv/792/792791/792791en.pdf
66 Project plan made available to the author, but not yet published.

THE IMPACT OF "VOLUNTARY SELF-REGULATION" ON LEGAL CONTENT

While some content may be objectionable for any number of reasons, it is inappropriate and dangerous for democracy if the actions of private companies result in legal material being effectively banned.

An NGO service provider disappears – child abuse sites go ignored

An innovative online intermediary based in Malaysia and the USA was providing a variety of services to non-governmental organisations. To offer the NGOs maximum protection, it rented server space provided by a major European Internet access provider. In early 2010, it launched a new service, where people could create very short web addresses, for use on Twitter and similar social networking outlets/ sites.

Shortly afterwards, all of its services stopped working, with no warning. Subsequently, the European service provider alleged (based on unspecified information) that some of the shortened addresses had been used to link to (unspecified) child abuse websites. Despite the seriousness of the crimes in question, at no stage were law enforcement authorities involved, or asked to be involved, in the case.

The intermediary was provided with the list of shortened addresses that were being blamed but, as the server no longer functioned, it had no way of:

- verifying that the accusations were genuine or
- collecting the evidence that might have been useful for law enforcement authorities to investigate the crimes in question.

Even when the online intermediary offered to provide more detailed data preservation for law enforcement purposes, the offer was refused. Some time later, when the data was of significantly less potential use, the service provider asked for the IP addresses used to set up the links to the child abuse websites but, even then, there was no indication that this information would be passed on to the appropriate authorities. The outcome of the devolved enforcement powers exercised by the European intermediary was therefore:

a. The removal of all of the online service provider's legal services from the Internet, including all of the NGO services that were in no way involved with the accusations.

b. The exclusion of law enforcement authorities from an incident allegedly involving serious crimes against children.

The owner of the service in this section asked that specific details of the intermediary and his own identity not be included to avoid the risk that his Internet connection would be cut again.

An NGO service provider disappears - child abuse sites go ignored

The Yahoo! Nazi memorabilia case In 2000, a French court ruled[67] that Nazi memorabilia being sold through Yahoo! in the United States was a breach of French law, as the Yahoo! website was accessible in France. As a result, the court ruled that Yahoo! (USA) had to render it impossible for French Internet users to access the offending page, while Yahoo! (France) had to remove all links to the US site and insert warnings concerning the illegal content on the US page. The French judge was prepared to accept a success rate of about 80% (based on expert advice) for a blocking system based on IP address data.

Yahoo! then had to work out how to deal with a situation where Yahoo! France would have to remove links to its US counterpart, warn its own customers about "illegal material"

The Yahoo! Nazi memorabilia case

hosted by its own parent company and invest in a blocking system which would not work for 20% of Internet users – nor for anyone who actually wanted to access the offending pages. It therefore took the decision to ban the memorabilia, which was perfectly legal in the United States, for all of its websites globally. As has become typical in such cases, it then did its best to make a virtue out of being coerced to limit access to legal material. Yahoo! argued that "it does not want to profit from items that glorified or promote hatred[68]."

Facebook – the Sarah Palin takedown

Facebook – the Sarah Palin takedown

Companies such as Facebook come under intense pressure in relation to individual incidents that attract the interest of politicians and/or the press. These create strong pressure for private companies to regulate their clients in order to prevent possibly illegal activities (and this will be exacerbated by any weakening of the intermediary liability regimes), it also creates pressure to regulate any activity that creates a liability or public relations risk for the company.

Intermediaries design their terms and conditions in order to prepare for exactly such an eventuality. For example, Facebook, in section 5.2 of its Terms and Conditions gives itself the right to delete any content or information that it "believes" is in contravention. For the moment, this appears to have created a system where Facebook employees have the courage to stand up to political and media pressure[69] in some cases, while its automated systems are somewhat less robust. These automated processes, whereby a piece of information is "flagged" by a certain (often small) number of users, are easy to exploit, particularly in a political environment. In Sarah Palin's case, one blogger appears to have concerted activities among his readers to report a particular (contentious but not illegal) statement and cause it to be automatically taken offline[70]. While the robust stands taken in the face of sometimes huge media pressure by Facebook in the past must be recognised, this policy position may change. On the other hand, the automated deletion of pages, as in Sarah Palin's case, shows the dangers for the right to communication.

67 All relevant documents are available from: http://www.juriscom.net/txt/jurisfr/cti/tgiparis20000522.htm
68 Salis 2001.
69 "Facebook Defies David Cameron and Keeps Moat Tribute Page" 2010.
70 Ries 2010.

