# How 'Liberty' Disappeared from Cyberspace:
# The Mystery Shopper Tests Internet Content Self-Regulation

Christian Ahlert, Chris Marsden and Chester Yung

**Table of Contents**

Introduction ..... 2
Internet Industry and the Role of ISPs ..... 3
Liability for Harmful and Potentially Illegal Content on the Internet ..... 5
Overview of the Notice and Takedown (NTD) procedure ..... 7
Legal provisions of NTD in the US and EU ..... 8
ISP Codes of Conduct and Notice and Takedown ..... 12
ISP Market and Regulatory Cost-Benefits ..... 13
How Much NTD Activity? Results of a Questionnaire Survey in the Netherlands ..... 15
The Mystery Shopper Test ..... 17
Objectives ..... 17
Design and schedule ..... 17
Result of the pilot experiment: US ISP ..... 19
US Conclusion ..... 23
UK Test ..... 24
Preliminary Conclusion: US vs UK ..... 26
Policy Conclusions ..... 27
References ..... 29
Appendix I—Questionnaire on Notice and Take Down Procedure ..... 31
Appendix II—Overview several ISPs in the UK ..... 34
Thus-plc-Demon Internet ..... 34
Freeserve.com ..... 35
AOL Europe ..... 36
POPTEL ..... 37
Which? Online ..... 38
Fastnet International ..... 38
Yahoo!UK ..... 39

***Introduction***

The internet represents an immense challenge for established forms of content control, which cannot be met, by common understanding, via the traditional, by and large national, legal system. It is argued that courts are to slow to respond efficiently and effectively to the millions of copyright infringements, harmful and racist websites occurring on the net. Governments have been pressured by copyright holders and mounting concerns regarding the protection of minors from harmful content, child porn and other worries about abuse of the Internet. In practice, "single points of content control" have been identified, which are increasingly used to remove content from the internet. Governments, companies, and increasingly individuals, have realized: publishing, posting and propagating content on the internet needs the services of an Internet Service Provider (ISP). They make access to the internet possible and they provide hosting for most of the content available on the World Wide Web, and have been identified in the Internet's communication chain as best suited to removing illegal and harmful materials from the Internet.[1] Consequently the regulation of content has been delegated to ISPs. This response to the architecture of the Internet has given rise to a strategy available to an ISP: so called *notice and takedown procedures*.. Both in the US and Europe the rationale of governments, seem to be similar. Though this may be termed self-regulation, we suggest using the term 'delegated self-regulation' as it more appropriately describes that the state has imposed genuine powers on private actors. Nas describes the European situation: "Through the E-Commerce Directive governments have forced liability on ISPs (…), hidden under a black veil of 'self-regulation'."[2]

This paper represents the results of a research project on Notice and Take Down attempting to shed light on the "reality" of content self-regulation by Internet Service Providers in general and in particular on differences between the US and the EC legal framework in this area. Under Notice and Takedown (NTD) regimes Internet Service Providers have the duty to remove illegal and harmful content from the internet once they are made aware that their servers host it. The quantity of complains and websites removed under NTD is unknown, and the process by which ISPs determine whether or not a website contains illegal or harmful content remains obscure, raising questions of accountability, transparency and the overall appropriateness of delegating content regulation to private actors under a self-regulatory framework; as in principle this could be seen as a privatization of censorship. However, the consequences are much clearer: once an ISP disables access to a website the content disappears from the internet, which is effectively a form of censorship. The question we then posed was quite simply: How does NTD actually work?

[1] See Zittrain, Jonathan (2003): "Internet Points of Control". The Berkman Center for Internet & Society: http://cyber.law.harvard.edu/publications

[2] Nas, Sjoera (2003) Spread the Word. OSCE p. 165

To investigate how ISPs make use of NTD we developed a method we term in this paper the "Mystery Shopper". We made a complaint to an ISP about alleged copyright infringement on a website we had previously uploaded, which contained perfectly legal material:

- The identity of the person who uploaded the site is disguised[3] and we made use of free website services of major ISPs.
- We uploaded one site with a very prominent US ISP and one with a major UK based ISP.
- Both displayed parts of a chapter of John Stuart Mill's "On Liberty"[4]; for symbolic reasons we selected chapter two in which Mill discusses freedom of the press and the dangers of censorship.
- This content is clearly public domain, as it was published in 1869, and does not constitute any form of copyright infringement.

Result:

- The US ISP followed up on the dubious complaint with detailed questions;
- The UK ISP took the site down almost immediately effectively censoring (JS Mill "On Liberty") legal content without investigation.

.This experiment, whilst it in no way can claim to be representative of all ISP's practices, does offer a clear window on NTD procedure in practice and the scope for abuse and a lack of due diligence.

In addition to making experimental complaints, we collaborated with the Dutch ISP Association (ISPA NL) to conduct a survey on NTD. Our experience was sobering from the point of view of transparency and accountability of the NTD regime. We might expect that minimal standards of openness might be observed, but even though the ISPs were contacted by their industry association to investigate the current NTD regime, ISPs provided only meagre feedback, which raises questions about the effectiveness of the ISP association itself Despite the lack of data, , we could deduce that ISPs with many private customers get a huge number of complaints, whereas ISPs with business customers do not get many. Nevertheless this seems to be a result in itself: industry is neither willing to discuss NTD, nor to provide insightful data on it. Hence, self-regulation in this area, which can have drastic consequences for freedom of speech, is neither transparent nor, subsequently, sufficiently accountable.

### *Internet Industry and the Role of ISPs*

Noam has shown that consolidation in the Internet industry increased in the U.S. from about 1996, though most sectors remain competitive[5]. He examines eight sub-sectors:

[3] We complained on behalf of the chairman of the non-existent John Stuart Mill Heritage Foundation.

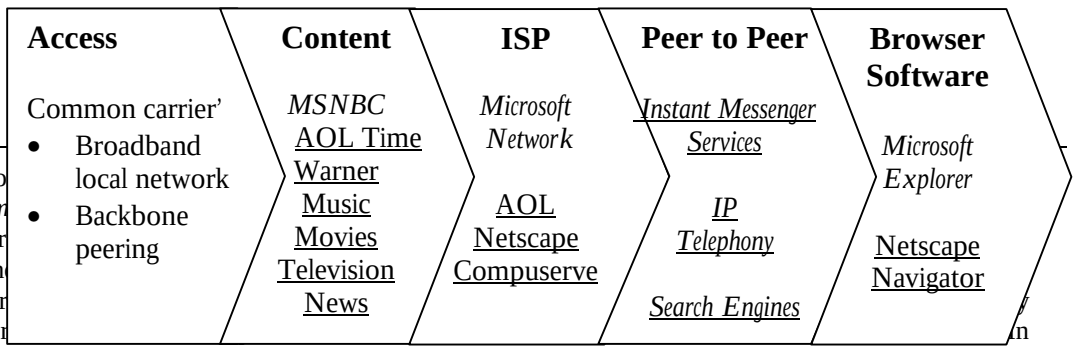
[4] The authors would like to thank Christian Sandvig for the idea of using JS Mill's 'On Liberty' for this project. In addition we want to thank Ola-Kristian Hoff, Wendy Seltzer and Woiter Diephous for their help.

- Internet backbones, which connect the global Internet;
- Internet service providers (ISPs);
- broadband access providers, providing high-speed access in the local loop;
- portals which aggregate content and functions as a 'home page' for users;
- browser software such as Microsoft Explorer or Netscape Navigator;
- search engines, such as Google or Altavista;
- media-player software, such as RealPlayer or Windows Media; and
- Internet Protocol (IP) telephony.

He explains that "common elements are high economies of scale (scalability) based on the high fixed costs and low marginal costs, and the way they are often complemented on the demand side by network effects (which economists call 'positive externalities')." Representing the value chain diagrammatically:

- Network encompasses **broadband providers and backbone providers**, such as UUNet;
- ICP (Internet Content Producer) encompasses **portal** (though often integrated into ISP functions), **search engine**;
- **IP telephony**, Instant Messaging, and the two most common **browsers**, Netscape and Internet Explorer, are owned by two large ICPs, AOL and MSN respectively[6];
- The two largest **media player** companies are integrated into ICP conglomerates (Windows Media, Real Networks);

**ISPs** provide the actual connectivity to the end-user. ISPs are integrated with content services and access suppliers. Most large ISPs provide a default home page 'portal', with news, features, search facility. The largest ISPs are subsidiaries of either access providers (local cable or telephone companies) or software companies such as Microsoft and AOL-Netscape-Compuserve (though note the new strategy of the latter in the broadband environment). Below, the italics illustrate Microsoft products and services, the underlined items belong to AOL Time Warner, and those offered by both conglomerates are italicized and underlined.




