Journal of Information, Law and Technology

Nazis, Porn and Politics: Asserting Control Over Internet Content

Carolyn Penfold
Lecturer, Faculty of Law, and
Research Associate, Cyberspace Law and Policy Centre,
University of New South Wales, Sydney, Australia
c.penfold@unsw.edu.au

This is a **refereed** article published on: 2 July 2001

Citation: Penfold C, Nazis, Porn and Politics: Asserting Control Over Internet Content', 2001 (2) *The Journal of Information, Law and Technology (JILT)*.
<http://elj.warwick.ac.uk/jilt/01-2/penfold.html>

Abstract

Australia's attempts to control content on the internet were criticized as making Australia the 'village idiot of the internet world,' lacking understanding of a global technology not susceptible to control by national governments. A recent French Court decision, ordering Yahoo Inc (US) to block French internet users' access to certain content on its site, is another attempt to use one country's laws to control local access to internet content. This paper examines the Australian legislation and the French court decision and concludes that these two attempts to control access to internet content presently appear equally ineffective. However, by signaling to other nations their willingness to act to regulate internet content, these actions may in fact increase the impetus for moves toward more effective international agreement in this area.

Keywords: Internet Censorship, Internet Content Control, French Decision v Yahoo! Inc, Australian Internet Regulation**.**

1. Introduction

The regulation of internet content has been topical for some time, but no consensus has arisen as to whether or not there should be any such regulation, the extent to which there should be regulation, nor as to the means by which regulation might be achieved. However, in recent years a number of attempts have been made in individual nations to regulate access to content on the internet. This paper discusses the *Broadcasting Services Amendment (Online Services) Act 1999 (Cth)* introduced in Australia specifically to regulate internet content, and the case of *LICRA et UEJF vs Yahoo! Inc and Yahoo France,* which applied general law in an attempt to restrict access to illegal content available over the internet to users in France. The very different methods applied in Australia and France, and criticisms of both, illustrate the difficulties faced by individual nations in trying to assert control over internet content.

2. Australia's Attempt to Regulate Internet Content

A major study conducted by the Australian Broadcasting Authority in Australia in 1996 recommended against legislative restriction of internet content, favouring instead the pursuit and development of better labeling and filtering products and protocols. However, against this advice the Australian government introduced 'a regulatory framework for Internet content' through the *Broadcasting Services Amendment (Online Services) Act 1999* (Cth). During the passage of this legislation through parliament, and after it was enacted in June 1999, the Australian government was lampooned by internet users, and by parts of the internet industry. It was said that the government did not understand internet technology, that the legislation would make Australia the 'Village Idiot' of the internet world, and would slow, if not kill, the burgeoning Australian internet industry. A major criticism was that the proposed legislation simply could not work, as the government was trying to legislate locally over a global phenomenon.

2.1 The Provisions of the Broadcasting Services Amendment (Online Services) Act 1999 (Cth)

The Australian *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) is intended to operate through a system of co-regulation, whereby the Australian Broadcasting Authority (ABA) investigates and makes decisions about internet content, and industry bodies develop codes or standards which specify the technical aspects of how those decisions are to be applied.

The ABA is given the power to investigate complaints made about online material, and this complaints mechanism has been referred to as 'the cornerstone of the regulatory framework'. The ABA may also investigate material of its own volition, although 'it is not intended that this discretion will be used to monitor content actively'.

Complaints may be made about prohibited or potential prohibited content accessible via the internet. The Act defines 'prohibited content' to include Australian hosted R-rated material which is not subject to a restricted access scheme, and all material rated X or RC, wherever hosted. 'Potential prohibited content' is unclassified content which, if classified, would be substantially likely to be prohibited content.

Where the ABA identifies internet material which is, or would likely be classified R, X, or RC, the action to be taken by the ABA depends on whether the material is hosted in Australia or is hosted overseas.

2.1.1 Material Hosted Within Australia

The ABA may issue interim take-down notices to Australian sites hosting what is believed to be X or RC material, and refer such material to the Office of Film and Literature Classification (OFLC) for classification under the guidelines currently used for rating films. Material hosted within Australia and believed to be R-rated is not subject to interim take-down orders, as it is generally of a less serious nature, and issuing interim orders for such material may substantially increase both the ABA's administrative costs and the industry's compliance costs. However, the ABA will still refer such material to the OFLC for classification.