CONCLUSION

There is unquestionably a huge volume of initiatives on a national, regional and international level that seek to change the nature of the relationship between Internet intermediaries and their consumers. The purpose of all of these initiatives is to create, as the OECD puts it, an increased role for these intermediaries in the achievement of "public policy objectives."

It is also clear that technological and market developments since the beginning of the last decade (when the current intermediary liability regime was created) have led both to increasing legal uncertainty and increased incentives for intermediaries to become more involved in the data that they enable access to, in order to provide "non-neutral" access to the Internet.

Interested third parties, such as intellectual property owners, who find it understandably easier to focus their efforts on a comparatively small number of intermediaries rather than a larger number of individual infringers, have lobbied for courts and governments to look again at such intermediary liability, in order to encourage policing of the Internet by these private companies. Similarly, some governments see it as easier and quicker to coerce online intermediaries into carrying out policing (and prevention) duties rather than devoting scarce public resources to this purpose.

Despite a wealth of academic research showing the dangers of this approach for transparency and fundamental rights, governments and regional organisations such as the European Union appear to treat delegated law enforcement (commonly referred to as "self-regulation" in order to borrow the positive connotations that this has in relation to projects where the intermediaries are actually regulating themselves) as an unquestioned good. Governments appear to see no need to identify and learn the lessons of the past, no need to ensure adequate legal underpinning (even when its own research indicates that this is necessary[71]) and no need to take any account of, or plan for, market and technological developments – developments which are radically changing the priorities of the intermediaries. As a result, due process,

freedom of expression and the democratic nature of the Internet itself is now in grave and increasing danger.

As a consequence of these market and political developments, while there has been a degree of law- based regulation in the digital environment, we have now reached a stage in the development of the Internet where essentially every aspect of our online activity is subject to regulation by private companies, based on and motivated by – in various proportions at various moments - public relations concerns, business priorities, threats of strict regulatory interventions and worries about civil and even criminal liability. Governments are freely, and probably definitively, surrendering political and judicial power and placing it in the hands of an industry which is changing rapidly and whose technical capacities are changing incessantly. This presents a major threat to democracy and the concept of the rule of law. At every turn, citizens' fundamental right to freedom of communication is under threat.

Finally, a stage has been reached where a veritable "censorship ecosystem" is foreseen. Internet access providers have been coerced in several European countries into the blocking of entire domain names (such as www.example.com). Promoted and funded by the European Commission, the CIRCAMP project uses the threat of the blocking of entire domains as a way of encouraging domain owners to police their systems to ensure that their domain remains "clean". CIRCAMP explains that it believes that "this will motivate content providers on the Internet to actively make an effort to avoid files with child sexual abuse on their systems/services"[74] - of course it may also motivate them to ensure that anything liable to be mistaken for being illegal will also be removed. This approach was adopted in the absence of any evidence suggesting that such an approach was needed.

It is arresting that a move of such importance to society has so far been carried out with very little analysis about the long term consequences of this strategy and without a clear democratic decision indicating that this is genuinely in the best interest of society.

71 Nas 2004.
72 A method of imposing detailed surveillance and filtering of Internet traffic http://en.wikipedia.org/wiki/Deep_packet_inspection
73 "Ryanair Wins Ihateryanair.co.uk Because of £322 Ad Revenue" 2010.
74 CIRCAMP 2010.

Examples

#1
Access to the Internet is threatened by growing calls for Internet access providers to disconnect users based on accusations from third parties.

#2
The ability to communicate privately is under threat by the "voluntary" or self-interested use of surveillance such as deep packet inspection[72].

#3
The ability to upload a website or blog is threatened by terms and conditions of hosting providers and "codes of conduct" whereby sites can be deleted without judicial orders.

#4
The ability to sell products online is threatened by "self-regulatory" measures both to have sales blocked and allegedly "repeat offenders" prevented from using online platforms.

#5
The ability to have a domain name for one's personal or business purposes is threatened by overly broad terms and conditions of domain name registries.[73]

BIBLIOGRAPHY

ACTA. "Article 2.7: Enforcement Procedures in the Digital Environment." Feb. 2010. Last visited 5 November, 2010
http://sites.google.com/site/actadigitalchapter/acta_digital_chapter.pdf

Alhert, C., C. Marsden, and C. Yung. "How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation." (2002): 1-39. Print

Article 29 Working Party. Privacy on the Internet - An Integrated EU Approach to On-line Data Protection – Working Document. 21 Nov. 2000. Last visited. 3 Nov. 2010
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2000/wp37en.pdf.