[5] No
*Com*
instr
[6] Th
inter
Inter
contrast to both IAPs and ISPs, Internet Content Providers provide their own proprietary content, often in addition to Internet access. See Yen. A. (2000) *Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment* 88 Georgetown L.J. At http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID236478_code000726304.pdf?abstractid=236478

Often, ISPs are joint venture partners with content or access providers, such as BT Yahoo! (UK) or Yahoo! Softbank (Japan), or AOL Deutschland (formerly a Bertelsmann joint venture). Both Microsoft and AOL are also content providers, own search engines, have Instant Messenger services. All European access providers and US cable companies provide proprietary Internet services for their customers, making AOL and Microsoft unusual ISPs in that their content-software focus has prevented their leveraging their ISP dominance into access. In broadband markets, those ISPs who also control access include T-Online, Wanadoo in France, Telefonica, BT Yahoo! Though other ISPs can access the local loop at wholesale prices, competitors fear that the regulated access price leaves them disadvantaged.

Public access, through work, government institution, cybercafe or school, and the device itself, are not included in Noam's list; but the filtering software that end-users and these intermediaries rely on is integrated into such software as search engines, media players, portals and especially browser software. Filtering software is now compulsory in libraries in the US[7] and schools in France[8], amongst other places – where the state can control public access to illegal and harmful content, it does so.

### *Liability for Harmful and Potentially Illegal Content on the Internet*

Communication through the Internet requires the passive reproduction and distribution of material. ISPs automatically reproduce and distribute material to subscriber requests. Content creators upload to web pages by instructing the ISP's computer to store a copy of the uploaded material. The ISP's computer also makes copies of the material every time a computer asks to view the subscriber's web page and sends those copies through the Internet. That file does not travel directly to the user. Instead, it generally goes through other computers hooked up to the Internet. Each of these computers makes at least a partial copy of the relevant file. As Yen has described, "a practically unlimited scope of liability soon follows."[9] In order that these nodes on

[7] *Child's Internet Protection Act 2003*, building on the *Communications Decency Act 1996*.
[8] Reuters (March 18 2004) *Central Filter Against Web Hate for French Schools* at http://www.reuters.com/newsArticle.jhtml;?storyID=4599516
[9] President Clinton's 1995 Copyright Taskforce supported such liability: *Working Group On Intellectual Property Rights, Information Infrastructure Task Force, Intellectual Property And The National Information Infrastructure* 1-6, 114-24 (1995).

the network between content provider and end-user are not all held strictly liable[10] for the billions of web files they continually copy in the act of transmission, legislators in the US and European Union have held that only a limited liability holds for these intermediaries, typically ISPs[11]. In the US, liability regimes have differed according to speech-based and copyright-based liabilities.The Communications Decency Act of 1996 provides that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider[12]. Yen states: "the general philosophy motivating these decisions—namely, that the liability against ISPs for subscriber libel would result in undesirable censorship on the Internet—remains vitally important in assessing the desirability of ISP liability." Holznagel has indicated that US courts have applied these 'safe harbour' provisions to widely protect ISPs, even where [a] it was aware of unlawful hosted content; [b] it had been notified of this by a third party; [c] it had paid for the data[13]. Frydman and Rorive observe that courts "in line with the legislative intent…applied the immunity provision in an extensive manner"[14].

In Europe, 'safe harbour' protection of ISPs from liability was implemented on 17 January 2002, when the E-Commerce Directive came into force. Article 12 protects the ISP where it provides 'mere conduit' with no knowledge of, nor editorial control over, content or receiver ("does not initiate [or] select the receiver"). Benoit and Frydman establish that it was based on the 1997 German Teleservices Act, though with "slightly more burden on the ISPs in comparison with the former German statute"[15]. Where ISPs provide hosting services, under Article 14 they are protected from liability, in two ways:

> [a] the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity is apparent; or
>
> [b] the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disrupt access of the information.

---

[10] Some legal commentators forcefully argued that strict liability should apply. See Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1042-46 (1994) (advocating strict ISP liability); Kelly Tickle, *Comment, The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards*, 80 IOWA L. REV. 391, 416 (1995) (favoring limited ISP liability).

[11] See, for example, Niva Elkin-Koren, *Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators*, 13 CARDOZO ARTS & ENT. L.J. 345, 399-410 (1995), who argues opposing liability.

[12] Section 30, 47 U.S.C. § 230(c)(1) (Supp. II 1996). This language might shield ISPs from liability for subscriber copyright infringement as well. However, Section 230(e)(2) specifically states, "Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property."

[13] Holznagel, B. (2000) *Responsibility for Harmful and Illegal Content as Well as Free Speech on the Internet in the United States of America and Germany*, in C.Engel and H. Keller (eds) *Governance of Global Networks in Light of Differing Local Values*, Nomos, Baden Baden.

[14] Frydman, B. and Rorive, I. (2002) *Regulating Internet Content Through Intermediaries in Europe and the USA*, Zeitschrift fur Rechtssoziologie Bd.23/H1, July 2002, Lucius et Lucius.

[15] Ibid at 54.

Like the proverbial 'three wise monkeys', ISPs, IAPs, and web hosting services should 'hear no evil, see no evil, speak no evil'. As mere ciphers for content, they are protected; should they engage in any filtering of content they become liable. Thus masterly inactivity except when prompted by law enforcement is the only – and economically most advantageous - policy open to them. Frydman and Rorive state "undoubtedly the Directive seeks to stimulate coregulation". It does this by formally permitting national courts to over-ride the safe harbour in the case of actual or suspected breach, of national law, including copyright law and certain types of illegal content, such as hate speech or paedophilia.

Whereas in the US, the absolute speech protection of the First Amendment and procedural concerns mean that Notice and Take Down is counter-balanced by 'put back' procedures, in Europe no such protection of free speech exists, where speech freedom is qualified by state rights. In both jurisdictions, Notice and Take Down regimes cause Frydman and Rorive state that "this may lead to politically correct or even economically correct unofficial standards that may constitute an informal but quite efficient mechanism for content-based private censorship"[16]. It is clear that the economic incentive for ISPs is simply to remove any content notified, otherwise do nothing to monitor content, and let end-users, the police and courts, and ultimately the ethics of the content providers decide what is stored and sent over their access networks. Frydman and Rorive state that:

> Business operators should never be entrusted with … guidelines defining the limits of the right to free speech and offering procedural guarantees against censorship… which belong to the very core of the human rights of a democratic people[17].

That is nevertheless the situation which ISP CoCs seek to self-regulate.

**Overview of the Notice and Takedown (NTD) procedure**

Notice and takedown (NTD) procedure, as noted above, is a peculiar kind of internet content self-regulatory measure. In theory it consists of a scheme which sets forth that the parties hosting content agree to remove content in case of a legitimate notice by the consumer, without having to prove the legality of the content before a court of law. However, it seems that this is exactly the potential shortcoming: ISPs have to determine whether or not a complaint is legitimate.

At the same time the major advantage of the NTD procedure is that they reduce the high costs of litigation by providing a quick way to address consumers' complaints. Also, the procedure in principle promotes self-regulation which relies on constant cooperation between all actors.[18] The drawback of NTD is that the procedure puts a new burden on the content host—the ISP who deals with this burden in the self-regulatory scheme. The quandary for the ISP is

[16] Ibid at 56.
[17] Ibid at 59.
[18] Alexander M, Tambini D, (2003)European Mobile Industry Self-Regulation: IAPCODE Background Paper p13

whether to strictly investigate all claims of legal infringement, which is higher cost to itself in legal and forensic resources, or to adopt a more self-serving, cheaper and easier regime. To save costs and liabilities, the ISP may remove content immediately upon notice in order to protect itself against liability or to satisfy content consumers.[19] The ISP is encouraged to become a censorship body, to avoid liability when they choose to take down the information from a website upon receipt of a claim.