The ABA may revoke its notices, or issue final take-down notices, depending on the classification which the material receives, whether there has been a voluntary take-down of the material, and in the case of R-rated material, whether or not an approved restricted access system is in place. The ABA may also issue notices for removal of material 'substantially similar' to that which is the subject of such a notice.

2.1.2 Material Hosted Outside Australia

Where the ABA is satisfied that material hosted outside Australia is prohibited content (that is X or RC material), two possibilities arise. In the absence of an industry code dealing with the topic, the ABA may issue a standard access prevention notice requiring

internet service providers (ISPs) to 'take all reasonable steps to prevent end users from accessing the content'. Where a relevant industry code of practice has been registered ISPs must comply instead with that code. Under the code currently registered ISPs will be notified of overseas-hosted prohibited content via a Designated Notification Scheme, and must then provide an approved filter or filtered service to subscribers. In the case of commercial subscribers ISP's must provide appropriate software (which may be an approved filter) or facilitate access to a consultancy service with respect to appropriate technology. Provision of filters and access to consultancy services is not required where subscribers already have in place alternative access prevention arrangements such as firewalls. R-rated material housed overseas will not be subject to blocking under the Act, although the inclusion of such material will be looked at during a review of the legislation.

2.1.3 General Provisions

The ABA is also empowered to register appropriate industry codes, and to draft codes or industry standards where there is no relevant industry body, where the industry body has not done so, or where the ABA believes that the code or standard is deficient. The ABA must also monitor compliance with such codes or standards. Further, the ABA is given power to approve restricted access systems (RAS) behind which Australian R-rated material must be housed.

Not all of the powers given to the ABA under the Act are so technical however. Further functions include advising and assisting parents and adults in relation to supervision and control of children's internet access, conducting and co-ordinating community education programs, conducting and commissioning research into related issues, liaising with regulatory and other bodies involved in the internet industry, and gathering information on technological developments and service trends in the industry.

Industry codes likewise are required to cover more than just the technical aspects of content regulation, and should deal with topics such as advising and assisting parents and responsible adults in relation to supervision and control of children's internet access, giving content providers information about their legal responsibilities, and informing users of complaints procedures regarding online content.

2.2 Effects of the Australian Legislation

The Australian legislation, read in conjunction with the Internet Industry Codes of Practice, does not in fact restrict or control access to internet content. While the legislation initially aimed to:

> 'restrict access to certain Internet content that is likely to cause offence to a reasonable adult, and to protect children from exposure to Internet content that is unsuitable for children',

this has not been achieved. The legislation does prohibit the hosting of X and RC material in Australia, but does nothing to stop access to the same material hosted overseas. While

the legislation itself required ISPs to 'take all reasonable steps to prevent end-users from accessing that content', this requirement has been greatly undermined by the Internet Industry Codes of Practice which allow ISPs to fulfill their responsibilities simply by offering subscribers access to a content filter or filtered service.

While the legislation could have placed much heavier burdens on industry, or the Industry Code could have been refused registration as not allowing for sufficient content control, the government was very concerned about stymieing growth in the internet industry. The government felt that the legislation it enacted:

> 'steered a middle course between heavy handed prohibitions that could hinder industry development and a laissez-faire 'do nothing' approach'.

It acknowledged that any prohibitive legislative regime would encounter difficulties but believed that:

> 'it would be an abdication of responsibilities … to put the whole issue into the 'too hard' basket … given the level of community concerns about the dissemination of illegal and offensive material on the Internet'.

The government wished to be seen by the community to be doing something to regulate internet content, although its desire not to place too great a burden on industry meant that the law it enacted was in fact ineffective.

3. Territorial Limits

While the Australian government was trying to steer a middle course between industry and those calling for content control, it was conscious also of the issue of jurisdiction, and the need to confine its legislation to Australian matters.

Although in some respects the *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) does not spell out its intention to deal only with Australian activities, and its definition of an ISP as a person who 'supplies, or proposes to supply, an internet carriage service to the public' is not specifically limited to ISP's within Australia, it is clear that the legislation is in fact intended only to cover ISPs providing carriage services 'supplied to end-users in Australia'. If no industry code is in place, notices regarding prohibited content are to be sent to ISPs 'known to the ABA', and under the codes currently in place only Australian ISPs are notified. The Act, when read in conjunction with these Industry Codes of Practice, does not attempt to bind anyone outside Australia, nor to hold anyone outside Australia responsible for access to internet content within Australia; its reach is clearly territorial only.