Bits of Freedom, and EDRi. Publication. 30 Sept. 2010. Last visited. 3 Nov. 2010.
http://www.edri.org/docs/netneutralityreaction300910.pdf.

CIRCAMP: Cospol Internet Related Child Abusive Material Project. Last visited. 3 Nov. 2010.
http://www.circamp.eu/.

"CIRCAMP Overview." CIRCAMP. Last visited. 03 Nov. 2010.
http://circamp.eu/index.php?option=com_content&view=article&id=11:circamp-overview&catid=1:project&Itemid=2

Clayton, Richard, "Failures in a hybrid content blocking system" in Privacy Enhancing Technologies" pages 78-92, 2005.
Available online at http://www.cl.cam.ac.uk/~rnc1/cleanfeed.pdf. Last visited 20 November 2010.

Collins, John. "Eircom to Cut Broadband over Illegal Downloads - The Irish Times - Mon, May 24, 2010." The Irish Times. 24 May 2010. Last visited. 03 Nov. 2010.

http://www.irishtimes.com/newspaper/frontpage/2010/0524/1224271013389.html.

Commission of the European Communities. Commission Staff Working Document.

Accompanying Document to the Proposal for a Council Framework Decision Amending Framework Decision 2002/475/JHA on Combating Terrorism. 6 Nov. 2007. Last visited 3 Nov. 2010.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2007:1424:FIN:EN:PDF.

Commission of the European Communities. Commission Staff Working Document. Proposal for a Council Framework Decision on Combating the Sexual Abuse , Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA, Impact Assessment,SEC(2009) 355. 25 Mar. 2009. Last visited 3 Nov. 2010.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0355:FIN:EN:PDF

Commissioner Malmström. "Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography: the Commission's Proposed Directive." Speech. ENACSO Conference. 6 May 2010. 6 May 2010. Last visited Nov. 2010.
http://ec.europa.eu/commission_2010-2014/malmstrom/archive/Speech%20%20Malmstrom%20-%20Combating%20sexual%20abuse%2006_05_2010.pdf

Committe on Culture, Science and Education. "Rethinking Creative Rights for the Internet Age." Council of Europe Parliamentary Assembly (PACE Web Site). 7 Jan. 2010. Last visited 03 Nov. 2010.
http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc10/EDOC12101.htm

Committee of Ministers. "Declaration on Freedom of Communication on the Internet (Adopted by the Committee of Ministers on 28 May 2003 at the 840th Meeting of the Ministers' Deputies)."Council of Europe. 28 May 2003. Last visited 03 Nov. 2010.
https://wcd.coe.int/ViewDoc.jsp?id=37031

Consolidated Text: Anti-Counterfeiting Trade Agreement. 1 July 2010. Last visited 3 Nov. 2010.
http://www.laquadrature.net/files/ACTA_consolidatedtext_EUrestricted130710.pdf

Consolidated Text: Anti-Counterfeiting Trade Agreement. 18 Jan. 2010. Last visited 3 Nov. 2010.
http://www.laquadrature.net/files/201001_acta.pdf.

Cooke, Louise. "Controlling the Net: European Approaches to Content and Access Regulation." Journal of Information Science 33.3 (2007): 360-76. Print.

Council of Europe. "Reconmmendation No. R (2001) 8 of the Committee of Ministers to Member States on Self-Regulation Concerning Cyber Content (Self-regulation and User Protection against Illegal or Harmful Content on New Communications and Information Services)."Council of Europe. 5 Sept. 2001. Last visited 03 Nov. 2010.
https://wcd.coe.int/wcd/ViewDoc.jsp?id=220387&Site=CM

Council of Europe Economic Crime Division. Directorate General of Human Rights and Legal Affairs. Guidelines for the Cooperation between Law Enforcement and Internet Service Providers against Cybercrime. 2 Apr. 2008. Last visited 3 Nov. 2010. http://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/cy_activity_interface2008/567_prov-d-guidelines_provisional2_3april2008_en.pdf

D'Allessandro, Manuela, "Google Executives convicted for Italy autism video", Reuters, 24 February 2010. Last visited 20 November 2010 http://www.reuters.com/article/idUSTRE61N2G520100224

Daly, John W. "Telefonica Wants Google and You to Pay at Both Ends - CEO Wants Money, Not Net Neutrality." TechEye. 8 Feb. 2010. Last visited 03 Nov. 2010. http://www.techeye.net/Internet/telefonica-wants-google-and-you-to-pay-at-both-ends.