**Legal provisions of NTD in the US and EU**

In this section we briefly examine the legal background as it exists in the US and in Europe. We believe there are major differences increasing the incentives for a European ISP to take down content without any form of investigation.

United States

NTD is formalised under the Digital Millennium Copyright Act (DMCA), which obliges ISP to take down material whenever they are notified of copyright infringement.[20] The DMCA establishes the NTD procedure as follows[21]:

- The online service provider [hereinafter OSP] must have a designated agent to receive notices and it must use a public portion of its Web site for receipt of notices;
- The OSP must notify the U.S. Copyright Office of the agent's identity and the Copyright Office will also maintain electronic and hard copy registries of Web site agents
- Proper written notification from a copyright owner to an OSP must include:
    - the name, address and electronic signature of the complaining party,
    - sufficient information to identify the copyrighted work or works, the infringing matter and its Internet location,
    - a statement by the owner that it has a good faith belief that there is no legal basis for the use of the materials complained of, and
    - a statement of the accuracy of the notice and, under penalty of perjury, that the complaining party is authorized to act on behalf of the owner.

At the same time, DMCA protects ISPs from liability for unknowingly transmitting or storing copyrighted material. It provides *safe harbour* or immunities to ISPs for infringing action from the ISPs' users under four circumstances: [22]

[19] Ibid.

[20] DMCA Section 512 (b) (2) (E) " if the person described in paragraph (1) (A) makes that material available online without the authorization of the copyright owner of the material, the service provider response expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement…"

[21] DMCA Section 512 (c)(2)(A), (c)(3)(A).

[22] Lemley, K M (2003) "Comment: Protecting Consumers from Themselves: Alleviation the Market Inequalities Created by Online Copyright Infringement in the entertainment industry" ,Albany Law Journal of Science & Technology 2003 Vol.3 pp 613

(1) The ISP acts merely as a conduit, unknowingly transferring infringing materials; (2) The ISP temporarily stores infringing materials for the users' convenience; (3) The ISP acts as storage for infringing material, except when "the ISP knows or should know, or financially benefits from, the infringing material"; or (4) The ISP uses information location tools, such as hyperlinks, to find infringing materials unless the ISP has actual knowledge or received notice of the infringing materials

The procedure works as follows:

**Report** - a complainant serves a notice of infringing material

**Remove** - the ISP removes it, without judging the merits

**Respond** - the author can contest this by asking for replacement

**Replace** - again the ISP acts automatically

ISPs are still liable for their direct infringement, but they cannot be held liable for contributory or vicarious infringement. However, even though the DMCA establishes more clarity than the EC Directive[23] it is nevertheless criticized for taking a 'shoot first, ask questions later' approach. It should also be noted that the DMCA only applies to copyright; in other areas of "harmful content" there exists a patchwork of regimes; for non-intellectual property speech, such as defamation, ISPs have immunity from liability under the CDA section 230; and child pornography seems to have its own set of rules. However, Wendy Seltzer, staff attorney of EFF for i.e. says "I do think that the DMCA safe harbor has caused a lot of self-imposed censorship on copyright claims", because "when notice and takedown is implemented by service providers to take down material on the mere _allegation_ of copyright infringement, with no proof that any infringement has occurred, or when individuals take down sites based on overblown threats, speech is chilled. The chilling effect is when the takedown happens before judicial determination of infringement."

Europe

In Europe the EC Directive on Electronic Commerce contains no standard NTD procedure, even though a framework is established for self-regulation, as we outlined in the Introduction – a bargain in the shadow of the law. The relevant reference to the scheme can be found in Articles 14.3, 21.2 and Article 46, which reads:

> "In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or to disable access to the information concerned; the removal or disabling of access has to be undertaken in

[23] The Electronic Commerce Directive on Electronic Commerce (2000/31/EC) Available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

> the observance of the principle of freedom of expression and of procedures established for this purpose at national level; this Directive does not affect Member States' possibility of establishing specific requirements which must be fulfilled expeditiously prior to the removal or disabling of information."

The key provision here is the establishment of the concept of "actual knowledge". ISPs argued in favour of being mere conduit providers, without any liability regarding the content passing or being hosted on their servers, because of the impossibility of screening all content and subsequently judging what might be illegal or harmful. The ECD, though maintaining the mere conduit principle, limits this principle substantially, because when an ISP now "obtains actual knowledge" of a site containing infringement it must act "expeditiously to remove or disable access to the information concerned". Critically, whereas in some cases it might be easy to define what "actual knowledge" means, in many it might not:

- When an ISP receives a notice from a hotline it treats the complaint as actual knowledge and removes the content[24].

This defers responsibility for judgement to hotlines, which might be better trained for such an investigation. What constitutes actual knowledge remains undefined:

- whether it is merely an email,
- what sort of proof this email must contain, or
- whether it must be a letter with proof of the identity of the complainant.

To make matters even more complicated the term "awareness" seems even vaguer. Even though the intention seems to be clear: this article places responsibility upon the ISP to "self-regulate" and remove content as soon as he is made aware of illegal activities. The EC framework therefore seems to be broader and less defined than the US framework, for two reasons:

- It does not provide an exemption from liability, if the ISP acts according to a clearly defined procedure. This would remove the burden of investigation and judgement of the ISP, and transfer it to the parties involved – the complainant and the content provider.
- It does not create an incentive for the ISP to properly investigate whether content is illegal, but rather to remove the content expeditiously.

Article 14.3 leaves Member States to ensure that self-regulatory NTD procedures are established; and Article 21.2 provides that, when the Directive is next re-examined, the issues to be analyzed will include the NTD procedures and the attribution of liability following the taking down of content. Article 14 establishes the concept of 'apparent' illegal content, which the ISP needs to remove expeditiously, if made aware. Nas[25] notes:

> "what expeditious is, or how 'apparent' can be construed in a universally understandable and predictable way, is left open to the market … left to this self-regulation, providers

[24] Interview (2003) with Fred Eisner, chairman of Inhope, European association of hotline providers.
[25] Ibid at 169.

don't see much space to refuse requests to take down offensive, damaging or illegal content."

ISPs are neither obliged to publish statistics nor to justify their actions. Nas further points to commercial pressures, which force ISPs to observe risk-avoidance so they rapidly take down. She points to the official conclusion of Rightswatch:

" 'Any self-regulatory regime within the context of NTD procedures cannot be truly effective without some form of legislative underpinning'."[26]

RightsWatch funded by the European Commission to standardise the NTD procedure in six steps: location, notification, verification, information, take down and confirmation[27] yet it failed to reach consensus between the participating stakeholders (ISPs, civil society, rightsholders, academics etc.) on how NTD ought to be coherently institutionalized.

The lack of standard NTD procedure poses several problems. Firstly, ISPs are not able to know whether they are properly informed, whether the information (complaint) received is correct (founded) or not and whether they can face liability claims by web page creators when their pages have been shut down[28], and it is established ex post that the content was neither illegal nor harmful. Consequently there is potential shortcoming in the protection of freedom of expression [29] and Baistrocchi (2002) suggests the current regime may actually promote unfair competition in some situations[30] where companies engage in a form of commercial war on the internet, putting bad faith claims against their competitor's Web content. The Directive does not specify the essential information that a notification should include, leaving the matter to be settled by agreement between business operators. Instead, it encourages the national marketplace to produce its own standard procedure. [31]

Measured against the potential impact of the actions of an ISP on accessibility of information and on freedom of expression and speech, the legal situation under which ISPs operate NTD leaves room for doubts. Neither the E-Commerce Directive, nor the European Cypercrime Convention, nor national laws in the EU specify in detail the process of NTD, leaving ISP's in an uncertain legal environment. They are faced with a dilemma: If they are

[26] Ibid at 172.
[27] Details at RightsWatch Report ( 2002) IST 10639 p.11
[28] In this regard, the DMCA provides that "a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringed." DMCA, supra note 2, at (g)(1).
[29] The Council of Europe Declaration envisages the problem of NTD procedure in threatening the freedom of expression, saying "If service providers act too quickly to remove content after a complaint is received, this might be dangerous from the point of view of freedom of expression and information. Perfectly legitimate content might thus be suppressed out of fear of legal liability." *4th paragraph "notice and take down" procedures and freedom of expression and information*
[30] Baistrocchi ,P A (2002) Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce, Santa Clara Computer and High Technology Law Journal p.130
[31] Ibid.

notified of for example a website hosted on their servers containing allegedly pirated materials, they face potentially huge liabilities. So the rational ISP will act immediately and to remove the site, or to block access to it. On the other hand they face a rather limited danger of losing a customer, if the website contained perfectly legal materials. There is also the risk of a liability towards the customer who might lose business because of a bogus claim.