Many other governments have also attempted to control internet content within their own borders through legislation. Singapore, China, and Cuba for example have sought to regulate their own internet industries, and material coming into the country, but not to regulate people or content outside the country. Others are pursuing co-operative arrangements to allow the regulation of internet content, and its enforcement, beyond the

borders of individual countries. Most governments have accepted that it is only with such agreement that legislation could be used to control or censor internet content beyond one nation, and that legislation simply asserting extra-territorial control would appear ludicrous and achieve nothing. However, such territorial limits were not seen as constraints in the application of French legislation to those outside France in the recent case of *LICRA et UEJF vs Yahoo! Inc and Yahoo France.*

The judge in that case took a novel approach to the censorship of internet content. Although the legislation in question in that case did not purport to have extra-territorial reach, nor did it relate specifically to the internet, a French court held that internet content hosts and service providers, even those outside France, fell within French jurisdiction through providing content to internet users within France. While many other nations have looked to internet specific legislation, the French Court instead applied general French legislation to those allowing access to internet content within France, although the content originated, and the carrier was situated, outside France. The case raises many difficult and interesting questions regarding the censorship of internet content by individual nations.

4. The French Case: LICRA et UEJF vs Yahoo! Inc and Yahoo France

Three decisions (in May, August, and November 2000) were handed down by the Superior Court of Paris in the case of *LICRA et UEJF vs Yahoo! Inc and Yahoo France*. The plaintiffs in the case were LICRA, a group whose objects include combating racism and anti-Semitism, and defending the honour and memory of the departed, and UEJF, a Jewish student group. The Court was asked to find that Yahoo's advertising and sale of Nazi objects and memorabilia on and through its portals breached Article R.645-1 of the French Penal Code, and Articles 808 and 809 of the New Code of Civil Procedure, banalized Nazism, encouraged the propagation of anti-Semitism, and constituted an offence against the collective memory of a country profoundly wounded by the atrocities committed by and in the name of a Nazi criminal enterprise. The plaintiffs requested that Yahoo France and Yahoo Inc (US), which listed and displayed Nazi items and memorabilia on its auction site, and hosted a 'revisionist' section, be ordered to make that material inaccessible in France, and that the Court impose heavy fines for breach of such orders.

4.1 The Decision Against Yahoo France

There was no dispute that the sites in question were accessible from France, that the objects complained of were available for sale through the Yahoo Inc auction site in the USA, nor that the advertising and selling of these objects would breach the French Codes. Although Yahoo's French site had no involvement in this selling or advertising, it did provide French web users with links to the US site.

Yahoo France defended itself on the grounds that the French site was not in breach of the Codes as it did not participate in the selling, advertising or display of the items. The Court accepted that Yahoo France was not itself hosting advertisements or auctions for Nazi

items. However, as a result of the links available from Yahoo France to Yahoo Inc's (US) auction site, the Court ordered Yahoo France to warn internet users that they must terminate their connection if the result of their searches (on Yahoo Inc (US) through links on Yahoo France) led to sites, pages, or forums, the title or contents of which constituted a breach of French law.

This finding against Yahoo France itself raises broader questions. As Yahoo France and Yahoo Inc (US) are separate entities, carrying on independent businesses although with a shared name, on what basis could the former be required to warn about material on the latter? Would the decision have been the same for any internet search engine and any internet portal which provided users in France with links to the Yahoo Inc (US) site, or did the name 'Yahoo' give Yahoo France an apparent connection which led to greater responsibility? These issues were not specifically discussed in the Court's judgment, but it appears that the Court's concern was the *link* which enabled users of Yahoo France to directly access Yahoo Inc (US), rather than any business connection between the two defendants. It happened in this case that Yahoo Inc (US) and Yahoo France were both before the Court as defendants, but it appears, although it is not stated, that any portal or site providing direct links to a site such as Yahoo Inc (US) would be in the same position as Yahoo France. Presumably then, search engines which find and display links to sites such as Yahoo Inc would be in the same position, as once their search results are displayed the links available are equivalent to those on portals such as Yahoo France. This was not however discussed by the Court.

