http://go.warwick.ac.uk/jilt/2007_2/george_scerri

Journal of Information, Law and Technology

Web 2.0 and User-Generated Content: legal challenges in the new frontier[1]

Dr Carlisle George
Senior Lecturer & Barrister, School of Computing Science
Middlesex University
Email: c.george@mdx.ac.uk

Dr Jackie Scerri
Attorney-at-Law
WH Law Advocates, MALTA
Email: jackiescerri@gmail.com

Abstract

The advent of Web 2.0 has enabled a host of new services and possibilities on the Internet. Among many new possibilities, users can easily upload online content that can be accessed, viewed and downloaded by other users around the globe. This has resulted in an explosive growth of User-Generated Content (UGC) which although creating exciting opportunities for users, presents many challenges, especially related to law and regulation. This paper discusses Web 2.0, UGC and the legal /regulatory challenges that have arisen in this new 'frontier' characterised by having a liberating democratic ethos (on one hand) but also sometimes tainted with illegal activity and disregard for accepted norms. Citing various researched case studies and legal cases, the paper highlights possible 'dangers' where traditional legal rules may be inadequate to address certain types of online activity, and discusses many of the legal challenges which this new frontier brings. These challenges are widespread and relate to intellectual property, liability, defamation, pornography, hate speech, privacy, confidentiality and jurisdiction among others. The paper also discusses the role of intermediaries (web hosts and service providers) and whether they can aid in effectively policing the new Web 2.0 frontier. Finally the paper attempts to discuss possible solutions for the way forward.

Keywords: Web 2.0, Internet, User Generated Content, Legal Rules, Protection

1. Introduction

User-generated content (UGC) exists in a large variety of forms (such as photographs, videos, podcasts, articles and blogs) allowing users to express their creativity and register their comments on anything imaginable. This has resulted in users gaining unprecedented power (in a virtual environment) to initiate and influence change on various social, cultural, political and economic issues in the non-virtual world. Examples of the extent of the power of these citizens include, ousting a sex predator from public office, exposing inappropriate behaviour resulting in election defeat, influencing musical and artistic tastes, detailing first-hand accounts of war, influencing book readers on a national scale, and creating global celebrities. This power appears to emanate from a ground swell of popular culture rooted in the western democratic value of free speech/expression, together with the decline of trust in traditional organisations (such as established media) and institutions of governance. TIME magazine's edition of January 1st 2007, profiles many citizens of this new digital democracy including a whistle-blogger, web-artist, social-networker, military-blogger, web-chef, book critic, web-celebrity, 'Intertainer', and Wikipedia author among others.

This paper examines the development and use of UGC and this new 'virtual community', with a view to analysing the legal challenges that currently arise, or may arise in the future. The paper begins with a background to the environment (Web 2.0) that has facilitated the widespread use of UGC. It then examines into greater detail what UGC is and attempts to give a taxonomy of UGC, classifying types of content and the intended purpose of such content. Next the paper examines the general regulatory framework for such content. This is followed by a discussion of some of the legal challenges that UGC bring to the law and to Internet Service Providers (ISPs). The paper then discusses whether some parts of the new digital democracy may be akin to the Wild West, where online users in pursuant of personal, political

or economic agendas freely roam cyberspace, unfettered with disregard for law and regulation. The paper finally concludes with recommendations for the way forward.

2. WEB 2.0

The term "Web 2.0" originated from Media Inc owned by Tim O'Reilly[2] in 2004, and is used to convey a set of principles and practices that describe a second generation (from the traditional Web 1.0) of web services mainly concerned with user collaboration and sharing. Tim O'Reilly's compact definition of Web 2.0 is as follows:

> "Web 2.0 is the network as platform, spanning all connected devices; Web 2.0 applications are those that make the most of the intrinsic advantages of that platform: delivering software as a continually-updated service that gets better the more people use it, consuming and remixing data from multiple sources, including individual users, while providing their own data and services in a form that allows remixing by others, creating network effects through an "architecture of participation," and going beyond the page metaphor of Web 1.0 to deliver rich user experiences."[3]

The original idea behind Web 2.0 consisted of various principles and core competencies that encapsulate the ethos of this new phenomenon[4]. These include:

- The Web as platform. The web is used for the distribution of services and also for harnessing the collective power of users. For example, P2P software providers like BitTorrent makes every client a server, and files are split into fragments to enable them to be served from multiple locations. As the number of users increase, the quality of the service improves. Every new BitTorrent user adds a new resource to the existing network increasing its capability. Popular files are located and downloaded faster the unpopular files. Hence an "architecture of participation" is implicitly formed, where users cooperate and collaborate. This is contrasted with a company that needs to add servers to improve its web service.
- Provision of services (not packaged software) with cost effective scalability. For example, Google's service has no software licensing, sale or scheduled release, just usage and continuous improvement.
- Control over unique, hard-to-create data sources that get richer as more people use them. For example, Amazon enhances basic data on books (provided by an ISBN registry) with publisher supplied material such as cover images, table of contents, index, and sample contents. They also claim ownership of user reviews. Amazon is now the primary source of bibliographic data on books and they have their own book identifier called the ASIN (corresponding to the ISBN).
- Trusting users as co-developers. Using open source development practices, products are developed and continually improved sometimes on a daily basis. For example while Microsoft makes an upgrade every two to three years, Google is continually upgraded based on the activity of users. Also Wikipedia software allows users to continually develop its content[5] which at the time of writing (April 2007) consists of over 7million entries in 251 languages[6].
- Harnessing collective intelligence. Examples include: Amazon's use of user reviews to enhance the buying process or user search activity to produce better results; Wikipedia's repository of information which allows web users to make entries and hence contribute to a body of knowledge which can be accessed and shared globally; Blogging and the presence of a "blogosphere" linking blogs.

- Software above the level of a single device. Services are not limited to the PC, but extend to handheld devices. Examples include: the iPod/iTunes combination, and TiVo[7].
- Lightweight user interfaces, development models and business models. Lightweight programming models enable simplicity and reuse (part of the Web 2.0 mindset). They should support loosely (rather than tight) coupled systems; syndication[8] (rather then coordination); and 'hackability' and 'remixability'.

Traditional Web 2.0 services include "blogs, wikis, multimedia sharing services, content syndication, podcasting and content tagging services."[9] A blog is a personal webpage where a user/blogger posts content such as opinions, commentaries and personal diary information usually arranged chronologically[10]. Usually visitors to blogs can also comment on blog entries. Wikis are webpages that allow users to contribute and edit content hence making a group contribution (e.g. Wikipedia)[11]. Wikis (unlike blogs) have a history function and enables previous versions of edited content to be examined and restored. Multimedia sharing services enable storage and sharing of multimedia content such as photographs (e.g. Flickr), video (e.g. YouTube, MySpace) and podcasts (e.g. Odeo)[12]. Content syndication refers to the process whereby content from one website (e.g. a news headline) is collected within a feed (i.e. usually facilitated by use of an XML application RSS 2.0 which allows bits of content to be placed into a simple text file) which can then be read (at specific intervals) by other websites or reader programs. Podcasting refers to the audio recordings in MP3 format (e.g. interviews, lectures) which are accessed via the web and played on computers or handheld MP3 devices[13]. Tagging services (e.g. Del.icio.us) allow keywords to be added to a digital object such as a website or photo. Users can create and store (on a remote server rather than on the client browser) lists of tags, which can be shared with other users[14]. Content can be tagged in different categories hence adding a rich and varied categorisation and organisation of digital objects.

Newer Web 2.0 services include[15]: social networking (e.g. www.flock.com) and professional networking (e.g. www.linkedin.com); aggregation services (bringing all feeds, news and email to a single web page, e.g. www.techmeme.com), data 'mash-ups' (putting together data from difference sources to create a new service, e.g. www.housingmaps.com), tracking and filtering content (tracks and filters content from blogs and other sharing services, e.g. www.digg.com), collaborating (collaborative reference works e.g. www.squidoo.com); Web-based desktop application/document tools (e.g. www.stikkit.com); and sourcing ideas or working from a crowd (using the power of the crowd, e.g. www.innocentive.com).

The philosophy of Web 2.0 focuses on activities such as collaboration, cooperation, interactivity and social networking. Central to participation in the Web 2.0 phenomenon is the user as publisher, critic, journalist, reviewer, public performer and broadcaster (among others), heralding the power and influence of UGC.

3. User-Generated Content (UGC)

Online UGC content can be distinguished from 'engineered' content generated by a content provider (not an ordinary Internet user) such as an established authority, knowledgeable expert or reputable body[16]. Engineered content usually has a high level of oversight and quality control and is generally considered to be more reliable and credible, with less author bias[17]. UGC exists in many forms including text-based UGC (e.g. web blogs), graphics-based UGC (e.g. Photos, illustrations), audio UGC (podcasts) and video UGC. Some of the many reasons why users generate content include:

- Advertising – e.g. Craigslist[18] allows users to place fee classified advertising online.