Thus the current regulatory settlement has created an environment in which the incentive to take down content from the internet is higher than the potential costs of not taking it down. The benefits for the ISP are higher to block access to content of an alleged illegal nature rather than to maintain it and to investigate a complaint thoroughly and to act only afterwards. Internet Service Providers are not surprisingly quite likely to take the path of least resistance and to take down quickly and not to ask too many questions beforehand. Furthermore there seems to be no coherent way of how NTD is practised: It remains unclear what constitutes a proper notice and how, if at all, the content provider needs to be notified and given time to respond to an accusation. Neither the terms of service of ISPs (see appendix 2), nor Codes of Conduct by the Internet Service Providers Association(s)(see below) specify in such detail NTD procedures.

Last but not the least, there are several loopholes in applying the NTD procedure in the EU. How are effective safeguards ensured to protect ISPs from acting on *wrongful takedown?* How are responses prioritized for copyright infringement and other claims of differing degrees of seriousness? Also, it is worth considering what type of liability is imposed upon the sender of unfounded notices to ISPs which lead to the takedown. These issues need to be addressed in the review of the Directive in 2006[32].

***ISP Codes of Conduct and Notice and Takedown***

ISP Codes of Conduct prescribe standards, norms and rules to which the industry should adhere. However, in the case of NTD most codes of ISP-Associations are notably quiet. The Code of Practice of the UK Internet Service Provider Association (ISPA) mentions the complaint procedure, but does not directly refer to the NTD procedure. However, all major ISPs in the UK have agreed to "use their reasonable endeavours to resolve a complaint within 10 working days of receipt of notice be it by email, letter, telephone call or in person", but make no data available about type and number of complaints and how fast, or slow, and how they react to those complaints.

[32] The Commission's first report on implementation, in 2003, generally concluded that transposition had occurred successfully, in all but 3 Member States. It found that only Finland and EEA member Iceland had implemented a statutory NTD procedure, for copyright. Given the high levels of Internet penetration and sophisticated user base in these countries, their statutory regimes deserve detailed comparative study as compared with the INHOPE hotline approach in for instance the UK and Ireland. See EC (2003) COM(2003) 702 final First Report on the application of 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) Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee Brussels, 21.11.2003 at p14 and footnote 76.

The only provision that can be found in this regard aims at protecting ISPs from too much government interference: it limits the liability of ISPs:

> "it is the role of the Government to engage in any filtering or censorship process above the consumer level. It should not be the responsibility of a Member to determine the legality or suitability, filter or otherwise restrict reception of, or access to, material save where such action is taken following an identified breach of the Code of Practice'[33]

Furthermore the Code lays out another rather political statement as opposed to a guideline, which would serve to help individual ISPs in their decision making process:

> "ISPA UK supports its Members in any independent decision taken by the Member to proactively limit the accessibility of illegal material via its service, but strongly states that no greater legal burden, standard of care or obligation should be placed on the Member who takes such action than is placed upon those Members who do not take such action."[34]

***ISP Market and Regulatory Cost-Benefits***

Self regulation is expensive, and businesses must see a clear benefit in order to support it. Costs include direct costs such as salaries of regulatory staff, which need to be spent to monitor, promote or enforce. There are also indirect costs of self-regulation work such as opportunity costs, i.e. markets that self-regalation leads them to forego. There will always be more directly profitable activities, which provide more benefits in the short run than those enjoyed as a result of the careful long-term investment into self-regulation. Hence it seems reasonable to speculate that the more costly the particular self-regulatory activity is, measured against the benefits, the less likely a business is to invest the needed resources to for i.e. (in the case of ISPs) provide a proper balance between potential liabilities and freedom of expression.

This might be further affected by the market structure. The more competitive a market, and the lower the profit margin, the less likely it is that businesses invest needed resources in self-regulation. This certainly appears to apply to the relationship between ISPs, the way they conduct NTD and the market. A quick overview shows that the market in the UK is very competitive: there are around 700 ISPs according to ISPA UK with Freeserve/Wanadoo, AOL UK and BT Yahoo! being the three major ISPs[35]. Freeserve is a subsidiary of French ISP Wanadoo and the UK's largest ISP in 2002 with 2.7m customers – with BT (1.8 m) and AOL (2.2m).[36] This consolidation of the market promises to make the situation for non-incumbents more difficult.

[33] The ISPA UK Code of Practice Statement of Policy at http://www.ispa.org.uk
[34] Ibid
[35] On 16 June 2003, BT and web content provider Yahoo! announced the joining forces to provide an enhanced broadband service. The new venture, called BT Yahoo! Broadband, replaces BT's Openworld brand.
[36] "What does Freeserve Wanadoo?" Sunday Times, June 15, 2003

Freeserve lost Euro 92m (£65m) in 2002.[37] Freeserve's market share has fallen from 27% in 2000 to 19% in May 2003, according to the latest figures from the Office of Telecommunications Oftel[38]. Hence one can conclude that ISPs will try to minimize the costs of NTD.

Furthermore, research by ISPA UK (2002) suggests that complaints related to copyright infringement now account for 54 percent of take-down notices.[39] ISPA-UK declined to provide further data on the topic. The remaining 46 percent is not clear, but it points to the second characteristic feature of the NTD regime: The responsibility for regulating content on the Internet has been transferred to private companies without developing proper criteria defining the duties and rights of the ISP, the complainant and the content provider. The procedure is open to abuse and creating doubts about its fairness, transparency and accountability and raising questions likewise about the effectiveness and desirability of self-regulation in this area.

An extensive literature search, as well as several searches on the internet of ISP's websites, do not provide any data regarding the frequency and type of complaints ISP's receive, how they investigate and react. A common characteristic feature of NTD is that is not transparent. Neither is there any information available on how many websites, chatrooms or blogs have been taken down, nor according to what criteria the ISP investigated, or how he actually removed the content; which is significant as an ISP has several means available to block access to websites. These range from:

- "soft" measures, which block access to anybody, but the content provider – leaving him time to respond and remove the section of the website subject to the complaint – to
- "hard(er)" sanctions, which can result in overblocking. ISP's can potentially block access to an IP-address entirely, making thousands of individual websites unreachable.

If the webmaster of a major e-commerce site uses his servers to peer-to-peer share mp3 files, a very likely scenario, and the ISP which hosts this very lucrative online business receives a notice by a rights holder, will the ISP dare to block the whole website? When it comes to less prominent customers the ISP might very well do so. Industry is neither willing to discuss NTD, nor to provide insightful data on it. Hence, self-regulation in this area, which can have drastic consequences for freedom of speech, is neither transparent nor, subsequently, sufficiently accountable.

[37] "AOL beats Freeserve to first net profits" Sunday Times June 29, 2003. Although AOL has fewer customers, it made a modest profit in 2002, generating about £340m in revenue from 2.2m paying customers.
[38] "Dixons' pounds 100m alliance with AOL threatens web woe for Freeserve" The Guardian, September 2, 2003
[39] Loney, Matt (2002) "ISPs buckle under copyright cases" 10th December 2002. Available at ZDNET http://news.zdnet.co.uk/story/0,,t269-s2127279,00.html

*How Much NTD Activity? Results of a Questionnaire Survey in the Netherlands*

Very little is known about the overall impact of NTD on internet content. Clearly, regulatory processes should ideally be transparent, in the case of NDT as we have seen, ISPs are not willing to provide data regarding frequency and types of notices and how they react. In light of this, PCMLP researchers, approached ISPA Netherlands to distribute a questionnaire to all its members. As noted above the results of the survey do not provide substantial evidence to support either of the above developed hypotheses, but neverthelessdo provide heuristic evidence.

- Only five (33%) out of 15 members of ISPA-NL responded to the survey.
- Ten (67%) were not willing to participate, even though we made clear that the intention of the research is not to put the blame on ISPs for removing content in an inappropriate way, but rather to get a clearer picture of what the problems are for ISPs.
- This seems surprising since their industry association contacted the ISPs, which should have increased responsiveness.