4.2 The Decisions Against Yahoo Inc (US)

In the first hearing of the case of *LICRA et UEJF vs Yahoo! Inc and Yahoo France*, Yahoo Inc (US) raised three main grounds of defence:

- Firstly, it disputed the jurisdiction of the French Court, claiming that the action complained of was committed on the territory of the United States, and could not therefore be in breach of the French Penal Codes.

- Secondly Yahoo Inc (US) argued that such a ruling would be contrary to the 1st Amendment of the US Constitution, and that Yahoo Inc (US) could not therefore comply with it.

- Thirdly Yahoo Inc (US) claimed that it would be technically impossible to comply with the orders requested by the plaintiffs, as Yahoo would be unable to identify which visits to the Yahoo US site were initiated in France.

The Superior Court of Paris was not persuaded by any of these arguments. On the issue of jurisdiction, the Court held that although the action of Yahoo Inc (US) in placing this material on a server occurred in the US, by:

> 'permitting the visualization *in France* of these objects, and [permitting] the participation of a surfer *in France* in such an exposition/sale, Yahoo! Inc thus

> has committed a wrong on the territory of France',

and the matter was therefore within the competence of the Court. It was irrelevant to the French Court that no breach of US law was involved. The material in question, while entirely legal in the USA where it was hosted, was accessible in France and contravened French law. In the November decision the Court went a step further, noting that although the offending material was not principally aimed at French internet users:

> 'Yahoo is aware that it is addressing French parties… [and] a sufficient basis is thus established…for a connecting link with France, which renders our jurisdiction perfectly competent to rule in this matter'.

The First Amendment issue was treated by the French Court as something of a furphy. The text of the First Amendment to the US Constitution - 'Congress shall make no law … abridging the freedom of speech' - places the burden on government to justify its encroachments on free expression.

It is concerned only with governmental interference with speech, and does not place requirements on individuals or companies such as Yahoo. The Court pointed out that in many areas Yahoo Inc (US) made selective choices about what material to carry or refuse to carry; it did not see itself bound for instance to carry on its auction sites live animals, human organs or drugs.There was nothing in the US Constitution to stop Yahoo Inc (US) from blocking Nazi material.

As for technical difficulties, the Court in its original decision found that the obstacles to identifying the geographical location of users and blocking their access to certain content were real but not insurmountable. Yahoo Inc (US) was therefore ordered to:

> 'take such measures as will dissuade and render impossible any and all consultation on Yahoo.Com of the auction service for Nazi objects…'.

However, due to technical concerns, Yahoo was given two months grace to make arrangements to carry out the court order, and to report back to the Court on the measures it intended to implement.

The parties returned to court in July 2000. The applicants sought enforcement of the Court's May decision, while Yahoo Inc (US) claimed that it was not technically feasible to block French web users from accessing its site. The Court, dissatisfied with this response from Yahoo Inc (US), appointed a panel of international experts to make a technical assessment of the claims of Yahoo Inc (US), and to identify ways in which Yahoo could screen out visits initiated in France.

Unfortunately for Yahoo, the experts advised that currently available technology would allow Yahoo Inc (US) to carry out the Court's order, and on November 20th 2000 the Court confirmed the rulings made in May. That is, it ordered that Yahoo Inc (US) to:

> '…take all necessary measures to dissuade and make impossible any access via

> Yahoo.com to the auction service for Nazi merchandise as well as to any other site or service that may be construed as an apology for Nazism or contesting the reality of Nazi crimes'.

4.3 Criticisms of the Judgments in LICRA et UEJF vs Yahoo! Inc and Yahoo France

There have been many criticisms made of this case on many different grounds. These include claims that screening and blocking won't work and can be circumvented, that encouraging methods of screening internet material along geographical lines will assist totalitarian governments and encourage others to censor content, that such decisions will change for the worse the nature of the internet, that no government should impose its will on those outside it's own territory, and that there is no way of enforcing the judgment. It is worth examining each of these issues.

4.3.1 Technology

The French ruling has been criticized on the basis that the internet is not technologically susceptible to the imposition of censorship. The newness of the medium, combined with the apparent impossibility of effectively regulating internet content, have indeed meant that very little content regulation has been attempted so far. However, the experts' report commissioned for the French court suggests internet censorship may be more possible than previously thought as there is now technology available to assist, albeit imperfectly, in differentiating the geographic location of internet users, and in filtering content.