- Analysis & Commentary – many bloggers give opinions, analysis and comments on social, technical, economic, religious and political issues amongst others, e.g. Lessig Blog maintained by the well known Professor Lawrence Lessig[19].
- Contribution to human knowledge - e.g. users edit or create articles on Wikipedia[20] hence contributing to the body of human knowledge.
- Criticism & Review – users make voluntary contributions to online reviews of books (e.g. Amazon reviews[21]), products (e.g. user opinions) and services (e.g. travellers' comments on hotels).
- Entertainment – users post a variety of personal videos online (on MySpace, YouTube etc) to amuse and entertain other users.
- Education/support – some users offer content for educational purposes, e.g. web forums where users give advice and support to other users, such as the Atkins dieters'[22] forum.
- Malicious Intent – some UGC are generated for malicious intent. Examples include: videos hosted on MySpace that install adware on a viewer's computer when played[23], cyberbulling of a US blogger Kathy Sierra via death threats comments on her blog[24], and online posting of nude photos of the celebrity Jennifer Aniston[25].
- News reporting – many users post amateur news (video) footage which major networks may not show due to public broadcasting guidelines. A noted example is a video showing the execution of Saddam Hussein[26] that appeared on YouTube before major networks were able to show a sanitised version of it. Other examples are videos of beheadings or public officials caught in questionable acts.
- Photo Sharing – e.g. Flickr[27] allows users to store, search, sort and share photos.
- Political Campaigning – e.g. in April 2007 the UK Labour Party launched its YouTube video channel.
- Protest – e.g. as a protest against the Iraq war, Julia Wilson of California posted content on MySpace showing a photo of the American Present being stabbed in the hand, together with comments on the photo that incite hatred. This resulted in a visit from the US Secret Service[28].
- Social Networking – e.g. Bebo[29] allows users to network and communicate.
- Vigilantism – many users post content online to settle disputes or to get justice, e.g. when a San Francisco radio aired comments which were considered to be violent, racially offensive and insensitive to religious groups, bloggers documented the audio clips online resulting in a boycott of the station by some advertisers[30].

4. Legal Concerns

The phenomenon of UGC has brought many benefits to society, however, it has also brought many challenges and concerns for the law. These challenges are widespread and are seen from the multiplicity of news reports, and cases that highlight various questionable user behaviour and practices. Some of these practices are evidently illegal, others border on legality, yet others are undesirable or morally indefensible. Many of the challenges for the law relate to intellectual property, privacy/confidentiality, hate speech, defamation, pornography, undesirable content and jurisdiction among others. These issues are further explored in the following subsections.

4.1 Intellectual Property

One of the most controversial issues in the growth of UGC is that relating to intellectual property ownership, especially copyright[31]. Web 2.0 (which has facilitated easily uploading of UGC) is a field of gold for amateur artists (who can use this medium to distribute their art) and ordinary users who are motivated to post some form of content online. While the idea of Web 2.0 is to allow users to publish their own material online, many users publish material belonging to other authors (either in their original form or in an adapted form) thus infringing

copyright. Postings of the entire or excerpts of musical and literary works, photographs, paintings, videos, and other types of copyrighted works have become the norm as users have little regard for copyright laws. It is therefore only natural that copyright owners are outraged by behaviour of copyright infringers; for example in January 2007, DMCA[32] take down notices were served on YouTube (by Viacom[33]) for over 100,000 works posted on the YouTube site.[34] Further in March 2007, Viacom sued YouTube for US$1 Billion alleging that YouTube were aiding copyright infringers[35]. There are many similar ongoing lawsuits taking place at the time on writing[36]. In a lawsuit filed by Universal against MySpace in November 2006 (*UMG Recordings Inc et al v. MySpace Inc.*,) Universal alleged that MySpace had made infringement 'free and easy,' and 'had turned MySpace Videos into 'a vast virtual warehouse for pirated copies of music videos and songs'.

It is pertinent to ask about the status of "original" material posted on UGC websites by users. Most websites hosting this kind of content tend to clearly state within their terms and conditions that such material belongs to the user. For example YouTube, states that **'***For clarity, you retain all of your ownership rights in your User Submissions*'**.**[37] However, a posting on any of these sites is likely to be used and re-used by other users without any form of control. In fact, there may even be arguments to the effect that by submitting one's material to such sites, the user is giving an implied licence for his/her work to be used in this way.