Two conclusions are possible:

- either ISPs perceive the NTD issue as unimportant, or
- they fear that intensified public discussion, and transparency, could harm their business.

We assume that the latter is the more likely explanation, given the failure of Rightswatch and the lack of legal clarity in Europe.

Some tentative conclusions can be drawn. There are different types of ISPs:

- ISPs for corporate clients;
- Consumer market ISPs with thousands of individual customers who increasingly use broadband connections;
- Those generally huge incumbent ISPs (cable and telecom carriers) with a mix of both.

The size and customer structure seems to influence the number and type of complaints ISPs receive. Whereas corporate orientated ISPs received almost zero complaints, large consumer orientated ISPs receive sometimes hundreds per month in 2003. A Dutch ISP with 150 000 customers hosting 24000 websites, of which 100% were personal homepages received in Jan: 732; Feb: 645; Mar: 624; Apr: 1048; May: 727; Jun: 839 complaints. Most of the complaints according to the ISP were not copyright related, but regarded the emanation of spam and viruses, stalking and defamation. They however reported copyright infringement claims from outside the Netherlands, mainly from the US. They reported their procedure as follows:

> "If (name of ISP) feels the complaint is valid, we first contact the customer and ask him/her to remove the offending content. If there is no response after a week, we block access via FTP, then we remove and locally store the offending content and after that we contact the customer again."

This is contradicted by recently published data of XS4ALL, another Dutch ISP (which was not addressed through the survey), with a similar customer structure, but known for its openness in dealing with the regulation of ISPs. Nas reports:

> "In the first six months of 2003, XS4ALL received a total of 750 serious copyright-related complaints: that is 31 complaints per week, or four and a half per day. The majority of these complaints are about straightforward infringements of copyright, and can be dealt with pretty easily. The remaining 10 per cent of the complaints however, demand a huge amount of time and attention from highly skilled legal professionals."[40]

The survey did not result in sufficient data to explain why some ISPs seem to receive more copyright infringement notices than others, though their customer structure seems similar. Nas noted further:

> "From January till July of this year (2003) XS4ALL received 265 complaints from the Motion Picture Association, 143 from the Interactive Digital Software Association, 110 from Mediaforce and 47 from the Business Software Alliance. On top of that, one specific right holder (Visualware) generated 125 complaints. So, out of the total 750 complaints, 681 stem from four large right holders, which amount to about 90 per cent. Most of these complaints are about FTP servers, usually on ADSL-nodes, about Usenet postings and sometimes about websites and home pages."

An interesting observation is that ISPs are getting a large proportion of complaints from the US, which do not even mention the ECD but the DMCA, which can also be backed up by our own research.

Further the ISPs which responded have one, or two, sometimes part-time staff dealing with complaints. None reported that they would involve a lawyer:

- It remains unclear whether technical personnel, or somebody with legal training, executes take down requests;

It seems probable that ISPs act on an ad-hoc basis rather than according to established and defined criteria. In summary, it was not possible to ascertain the overall impact of NTD on content available over the internet, or the amount of material that is being removed from the internet over time. This is because there is a lack of transparency in operation of the procedure. Even when contacted by their industry association and and EC funded university research group, they were not ready to respond to a survey. In the next part of this paper we outline a further piece of research designed to ascertain the detail of the operation of this procedure.

[40] Ibid at 165.

**The Mystery Shopper Test**

***Objectives***

Against this context, the objective of the research project was to conduct an analysis of NTD procedures under which ISPs were notified regarding illegal or harmful content and asked to remove ("take down") this content from a website.. Taking into account that it is not transparent to what extent and in what way NTD is being used, the objective of the research was to gather data to illustrate the reality of NTD. In particular we wanted to see how easily NTD can be abused, beyond theoretical speculations.

***Design and schedule***

Since we already suspected that the incentives are low for an ISP to provide data on cases where they misjudged and indeed removed lawful material from the Internet, a way to test the fairness of NTD was devised. We decided to post perfectly legal as opposed to borderline illegal or harmful materials with different ISPs and then to create artificial and (not immediately obvious) bogus complaints. Other ways of doing this part of the research project have proven to be legally difficult: It seems, both for legal, and for ethical reasons, undesirable to have illegal and controversial material hosted, such as racist or pornographic materials. What we wanted to investigate was how an ISP investigates a complaint, not its response to seriously harmful content per se.[41] Therefore we decided to conduct the test for the most common area of complaints – copyright infringement. We selected a section of John Stuart Mills "On Liberty", published in 1869 and hence freely useable in the public domain. Chapter II "Of the Liberty of Thought and Discussion" begins with the words:

The text is freely available throughout the web. The following is the excerpt of the text we used and available on the internet:

**ON LIBERTY**

**By John Stuart Mill**

CHAPTER II: OF THE LIBERTY OF THOUGHT AND DISCUSSION

THE time, it is to be hoped, is gone by when any defence would be necessary of the "liberty of the press" as one of the securities against corrupt or tyrannical government. (…)It is as noxious, or more noxious, when exerted in accordance with public opinion, than when in opposition to it. If all mankind minus one, were of one opinion, and only one person were of

[41] For the purpose of the research project the following terms are defined: "Content Providers", "Access Providers" and "Host Providers", which are some times separate businesses, but quite often an access provider provides also content, and hosts storage space for outside content. But in our case we most likely talk about third parties (individuals and companies) providing content. Backbone providers are excluded from the research as they are rarely in direct contact with individual internet users.
**Content Provider:** any provider supplying their own contents on the Internet
**Access Provider:** any provider supplying access to the Internet for Internet users
**Host Provider:** any provider providing storage space for outside Internet contents

the contrary opinion, mankind would be no more justified in silencing that one person, than he, if he had the power, would be justified in silencing mankind. Were an opinion a personal possession of no value except to the owner; if to be obstructed in the enjoyment of it were simply a private injury, it would make some difference whether the injury was inflicted only on a few persons or on many. But the peculiar evil of silencing the expression of an opinion is, that it is robbing the human race; posterity as well as the existing generation; those who dissent from the opinion, still more than those who hold it. If the opinion is right, they are deprived of the opportunity of exchanging error for truth: if wrong, they lose, what is almost as great a benefit, the clearer perception and livelier impression of truth, produced by its collision with error. (….)

We uploaded this extract to a website. We had two very simple websites created with free website services at major ISPs. Since we were interested in discovering if there is a difference between how ISPs react in the US as opposed to the EU we used a major US and a market leading UK ISP. We decided not to reveal the names of the ISP, because the research does not aim at criticizing a single ISP, but rather at developing a deeper insight on how ISPs react to a complaint. The next step then was to submit an artificial complaint. We submitted a complaint on behalf of the "John Stuart Mill Heritage Foundation" (which does not exist as research on the web suggests) and we claimed via a free email service, without providing a detailed address or other proof of identity, that this site has come to our attention and that it represents infringement of our copyright. The point was to find the right balance between an identity and an incident that is neither too obvious to be bogus, nor too difficult too discern for the ISP to judge, if she would investigate. Clearly associated with this is the problem of identity: How does an ISP judge that one who is sending the notice is whom she says he is? However, if an ISP would research she would deduce quickly that

a) John Stuart Mills written work must be in the public domain and that

b) the John Stuart Mill Heritage Foundation does not exist.

Subsequently the ISP should not have removed the site.

In the following pages we document the different steps undertaken.