Whenever there is talk of restrictions on internet content, issues of technology are critical. The internet, developed initially for defence purposes, was specifically designed to overcome interruptions, and to circumvent broken links. The claim that when one route was blocked a message would re-route and re-route, indefinitely, until the message reached its intended destination, has been used repeatedly to argue that intervention in internet communications is impossible, or at the least, impractical. Initial design made censorship difficult, but later developments have continued along that path. It is possible for example:

> 'to disguise the origin of material… or permit the origin to change location within seconds… material is easily encrypted making it difficult to discern the content of files, even if intercepted… tunneling technologies are well established and freely available [which permit] the circumvention of proxy filters…'.

Advice to the Australian government prior to the enactment of the *Broadcasting Services Amendment (Online Services) Act 1999* (Cth) concluded that 'content blocking implemented purely by technical means will be ineffective…'.

However, the internet which courts and governments now seek to regulate is not the same as it initially was. Both software and hardware have developed considerably, and there are many more techniques now available for preventing access.

In response to Yahoo's claim that French users could not be stopped from accessing its US web auction sites advertising Nazi material, the international panel of experts found that this could be done, possibly with up to 90% accuracy. A number of technological advances have made this possible. Firstly, the geographical location of internet users could be determined by IP address.

> 'It may be estimated in practice that over 70% of the IP addresses of surfers residing in French territory can be identified as being French',

the other 30% being those who connected through ISPs outside France, who connected via their own large corporations rather than ISPs, those using ISPs such as AOL (all AOL users are allocated local Virginian IP addresses as AOL is located in Virginia), and those using anonymiser services. The Court noted that Yahoo Inc (US) already used the technology available to identify user's geographical locations, to enable it to target advertising and display advertising banners in French.

The experts suggested that this identification of geographical location could then be combined with a declaration of nationality. Users could be asked either upon entering the site, or upon searching for Nazi-related items, to declare their nationality. This information could then be stored as a cookie to be read each time the site was accessed or a search performed.

The experts reported that 'the culmination of the two procedures', namely geographical identification of the IP address and declaration of nationality would be likely to achieve a filtering success rate approaching 90%. Once a user was identified as being French, or within French territory, keyword filtering could be used to stop access to offending material, from either search requests or search results.

The various methods of screening and blocking suggested by the Court and by the consultants have been criticized as both over-inclusive and under-inclusive. For example, IP addresses can be disguised and anonomysed, and those within France can use ISPs outside France, albeit at the cost of a long distance call. Screening those using French language browsers would likely also screen many people outside France. Even the Court's suggestion that those whose geographical location was unclear be required to declare their location could be circumvented by users simply lying. On top of these problems come difficulties of blocking content itself.

Once a user in France was identified it would be necessary to ensure that he or she could not access content prohibited in France. While this may be achieved by blocking access to the whole Yahoo Inc (US) site, or parts of the site, it is likely also to deny access to material not prohibited in France. More specific blocking would require Yahoo Inc (US) to monitor the user's request, or monitor responses to those requests, and to use content filters to block offending material. However, content filters themselves create real problems. While the French Court accepted that keyword filtering may be appropriate, blocking material which included words such as Nazi and Hitler would only block information actually including or described in these terms, and is likely also to block

considerable non-offending content, such as historical material.

4.3.2 Encouraging Censorship by Repressive (and Not So Repressive) Regimes

While it may by *possible* to block access to particular sites by particular groups of people, there is concern that the use of such blocking technology should not be encouraged or publicized, as the more readily available it is, the more use will be made of it by repressive regimes, to stop their citizens accessing political and other information unfavourable to government. It is said that the results of the French case could be to hand to:

> 'authoritarian governments the tools they need to censor the internet…'.

Realistically however, not using this technology in France and the USA doesn't make it less likely that it will be used by more repressive regimes. Indeed, a number of countries *are* already attempting to censor unwanted material, but who is to say which countries should and shouldn't have the technology to do so? Further, like other industries the internet industry is commercially driven, and the required technology and expertise will be available to these countries anyway - at a price. In fact, US companies already assist the Chinese government for example to filter unwanted internet content coming from outside the country.