Davies, C. J. "The Hidden Censors of the Internet." Wired.co.uk. 20 May 2009. Last visited 03 Nov. 2010. http://www.wired.co.uk/wired-magazine/archive/2009/05/features/the-hidden-censors-of-the-Internet

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market ('Directive on Electronic Commerce'). Vol. L178 17/07/2000. London: S.n., 2000. Print. P. 0001 – 0016.

Edwards, L, "Web 2.0 liability hits Europe - delete those borrowed cartoons fast, folks", October 31, 2007. Last visited 20 November, 2010, http://blogscript.blogspot.com/2007/10/web-20-liability-hits-europe-delete.html

"EU-Korea Free Trade Agreement Online." European Commission - Trade. 6 Oct. 2010. Last visited 03 Nov. 2010. http://trade.ec.europa.eu/doclib/press/index.cfm?id=443&serie=273&langId=en

European Commission. "A Digital Agenda for Europe." 19 May 2010. Last visited 3 Nov. 2010. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

European Commission. Directorate General for Trade. EU-India FTA Negotiations: Latest Texts on Goods, SPS and IPR. 24 Feb. 2010. Last visited 3 Nov. 2010. http://file.wikileaks.info/leak/eu-india-fta-feb-2009.pdf

European Commission. Directorate-General Justice, Freedom and Security. Programme "Prevention of and Fight against Crime": Targeted Call for Proposals "Illegal Use of the Internet" Action Grants 2010. 2010. Last visited 3 Nov. 2010. http://ec.europa.eu/home-affairs/funding/isec/call_10132/tc2_call_2010_en.pdf

European Commission. Draft Recommendations for Public Private Cooperation to Counter the Dissemination of Illegal Content within the European Union. Last visited Nov. 2010. http://www.edri.org/files/Draft_Recommendations.pdf

European Financial Coalition 2010. 14 Months On: a Combined Report from the European Financial Coalition 2009-2010: An Intelligence Assessment on the Commercial Distribution of Child Sexual Abuse Images. 2010. Last visited 3 Nov. 2010.
http://ebookpedia.net/14-months-on--A-combined-report-from-the-European-Financial-Coalition.html

European Parliament and Council. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC. 15 Mar. 2006. Last visited 3 Nov. 2010.
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT

"Facebook Defies David Cameron and Keeps Moat Tribute Page." Telegraph.co.uk. 14 July 2010. Last visited 03 Nov. 2010.
http://www.telegraph.co.uk/technology/facebook/7891206/Facebook-defies-David-Cameron-and-keeps-Moat-tribute-page.html

Flynn, Pat. "Fears over Cliffs of Moher Facebook Photos." Independent.ie. 5 Aug. 2010. Web. 03 Nov. 2010.
http://www.independent.ie/national-news/fears-over-cliffs-of-moher-facebook-photos-2284767.html
"French-German-Russian Summit: Sarkozy Dreams of a European Security Council."

SPIEGEL ONLINE International. 18 Oct. 2010. Last visited 03 Nov. 2010.
http://www.spiegel.de/international/europe/0,1518,723664,00.html

Gardner, W. David. "Deutsche Telekom Restricts Skype On IPhone." InformationWeek. 2 Apr. 2009. Last visited 3 Nov. 2010.
http://www.informationweek.com/news/personal-tech/smart-phones/216402527

Geere, Duncan. "Coalition Quietly Revives UK Web Surveillance Plans." Wired.co.uk. 21 Oct. 2010. Last visited 03 Nov. 2010.
http://www.wired.co.uk/news/archive/2010-10/21/coalition-quietly-revives-web-surveillance-plans

Gonzales, Nick. "Jajah Announces Deutsche Telekom As Second Series C Investor." TechCrunch. 28 May 2007. Last visited 03 Nov. 2010.
http://techcrunch.com/2007/05/28/jajah-announces-deutsche-telekom-as-second-series-c-investor

Karaganis, Joe. "Piracy and Jobs in Europe: Why the BASCAP/TERA Approach Is Wrong." Social Science Research Council. Mar. 2010. Last visited 3 Nov. 2010.
http://blogs.ssrc.org/datadrip/wp-content/uploads/2010/03/Piracy-and-Jobs-in-Europe-An-SSRC-Note-on-Methods.pdf

Leyden, John, "Anti-piracy lawyers' e-mail database leaked after hack", 27 September 2010. 6 Nov. 2010. Last visited 8 November, 2010
http://www.theregister.co.uk/2010/09/27/anti_piracy_lawyer_email_leak/