**Result of the pilot experiment: US ISP**

In early July this year, we designed a webpage and uploaded it on an ISP hosting page, which is based in the US. A week after, we sent a complaint letter to the "complaints department" of the ISP's webmaster, claiming the webpage was infringing the copyright. Two more complaint letters were sent to push the claim further yet the ISP requested the complainant for more information to formulate a standard notification according to DMCA. Since the complainant did not provide enough information the ISP did not remove the webpage.

| **Date** | **Action** |
|---|---|
| July2003 | Research different policies of ISP in UK and US - Selecting two ISPs for testing |

| **US ISP** | |
|---|---|
| Early Aug 2003 | Posting a webpage through the free homepage services from a selected ISP based in the US. |
| 30th Aug 2003 | A complaint letter was sent, alleging copy infringement of above webpage (the second letter was sent shortly after the first one) |
| 2nd Sept 2003 | The third complaint letter was sent. |
| 8th Sept 2003 | The corresponding ISP responded to the complaint, asking for more information to formulate a complaint according the standard procedure stipulated in the DMCA |
| 17th Sept 2003 | The complainant was informed the webpage will only be take down if "under penalty of perjury" (DMCA required language) the complainant provides accurate information. At this point this project was discontinued. |

Below the first email complaint:

US ISP
Xxxxx xxxxxxx
Xxxxx xxxxx
Xxxxx xx
Telephone: xxx xxxxx
Fax: xxxx xxxxxx
Email address: xxxxx xxxxxx

The John Stuart Mill Heritage Foundation
Oxford OX4 3UD
**johnstuartmill@netexecutive.com**

Dear Mr xxx xxxx,

I am writing to you as the Chairman of the John Stuart Mill Heritage Foundation, which has been authorised as the holder of the copyright of all the published works of John Stuart Mill.

I would like to inform you that we have reason to believe that you are hosting material, which is published at the website of a third party, and which allegedly constitutes infringement of the copyright which we hold.

The website which I refer to is http://xxxx.xxxxx.com/mill02.htm

I would like to confirm that, the use of the material in this website has not been authorised by the John Stuart Mill Heritage Foundation, and hence I have reasons to believe that constitutes an infringement of our copyright.

I therefore hope that you will take the necessary measures to discontinue any such possible infringement of our intellectual property rights.

Thank you for your courtesy and anticipated cooperation,

xxxxx

At first we did not get a reply and the free email service was not accessible so we could not check for some time whether or not we receive a reply by the US ISP. In the meanwhile we could check the inbox of the content provider; there was also no message. So we created a different email address and write.

Here we get the first, very detailed, response:

Hello Peter,
9/8/03

I am writing in response to your e-mail regarding content hosted through xxxxx on one of our free homepage services. You should understand that the content to which you have referred have has been stored on the xxx system solely at the direction of a xxxx user and has not been initially reviewed, monitored, or edited by xxxx employees. xxxx users bear sole responsibility for such material, and xxxx Inc. has no knowledge of the specific contents of member directories.

Xxx Inc. fully complies with all intellectual property laws. In particular, when the owner of an exclusive right is concerned that this right is infringed by material placed on a provider's system or network by a subscriber of that provider the Digital Millennium Copyright Act "DMCA") provides certain procedures to ensure that infringing materials are removed without wrongfully injuring the subscriber or unduly burdening the provider. In such instances, the owner of an exclusive right should send to the provider a notification containing the following information:

1. A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

2. Precise identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online sites are covered by a single notification, a representative list of such works at that site.

3. Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material including exact URL's and references to specific files.

4. Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, and electronic mail address at which the complaining party may be contacted.

5. A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

6. A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right is allegedly infringed.

You have not provided all of the information required above.If you are able to provide the missing information, please submit an appropriate notification meeting all of the above requirements to xxxx Inc.'s registered agent for receiving such notifications:
Registered Copyright Agent

xxxxxx

Upon receipt of a proper notification, xxxx Inc. will respond
expeditiously to remove or disable access to the materials properly identified in the notification. xxxxx will provide a copy of the notification to the subscriber and give the subscriber an opportunity to respond.

This letter is written without prejudice to any right, remedy, or defense that xxxxx may have which has not been asserted in this letter. All such rights, remedies, and defenses are expressly reserved. If you have any questions about this letter, please do not hesitate to contact xxxxx registered agent. For legal advice, you should consult an attorney.

Sincerely,

Xxxxx

Hello Peter,

The set of guidelines that you received are sent to all persons claiming copyright infringement. I apologize for the dry nature of this procedure, but this is necessary in order for us to address your concerns as quickly as possible while adhering to DMCA law.

Please pay particular attention to the wording that the complaining party is asked to use in #'s 5 & 6 (the phrases "good faith belief", and "under penalty of perjury" must be used). A scanned signature is not necessary, a typed one is fine.

Please do not include the numbered guidelines in the body of your complaint, since copies of the notice must be sent to the infringing parties. Feel free to contact me if you have additional questions.

Sincerely,

Xxxxxx

***US Conclusion***

At this point the test of the US ISP was discontinued, even though no signature was required and somebody with some "criminal energy" could have easily continued and used the required phrases. At the same time the project has shown that this ISP followed exactly the procedure laid out in the DMCA and did not act, before he had a proper notice.

***UK Test***

To get a comparative impression we conducted a similar test with a UK based ISP with a different outcome. Unlike to the standard NTD procedure listed in the legislation in the US, the corresponding ISP in the UK removed the alleged website shortly after receiving the complaint letter.

| **UK ISP** | |
|---|---|
| 9th Nov 2003 | Posting a webpage through the free homepage services from a selected ISP in based in UK. |
| 13th Nov 2003 | The same complaint letter was sent, alleging copy infringement of above webpage |
| 14th Nov 2003 | The ISP took down the webpage and that website user was notified |

Email to webmaster@xxx.com:

The John Stuart Mill Heritage Foundation
Oxford OX4 3UD
johnstuartmill@xxxx.com

Dear Webmaster,

I am writing to you as the Chairman of the John Stuart Mill Heritage Foundation, which has been authorised as the holder of the copyright of all the published works of John Stuart Mill.

I would like to inform you that we have reason to believe that you are hosting material, which is published at the website of a third party, and which allegedly constitutes infringement of the copyright which we hold.

The website which I refer to is at xxxx.mysite.xxxxx.com

I would like to confirm that, the use of the material in this website has not been authorised by the John Stuart Mill Heritage Foundation, and hence I have reasons to believe that constitutes an infringement of our copyright.

I therefore hope that you will take the necessary measures to discontinue any such possible infringement of our intellectual property rights.

Thank you for your courtesy and anticipated cooperation,

Peter S. Burton (Chairman)

**Your message has been sent!**

| | |
|---|---|
| **To:** | Webmaster@xxxxx.com |
| **Subject:** | breach of copyright |
| **Sent On:** | Thursday, November 13, 2003 07:25 AM |

Dear Mr Burton,

Thank you for your email.

We can confirm that this matter will be investigated and the appropriate action will be taken.

Kind Regards

Susie
xxxxx Customer Action Team

Fri, 14 Nov 2003 11:20:19 +0100 (CET)

| | |
|---|---|
| **From:** | support.mysite@XXXX.com [ [ |
| **Subject:** | Suspension of the site: mysite.XXXX.com/johannamuhle |
| **To:** | xxxx@xxx.com |

Text Size: S **M** L XL

Dear XXXX My Site User,

Your website does not comply with XXXXX's My Site Terms of Use.
For this reason we have temporarily suspended your site which means
it is no longer online. You can find our Terms of Use by clicking
on this link : http://www.XXXXX.com/xxxx .
If you wish us to reinstate your site, please send an email to
support.mysite@XXXXX.com after you have removed the offending material from it.

Regards

XXXX Community Services

***Preliminary Conclusion: US vs UK***

The result is illustrative. We learnt that with relative ease – sending one email –.an ISP could be prompted to remove a piece of public domain content from their servers. Whilst in our symbolic case of the JS Mill extract, this may be of little import given that JS Mill's work is replicated and downloadable in hundreds of other websites, there is no reason to believe that unique content should not be just as easily removable. We might think for example about the difficult area of defamation. It is at least theoretically possible that a powerful individual might use the apparent lack of due diligence on the part of ISPs to use the threat of liability for defamatory material to persuade ISPs to remove material.

It should, however, be noted that the content provider (see email above) would have had the option to complain to the ISP. We did not complain. We did not [1] expand this test to other ISPs; [2] use variations, or [3] replicate the test with ISPs in other European countries. Although our tests and the survey are not representative, they provide some insights about how NTD is practised and the difference between the procedures between the US and the UK. According to the Mystery Shopper test, the ISP in the UK, and probably likewise in other member states, has a high propensity to remove a website without careful examination of the content. This observation substantiates our concern over potential abuse of NTD. This is also supported by the absence of a standardized NTD procedure. Based on our experiment, it appears that the UK ISP did not investigate the validity of the complaint carefully, nor did she research whether the content is public domain.