Such nations are already able to restrict access to internet material, by making computers and internet connections available only to a chosen few, through strict licensing of ISPs, by allowing very few international connections, and by monitoring the material passing through those. While the availability of new technologies may make that control easier, the control is already being exercised one way or another.

On the other hand, easier methods of controlling internet content may be attractive to nations which do not currently seek such control, or which have sought such control but been put-off by its difficulty. In Australia for example, legislation initially proposed that ISPs notified of prohibited content must take:

> 'all reasonable steps to prevent end users from accessing that content'.

However, an acceptance of the difficulty of so preventing end users from accessing material led to the amendment of the Bill, and later to the ABA's registering an industry code which very much watered-down the original requirements. The code relieves ISPs of the requirement of preventing access where they make filter products or filtered services available to their clients. It may be anticipated however that if easier methods of access prevention become available, countries such as Australia may seek to introduce more onerous access prevention requirements.

4.3.3 Internet Content Ought Not Be Censored

Many net users have valued highly the internet's anarchic and unregulated nature. The internet was one place where freedom of information could be assured, and not only the

freedom to receive information but also to respond to it, and to add more. Once regulated,

> 'the virtual world would soon start to look much like the real one, stuffed as it is with borders and regulations…these legal and technical efforts could erode the very thing that has made the Internet so successful: the free flow of information'.

Content regulation, or censorship, may make a real difference from a user's point of view; if the regulation is effective users may be unable to access material they wish to access. But this is reality in every other medium, and far from introducing new restrictions, such regulations will likely just bring the internet more into line with other available media. However, this is the very argument of many internet users; the internet is something different from all other media, and should be treated as such. It is not pervasive like TV and radio, it is not public like the cinema. No-one is forced to 'tune in.' It is a different medium and should not be brought into line with other non-comparable media. It is disorganized and ad hoc, it offers great opportunities for making connections locally and globally, it does not have a hierarchical format and so users are as free to contribute and respond to what is on the net as they are to receive it. Further, although parts of the internet are commercially oriented, it is still brimming with non-commercial material not constrained by market forces. Anything can be published on the internet. Many users fear that the whole internet experience will change with regulation.

4.3.4 The Internet Ought Not Be Governed By National Laws

The decision in *LICRA et UEJF vs Yahoo! Inc and Yahoo France* has been criticized on the basis that no nation should impose its views or laws on those outside its borders. The material in question in this case clearly did not fall foul of US law, and Yahoo Inc's actions were perfectly legal where they were initiated. It is clear however in this case that the French judgment is concerned only with what occurs within France. Although the plaintiffs in *LICRA et UEJF vs Yahoo! Inc and Yahoo France* did ask the Court to order Yahoo Inc:

> 'to destroy any and all computer information held directly or indirectly on its server…',

the Court confined its orders to what occurred in France, and did not make the additional order requested. However, while the French ruling did not attempt to regulate or censor Yahoo Inc (US) content outside France, this type of content regulation within France would require action outside the territory.

It is in the nature of the internet that action occurring anywhere in the world can have effects anywhere else in the world, and this is likely to lead to recurring problems concerning jurisdiction. Material placed on servers in the USA can be viewed in France, and it is this ability to view which the French Court is concerned with. While the practical effect of the judgment may be that something needs to be done outside France, that is a side effect of the judgment; it is not an end in itself. In this respect the suggestion that France intends to act extra-territorially is wrong. The French Court is making a judgment not about the act which occurs in the USA, but about the repercussions of that act which

occur in France, and which could occur anywhere. While it may be arguable that France should not have any say over the actions of those in the USA, should not France have a say over what occurs within France, even as a result of actions occurring in the USA or elsewhere? This is the very dilemma of attempts to assert national control over internet content.

There is no reason in principle that individual nations should not attempt to regulate internet content. Every other industry is subject to some regulation, both in their home country and in the countries in which they do business. No-one would suggest that Toyota cars built in Japan but sold in Australia should not be subject to Australian safety laws because Toyota is a Japanese company, nor that Coca Cola should not be subject to Australian advertising standards for sales in Australia because Coca Cola is an American company.