Lemy, Mark. A, "Rationalising Internet Safe Harbors", 1 April 2007, Stanford Public Law Working Paper, No. 979836 (2007) Last visited 8 November. Draft available at:
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=979836

Metz, Cade. "IWF Confirms Wayback Machine Porn Blacklisting." The Register. 14 Jan. 2009. Last visited 03 Nov. 2010.
http://www.theregister.co.uk/2009/01/14/iwf_details_archive_blacklisting

Metz, Cade. "IWF Pulls Wikipedia from Child Porn Blacklist." The Register. 10 Dec. 2008. Last visited 03 Nov. 2010.
http://www.theregister.co.uk/2008/12/10/iwf_reverses_wikiban

Microsoft Corporation. Play Smart, Play Safe! A Family Guide to Video Gaming. Microsoft Corporation, 2007. Last visited 3 Nov. 2010.
http://www.euroispa.org/files/video_gaming.pdf

"Proposal for a Directive on Combating Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/JHA." EUROPA. 29 Mar. 2010. Last visited 03 Nov. 2010.
http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/10/107

Ray, Bill. "T-Mobile Terminates Truphone." The Register. 18 June 2007. Last visited 03 Nov. 2010.
http://www.theregister.co.uk/2007/06/18/t_mobile_truphone

Report of OSCE-ODIHR Expert Meeting: Role of Internet Industry in Addressing Hate on the Internet. Rep. 10 May 2010. Last visited 3 Nov. 2010.
http://www.osce.org/odihr/68743

Richardson, Tim. "Europe Warms to Spam Ban." The Register. 11 Jan. 2001. Last visited 03 Nov. 2010.
http://www.theregister.co.uk/2001/01/11/europe_warms_to_spam_ban/

Ries, Brian. "Palin's Facebook Ground Zero Mosque Post: How It Disappeared." The Daily Beast. 23 July 2010. Last visited 03 Nov. 2010.
http://www.thedailybeast.com/blogs-and-stories/2010-07-23/palins-facebook-ground-zero-mosque-post-how-it-disappeared/

"Ryanair Wins Ihateryanair.co.uk Because of £322 Ad Revenue." OUT-LAW.COM. 2010. Last visited 03 Nov. 2010.
http://www.out-law.com/page-11446

Safer Social Networking Principles for the EU. Publication. 10 Feb. 2009. Last visited 3 Nov. 2010.
http://ec.europa.eu/information_society/activities/social_networking/docs/sn_principles.pdf

Salis, Richard. "A Look at How U.S Based Yahoo! Was Condemned by French Law." Juriscom.net. 10 Nov. 2000. Last visited 03 Nov. 2010.
http://www.juriscom.net/txt/jurisfr/cti/yauctions.htm

Schneibel, Gerhard, and Cyrus Farivar. "Deutsche Telekom Moves against Apple, Google and NetNeutrality." Deutsche Welle. 7 Apr. 2010. Last visited 03 Nov. 2010.
http://www.dw-world.de/dw/article/0,,5439525,00.html

Moore, Tyler, and Richard Clayton. "The Impact of Incentives on Notice and Takedown." Proc. of Seventh Workshop on the Economics of Information Security (WEIS 2008). 22 June 2008. Last visited 3 Nov. 2010.
http://www.cl.cam.ac.uk/~rnc1/takedown.pdf

Tera Consultants. Building a Digital Economy: The Importance of Saving Jobs in the EU's Creative Industries. Rep. Mar. 2010. Last visited 3 Nov. 2010.
http://www.iccwbo.org/uploadedFiles/BASCAP/Pages/Building%20a%20Digital%20Economy%20-%20TERA%281%29.pdf

"Unintended Consequences: Twelve Years under the DMCA." Electronic Frontier Foundation. Last visited 2010. Web. 03 Nov. 2010.
http://www.eff.org/wp/unintended-consequences-under-dmca

"United Kingdom Parliament, Hansard (Verbatim Report)." www.parliament.uk. 14 Dec. 2004. Last visited 03 Nov. 2010.
http://www.publications.parliament.uk/pa/cm200405/cmhansrd/vo041214/text/41214w21.htm

Williams, Chris. "Virgin Media to Trial Filesharing Monitoring System." The Register. 26 Nov. 2009. Last visited 03 Nov. 2010.
http://www.theregister.co.uk/2009/11/26/virgin_media_detica

Brown, Ian, "Internet Self-regulation and fundamental rights", Index on Censorship, Vol 1, March 2010
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1539942

With financial support from the EU's Fundamental Rights and Citizenship Programme.