**Policy Conclusions**

The Mystery Shopper and Netherlands case study evidence hints that the NTD regime leaves room for easy abuse, which could amount to censorship. This suggests further that the current framework established by the E-Commerce Directive provides an incentive for ISPs to take down content without investigating the complaint. This is because it does not set forth a detailed "put back" procedure, as it exists in the US.

Under this delegated (self)-regulatory regime the peculiar, technological architecture of the internet is utilized to induce technological control mechanisms by private parties, without duly considering their powers, interests and normative standards. Under this arrangement ISPs have to assume the role of judge, jury and enforcer at the same time. They not only have to make a judgement whether a website is illegal, or not, on the merits of the evidence gathered by themselves (something that directly contravenes basic principles of due process), but they also have to behave as enforcing agents with executive powers. The difference to established forms of media regulation is the private nature of the regulator and the power that is, otherwise clearly separated in between branches of government, accumulated in one institution.

Nevertheless once an ISP removes content she does so with such technical force that it can be called the cyber-equivalent to deportation. When an ISP acts she could disrupt a business, censor a political campaign. ISPs could for example in theory eliminate the criticism of an anti-globalisation NGO of a corporation so effectively that she makes access to the website for everyone on the Internet impossible.[42]

In consequence this bears the potential for injustice, not tolerated in other media, as lawful information and materials might be censored. As the Electronic Frontier Foundation notes on its chillingeffects.org website, which documents NTD, even though the law in the US seems to be much clearer:

> "Anecdotal evidence suggests that some individuals and corporations are using intellectual property and other laws to silence other online users (…) and to "chill" legitimate activity."[43]

Some policy recommendations can be drawn.

1. First and foremost the legal framework needs to be clarified.
2. Legally it might also result in arriving at the conclusion that it might be necessary to remove, or limit, liability of ISPs, if they take the defined steps.
3. If this form of "delegated self-regulation" is to be continued clearer guidelines in the code of practice need to be included, and the duty to report and document complaints.

[42] Needless to say, that the whole operation is a potentially very costly responsibility for a business selling internet connectivity and webspace at its core, limiting in turn its incentives to perform the above mentioned functions appropriately.
[43] Chillingeffects House available at http://www.chillingeffects.org

4. In addition standardizing and restructuring NTD procedures will permit greater transparency. In particular, ISPs should have an obligation to read and make available detailed information on NTD activity.

**References**


Alexander M, Tambini D, (2003) European Mobile Industry Self-Regulation: IAPCODE Background Paper

Baistrocchi, P A (2002), Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce, Santa Clara Computer and High Technology Law Journal

Child's Internet Protection Act 2003

Chilling Effects Clearinghouse available at http://www.chillingeffects.org

Clayton, R (2000) Judge & Jury? how "Notice and Take Down" gives ISPs an unwanted role in applying the Law to the internet 26th July,2000 http://www.cl.cam.ac.uk/users/rnc1/Judge_and_Jury.html

Communications Decency Act 1996 Section 30, 47 U.S.C. § 230(c)(1) (Supp. II 1996).

Digital Millennium Copyright Act (DMCA)(1998) Section 512

Durman, P (2003) ,AOL beats Freeserve to first net profits, *Sunday Times* June, 29, 2003

Durman, P (2003) What does Freeserve Wanadoo? *Sunday Times*, June 15, 2003

EC (2003) COM(2003) 702 final First Report on the application of 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) Report From The Commission To The European Parliament, The Council And The European Economic And Social Committee Brussels, 21.11.2003

Electronic Commerce Directive on Electronic Commerce (2000/31/EC) Available at http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_178/l_17820000717en00010016.pdf

Elkin-Koren, Niva (1995) Copyright Law and Social Dialogue on the Information Superhighway: The Case Against Copyright Liability of Bulletin Board Operators, 13 Cardozo Arts & Ent. L.J. 345, 399-410

Frydman, B. and Rorive, I. (2002) Regulating Internet Content Through Intermediaries in Europe and the USA, Zeitschrift fur Rechtssoziologie Bd.23/H1, July 2002, Lucius et Lucius.

Hardy, Trotter (1994) The Proper Legal Regime for "Cyberspace", 55 U. PITT. L. REV. 993, 1042-46

Holznagel, B. (2000) Responsibility for Harmful and Illegal Content as Well as Free Speech on the Internet in the United States of America and Germany, in C.Engel and H. Keller (eds) Governance of Global Networks in Light of Differing Local Values, Nomos, Baden Baden.

Lawson, A (2003) Dixons' pounds 100m alliance with AOL threatens web woe for Freeserve, *Guardian*, September 2, 2003

Lemley, K M (2003), Comment: Protecting Consumers from Themselves: Alleviation the Market Inequalities Created by Online Copyright Infringement in the entertainment industry, Albany Law Journal of Science & Technology 2003 Vol.3

Loney, M (2002) “ISPs buckle under copyright cases” ZDNET 10th December 2002 Available at http://news.zdnet.co.uk/story/0,,t269-s2127279,00.html

Nas, Sjoera (2003) Spread the Word. OSCE

Noam, Eli (2003) Oxford Internet Institute Issue Brief No.1 The Internet: Still Wide Open and Competitive?

Polygram Int’l Publ’g v. Nevada/TIG, Inc., 855 F. Supp. 1314, 1317-18 (D. Mass. 1994).

Reuters (March 18 2004) Central Filter Against Web Hate for French Schools at http://www.reuters.com/newsArticle.jhtml;?storyID=4599516

RightsWatch Report (2002) IST 10639

The ISPA UK Code of Practice Statement of Policy Available at http://www.ispa.org.uk

Tickle, Kelly (1995) Comment, The Vicarious Liability of Electronic Bulletin Board Operators for the Copyright Infringement Occurring on Their Bulletin Boards, 80 IOWA L. REV. 391, 416 (1995)

Working Group On Intellectual Property Rights, Information Infrastructure Task Force, Intellectual Property And The National Information Infrastructure 1-6, 114-24 (1995).

Yen. A. (2000) Internet Service Provider Liability for Subscriber Copyright Infringement, Enterprise Liability and the First Amendment 88 Georgetown L.J. At http://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID236478_code000726304.pdf?abstractid=236478

Zittrain, J (2003): “Internet Points of Control”. The Berkman Center for Internet & Society: http://cyber.law.harvard.edu/publications

**Appendix I—Questionnaire on Notice and Take Down Procedure**

**Programme in Comparative Media Law and Policy**
**Oxford University, Centre for Socio-Legal Studies**
**PCMLP**

**Questionnaire on Notice and Take Down Procedures**

**The Programme in Comparative Media Law and Policy at University of Oxford conducts an analysis of notice and take down procedures under which Internet Service Providers are contacted regarding illegal or harmful content and asked to remove ("take down") this content from a website.**

**The European Cypercrime Convention does not specify in detail the process of notice and take down, leaving ISP's in an uncertain legal area. Nevertheless notice and take down is seen as a means to control illegal and harmful content on the Internet, but it remains unclear whether it is an effective and politically acceptable way to regulate content on the Internet.**

**So far almost no data on number, types of complaints and reaction of ISP's is available. The following questionnaire is designed to gather data to shed light on the issue and will be used in a report that aims at increasing our understanding of notice and take down procedures. The Programme for Comparative Media Law and Policy is conducting this research as part of its selfregulation.info project. This questionnaire will be distributed to all members of ISPA-NL and the results will be published as part of a larger report on NTD. Please send the completed questionnaires to: wouter.diephuis@nlip.nl**
**If you have additional questions please contact:**
**Christian.Ahlert@wolfson.oxford.ac.uk**
**Thank you for your cooperation.**

1. How many customers does your ISP have?

Please distinguish between hosting-customers and the total (including access-) customers?)
How many of them are consumers?
How many are business/companies?

2. How many websites do you host (in total)?

3. How many complaints did your ISP receive in the last six month (please provide information for each month)?

4. Who were the complainants (please provide categories such as rightsholders associations, individual companies etc.)?

   Note: Considering the Dutch draft liability-regime please distinguish in between civil complainants and criminal complaints and treat for i.e. rightsholders associations differently.

5. Where did the complaints originate from (inside your country, or from abroad) – was there any difference related to type of complaint and point of origin?