On the other hand however, no-one would expect Toyota to meet Australian safety standards just in case one of their cars came into Australia, nor that Coca Cola should advertise to Australian standards just in case someone in Australia is picking up US television via satellite. The French Court accepted that Yahoo's auction site was not *principally directed* at French web surfers, but found also that Yahoo was aware that French surfers were accessing the site:

> 'because upon making a connection to its auctions site from a terminal located in France it responds by transmitting advertising banners written in the French language'.

This may suggest that Yahoo's awareness of French surfers placed upon it a greater responsibility to comply with French law. It is unclear however whether the decision would have been different if Yahoo were not aware of, or made no effort to identify, French surfers. The May decision asserted that it was sufficient for jurisdiction that French surfers could access in France material illegal in France, but in the November decision Yahoo's knowledge of French surfers was said to give it an even closer jurisdictional link. This raises the question of when and in what circumstances an internet service provider or internet content host will be held responsible for applying censorship or content regulation; whether knowledge will be required, or whether the mere possibility of access will suffice for assertions of liability.

For the internet industry, which in many jurisdictions has thus far enjoyed virtual freedom from restriction, acting to give effect to national regulation of internet content would be difficult and costly. It is suggested that the French ruling:

> 'could embolden other countries to try to impose their laws on foreign web services…[Firms] worry that they might have to re-program their sites to comply with many different jurisdictions - and in the process get snarled by conflicting national laws'.

Complying with myriad laws would certainly push up the industry's costs. Moreover,

there is the concern that if the industry did try to comply with all national laws, material available on the internet would be only that of 'the lowest common denominator.'

One alternative would be to configure services based on laws of individual nations, which would be at huge cost, create considerable complexity, and destroy the seamless nature of the web. Allowing users to see only what their country wanted them to see would in effect 'zone' the internet; users would then see the French web, the Japanese web, the Australian web and so on. Another alternative may be the creation of one or a number of international standards by agreement between nations, depending on what content the various nations were interested in regulating or restricting.

4.3.5 Enforcing the Judgment

Another criticism of the French Court's judgment is that it may be unenforceable against defendants outside the jurisdiction. The most widely accepted basis for the exercise of criminal jurisdiction is territoriality, but states may also assert jurisdiction, as in this case, where the effects of the alleged criminal act are felt within the territory, although the commission of the offence occurs elsewhere. However, while a court may *assert* criminal jurisdiction, unless a defendant comes into or voluntarily submits to the jurisdiction, an extradition agreement would be required to bring the defendant into the jurisdiction for trial or punishment. Even where such agreements exist, extradition is commonly only allowed where the activity giving rise to the charge is illegal in both states. Generally then the reach of a nation's criminal law in relation to internet content provided, hosted or transmitted by those outside its territory, will be minimal. As a result, some states are now attempting to negotiate agreements regarding the establishment of uniform internet content related criminal offences, to make prosecution for specified activities easier at least in signatory states.

Pursuant to the ruling in *LICRA et UEJF vs Yahoo! Inc and Yahoo France*, Yahoo Inc (US) pre-empted any attempt to have the French judgment enforced against it, by itself filing suit in the Federal District Court in San Jose California, asking that Court to declare the French ruling unenforceable. Furthermore, without waiting for a decision in that case, Yahoo Inc (US) announced that it will attempt to screen and eliminate hateful and racist material such as Nazi memorabilia and Klu Klux Klan objects from its auctions sites. It will not interfere however with non-commercial material in chat rooms, personal web sites and youth clubs which it hosts. Yahoo officials asserted that the new monitoring scheme:

> 'had nothing to do with the actions of Judge Gomez, but rather were part of a general housecleaning of its auction policy and the result of ongoing discussions with Jewish groups in the United States'.

However, as Yahoo Inc (US) was ordered to:

> '…take all necessary measures to dissuade and make impossible any access via Yahoo.com to the auction service for Nazi merchandise *as well as* to any other site or service that may be construed as an apology for Nazism or contesting the

reality of Nazi crimes',

the outcome of Yahoo's request for a declaration that the judgment is unenforceable in the US remains important. The French decision requires more of Yahoo Inc (US) than simply ceasing to host 'Nazi auctions'.