6. About what did you receive notices (defamation, pornography, copyright infringement)?

7. Please describe who is dealing in your ISP with the complaints and provide number of employees engaged in investigating complaints?

8. How do you reach a decision regarding a complaint? Who is involved and do use a certain set of criteria to decide complaints?

9. How have you been contacted?
   -directly
   -via hotlines
   -via the authorities

10. How many complaints have been upheld (specify area)?

11. How many and what type of sites have been removed?

12. Did complainants indicate the action desired?

13. How did you remove the site (blocking of IP address etc.)?

14. (How) did content providers react – please describe?

15. How many sites have been put back, after they have been taken down?

**Appendix II—Overview several ISPs in the UK**

**Thus-plc-Demon Internet**

Region: Scotland

Location: Glasgow and London

Category: Large

Website: www.demon.net

Contact: 0845 272 0666

Email: sales@demon.net

Internet Acceptable Usage Policy (AUP): Yes

**Complaint procedure**: Yes

"We have in place a procedure for handling your complaints about material stored and/or accessed via our service. If you wish to make such a complaint, please ensure that you make your complaint by email to abuse@demon.net. If you do not use this facility we cannot guarantee that your complaint will be dealt with promptly"

abuse@demon.net

Fax: 0208 371 4070

**Webpage Takedown**:

**"Demon reserves the right to remove any material from a web site at our sole discretion, without prior notice and without explanation.**

A web site may not be used to offer, advertise or distribute any of the following types of material:

- software for sending 'spam' (bulk emails, excessive news postings, etc.);
- illegal material
- lists of email addresses, except where all the owners of the addresses have given you explicit permission;
- any collection of personal data other than in accordance with the Data Protection Acts 1984 and 1998.

You must comply with the Data Protection Acts 1984 and 1998 (and any amendments or re-enactments of them) regarding all information received, stored or communicated through the use of your web site.

If your web site contains material that may cause general offence, a clearly readable warning page must be shown before any such offensive material is displayed.

To avoid doubt, this means that your top-level web page (usually index.htm or index.html) must not contain any adult material or other material that may generally offend. Where part of a web site forms an independent area that is not linked to by a topmost page, it will be considered as a site in its own right when considering whether appropriate warnings are present. Warnings are also required where the material is referenced directly from a web site, with no intervening pages, or where the use of frames makes the material appear to be part of a web site.

All of the web pages on a web site are considered to be publicly visible and may be downloaded by any person, whether or not they are linked from any central contents or home page. However, specific mechanisms are available as part of some services to prevent unauthorised access. Pages protected in such a manner will not be considered to be public.

Web sites may not be advertised by you, or by another person, using techniques that would be classified as "abuse" if they were carried out from a Demon account including, but not limited to, bulk emailing and excessive news posting. Such action will be treated under the Demon AUP as if it had been done from the Demon account.

Web sites must display a valid, up-to-date email contact address for the person responsible for the site. The use of the generic address of "webmaster" is acceptable for this purpose. This address must appear on the top-level page or be easily locatable from the top-level page.

**Freeserve.com**

Region: South East
Location: Herts
Category: Large

Website: www.freeserve.co.uk
Contact: 0870 872 0099
Email: info@freeserve.com

Internet Acceptable Usage Policy: Yes

**Complaint Procedure**: Few Details

“If you have a complaint about any aspect of the Services, please let us know by calling the Customer Number and we will endeavour to resolve any complaints as soon as is reasonably possible.”

"If you are not satisfied that your complaint has been resolved, you can escalate your issue, in writing, to the Customer Action Team, Freeserve, PO Box 73, Leeds, LS10 1WZ. Once your complaint has been fully investigated we shall reply back to you"

**Webpage takedown**

"In the event that Freeserve receives a complaint concerning the contents of personal Web Pages, **Freeserve reserves the right to either block access to or delete the Web Pages and/or terminate your access to the My Site Builder service depending up on the severity of the complaint.**

Freeserve will endeavour to contact the User concerned to inform them that a complaint has been received, the action that has been taken by Freeserve according to Freeserve's evaluation of the complaint allegation, and what steps (if any) that are required to be taken by the User."

**AOL Europe**

Region: London
Location: London
Category: Corporate

Website: www.aol.co.uk
Contact:
0800 279 1234 (Residential)
0800376 5432 (Business)
Email: N/A

Internet Acceptable Usage Policy: Yes

**Complaint procedure**: No Details (only enquiry contact)

"To report unacceptable online AOL member behaviour which you feel breaches the AOL Conditions of Service email COSMonitor@aol.com"

**Webpage Takedown:** No Details

**Terms of Use**

"AOL.co.uk is provided to you free of charge and without any warranties or guarantees.

You may only use AOL.co.uk for legal purposes and for your own personal use and not for profit or commercial purposes. You may not use AOL.co.uk, or its services to publish, post, distribute or disseminate any defamatory, obscene, or other unlawful material or information, including another's proprietary information, including trademarks or copyrighted information

(other than where you have a licence to do so). Additionally, you may not use AOL.co.uk to collect or harvest personal information, including internet addresses, about AOL.co.uk users.
You must abide by any policies posted on AOL.co.uk. You understand that AOL provides no assistance, including the review, removal or editing of content posted on, or any customer support for the use of, the AOL.co.uk Web site(s)."
AOL, Inc. uses its best efforts to maintain AOL.co.uk but is not responsible for the results of any defects that exist in AOL.co.uk, or any resulting lost profits, loss of data or other consequential damages. You should not assume that aol.co.uk or its content is error-free or that it will be suitable for the particular purpose that you have in mind when using it. **AOL may, in its sole discretion and at any time, modify or discontinue aol.co.uk; limit, terminates or suspend your se of or access to aol.co.uk;** and/or make changes to these Terms of Use."

**POPTEL**

Region: North West
Location: Manchester and London
Category: Medium

Website:www.poptel.net
Contact: Stephanie Gay 0800458 9465
Email: info@poptel.net

Acceptable Usage Policy: Yes

**Complaint procedure**: Yes ( Few details)
"If you feel that someone using a Poptel service has contravened one of the above policies please inform us by email at abuse@poptel.net
**Webpage Takedown**
**"Poptel reserve the right to remove a site or material from a site under any of the following circumstances:**

- Data contained on the site is suspected to be illegal.
- The site gets an abnormality high number of hits.
- The customer closes their account or the customer's account is suspended for any reason.
- The presence of the site adversely affects, in any way, the ability of Poptel to provide its services to other customers.

It is not permitted for any customer to resell their web space, unless a previous agreement with Poptel has been made."

**Which? Online**

Region: London
Location: London
Category: Medium

Website: www.which.net
Contact: 0645 830240
Email: support@which.net

Internet Acceptable Usage Policy: No Details

**Complaint procedure**: No details

**Webpage Takedown**:
No details

**Set-up information/Publishing website:**
No Details

**Fastnet International**

Region: South East
Location: Brighton
Category: Medium

Website: www.fastnet.co.uk
Contact: 01273 677 633
Email: sales@fastnet.co.uk

Acceptable Use Policy: Yes

**Complaint Procedure**: Few details

"FastNet will always respond to complaints about UCE/UBE/SPAM and any incidence should be reported to abuse@fastnet.co.uk, complete with a copy of all the mail headers."

**Webpage Takedown**: Unclear

**Yahoo!UK**

Region: London
Location: London
Category: Large

Website: www.yahoo.co.uk
Contact: No details
Email: No details

Connection:
56Kbps Modem / ISDN 64

Acceptable Use Policy: Few Details

**Complaint Procedure**: No Details

**Webpage takedown**: Few Details

*Term of Service*:
"You agree that Yahoo! in its sole discretion, may terminate your password, account (or any part thereof) or use of t he Service, and remove and discard any Content within the Service, for any reason, including, without limitation, for lack of use or if Yahoo! believes that you have violated or acted inconsistently with the letter or spirit of the TOS. Yahoo! may also in its sole discretion and at any time discontinue providing the Service, or any part thereof, with or without notice. You agree that any termination of your access to the Service under any provision of this TOS may be effected without prior notice, and acknowledge and agree that Yahoo! may immediately deactivate or delete your account and all related information and files in your account and/or bar any further access to such files or the Service. Further, you agree that Yahoo! shall not be liable to you or any third-party for any termination of your access to the Service."