5. Implications

It appears clear from the experts' report in *LICRA et UEJF vs Yahoo! Inc and Yahoo France* that even if Yahoo Inc (US) does try to block access to offending sites, French users who wish to access these sites will still be able to do so, and France will be unable to stop them. However, the decision sends important messages. It tells the internet industry that France wants and intends to claim sovereignty over what occurs in France, and will not be put-off enforcing its own laws by claims of technological difficulties. It appears also that the French Court is happy to make such judgments despite both jurisdictional and technological problems. The lengths the Court went to investigate technical solutions evidence the Court's desire that the decision be more that symbolic; symbolic decisions require no technical backup.

The Australian legislation on the other hand was said to be the embodiment of symbolic politics, the government knew the legislation couldn't work but wanted anyhow to be seen to act. While the Australian legislation sets strict controls for internet content hosts within its jurisdiction, it makes no attempt to influence those outside, even where their material is being accessed within Australia. It enables take-down notices to be issued only for content hosted within Australia, and notifies only Australian ISPs of prohibited content. The Internet Industry Code of Practice requires ISPs to make content filters or filtered services available to subscribers, but there is no requirement that these filters be used. While some content hosts within Australia may be required under the legislation to remove material, there is nothing to stop them hosting the same material overseas, but equally accessible to Australian internet users who choose not to use content filters. Like the French decision, the Australian legislation has little practical effect on internet content presently; those wishing to access pornography from Australia, or sites contesting the reality of Nazi crimes from France, can still do so.

However, the Australian legislation and the French decision, while practically ineffective, may not be meaningless. They may rather be indicative of an increasing willingness to attempt to assert some kind of sovereign control over internet content. It seems likely that as more countries try to assert control over more aspects of the internet, the chances increase of international agreements arising, allowing the development of international or at least multi-national standards to be set, and/or allowing enforcement of internet-related judgments across jurisdictions. Such agreements, when coupled with constant technological developments in the ability to screen, monitor and block internet access and content, could initiate real shifts in internet industry regulation and responsibility.

Two considerations must however be borne in mind. Firstly, the USA is by far the largest provider of internet content, and is also the most protective of freedom of speech. It is therefore the country least likely to be willing to be involved in enforcing decisions or

entering agreements aimed at censoring internet content, but the most needed party if such agreements are to be meaningful.

Secondly, it may be impossible to reach any useful level of agreement (even absenting the USA), when various nations wish to censor or regulate such different aspects of internet content. For example,

> 'what constitutes 'political speech' in the United States (Nazi speech) is banned in Germany; what constitutes 'obscene speech' in Tennessee is permitted in Holland; …what is harmful to minors in Bavaria is Disney in New York'.

Some nations may be willing at least to identify matters of common ground and work toward agreements on those. Negotiations on such topics are already taking place, and the Council of Europe for example has already released a draft Convention on Cyber-Crime. However, even nations with seemingly similar views on censorship may disagree on the detail, and agreements are likely therefore only to cover the less controversial aspects of content regulation. Co-operation such as the monitoring and policing of internet material carried out by INHOPE members may be possible where material is clearly recognized by all involved as illegal or harmful, but where there is any question about the categorization of that material, such co-operation is less likely.

With various nations taking such broadly varying views on what censorship or regulation is desirable, it seems almost impossible that any global agreement could be made, and with the global nature of the internet, non-global agreements may be of little assistance. In fact, attempts by individual nations or even groups of nations to control internet content may only lead to material being moved, and hosted in less restrictive jurisdictions. Nations wishing for greater censorship or regulation could block material originating in such jurisdictions, but if such jurisdictions included, for example, the United States, it is unlikely that any western nation would be willing to entirely block content hosted there.

6. Conclusion

Many issues still require resolution before any widespread and useful agreements could be made relating to the regulation of internet content. However, the decision of the French Court and the enactment of Australian legislation may be seen as incremental steps toward assertions of sovereignty over internet content. Already Germany appears to be following the same path as France, with a ruling that an Australian, making holocaust denial literature available from an internet server in Australia, is subject to and should be tried under German law. None of these actions may be practically useful in isolation, in that they are attempts to control local access to internet content, but attempts which, alone, are unlikely to achieve their aims. However, they may all be useful as signs to the internet community, and to other nations, of a desire to control internet content and of a willingness to take bold actions to this end. This may encourage other nations to try to control internet content, and give impetus to negotiations aimed at co-operation in this sphere. It is likely that such co-operation will be the only way for governments to achieve any real control over internet content.