4.2 Privacy

The publishing of content without control and verification means that many users can post material that is an invasion of the privacy of others. The majority of content falling into this category are the famous homemade sex videos (or sex photos), usually of celebrities, but also of ordinary citizens (especially by former lovers seeking to address a grievance). When such content is posted online it is difficult to ascertain whether the subject of the content has agreed to publication and also who owns the copyright in the content. Further it is sometimes impossible to stop the spread of such content which can be easily downloaded and distributed in other ways such as via peer-to-peer networks or email. For example in January 2007, a court in Brazil ordered that YouTube be 'shut down' until it has taken down a celebrity tape featuring the model and ex-wife of the Brazilian footballer Ronaldo having sex on a beach with her boyfriend[38]. Privacy is also a concern when ordinary citizens become popular public personalities through the success of their UGC (blogs, videos etc) and attract unwanted attention. For example in 2006 a popular YouTube personality in Australia, decided to remove all her video blog entries on YouTube after stalkers hacked into her personal computer and copied private information which was then posted online hence invading here privacy[39]. Another area of privacy concern is in social networking websites such as Facebook, where users (especially students) create profiles of themselves which can contain personally identifiable information that may be used for identify theft, stalking or other harmful intentions[40]. It appears, however, that many users may not fully appreciate the harmful effects of privacy invasion. A 2005 study of US college students at Carnegie Mellon University found that although students were aware of the potential dangers of making personally identifiable information public to the University population, many of them were comfortable providing it[41]. The increasing presence of personal information online may lead to an increase in activities such as identity theft and privacy invasions.

4.3 Hate Speech

The advent of UGC has also seen a lack of control over hate speech. Hate speech is any, content which deliberately offends an individual (or a racial, ethnic, or religious group) by reason of their nationality, gender, sexual tendencies, appearance or other such attributes[42]. One particularly unequivocal example is found on a website named 'God, I hate Arabs' and

amongst other things elucidates as follows: '*Have you ever seen an Arab smile? I sure haven't. They sneer, scowl, frown, and generally look menacing and threatening. To be honest, they have no place in a civilized Western country'*.[43] This website is freely available and accessible online for users who wish to view the content or add to it. Many other websites containing offensive material especially relating to race and religion are easily accessible[44]. In the future, as more conflicts arise between groups, the Internet may be increasingly used to spread hateful information and to air grievances.

4.4 Defamation

A statement is defamatory if it causes injury to the reputation of a person. Web 2.0 has increased the ease of publishing defamatory material with the ease of uploading content, blogging and publishing content online. Hence anyone is now able to use a virtual pen to write untrue or injurious material for online consumption. Wikipedia, the open source online encyclopedia which allows users to add to its content, has been involved in a number of situations involving defamation. One recent case involved a professional golfer, Fuzzy Zoeller, who instituted action against the alleged author of an edit to his Wikipedia biography[45]. The edit portrayed Zoeller as a drug addict and alcoholic who abused his family when under the influence of these substances. Another case involved John Seigenthaler Sr., (former assistant to Attorney General Robert Kennedy) whose Wikipedia biography stated that 'for a brief time, he was thought to have been directly involved in the Kennedy assassinations of both John, and his brother, Bobby. Nothing was ever proven'.[46] Yet in another case Skutt High School in Nebraska, USA, was the victim of malicious entries on Wikipedia when the posting for this school mentioned drug use amongst students, and contained harmful comments about the principal. Finally, in 2006, Mumsnet, a site offering advice and support to pregnant and new mothers, was threatened with legal action by Gina Ford (an author of childcare books) due to discussions about her books on this site, which Ford claimed amounted to defamation. In response, Mumsnet published a statement asking its users not to discuss the author.[47]

4.5 Pornography

Another major concern on sites allowing users to upload content is pornography. The possibility of monitoring what children can view on the Internet has become an impossible task. Before Web2.0, it may have been possible to block out pornographic material originating from Adult-Only sites; however, pornographic material can be easily uploaded by anyone via sites allowing UGC. This means that it is equally readily available through such sites to anyone, anytime and anywhere, without the requirement of age or identity verification. As an example, YouTube, a site which is supposedly targeted at 'family entertainment', and which is possibly one of the most popular sites amongst youths, hosts a large variety of unsupervised and unedited pornographic material (including fetish videos).[48] Pornography is also easily accessible via video blogs and UGC sites (e.g. YouPorn) which cater exclusively for pornographic content. The instinctive human attraction and curiosity that sexual content generates, means that in the future there will always be a demand for pornography, and hence an increase in online user generated pornographic content. A more disturbing aspect of pornography however is the increase in the availability of child pornography online[49].

4.6 Other Undesirable Content

The nature of user generated content is that is free to view by anyone. It is no longer a matter of parents blocking access to certain sites. Such content is everywhere, in blogs, message boards and the like, which cannot be controlled in the manner done beforehand. Impressionable young people have access to answers to such questions as '*What is the best way to kill yourself when you are under 13*?'[50]. The site which contains this material offers help and advice but also

some less than enlightening reply: '*duct tape a plastic bag over your head'*. CNN published an article in November 2005 with regard to parents who were blaming an online newsgroup for the suicide of their 19 year-old daughter, Suzanne Gonzales[51]. It appears that Suzanne was a member of an online newsgroup called ASH (Alt.Suicide.Holiday), which existed in order that its members could provide each other with support, advice and methods to commit suicide. The article quotes one of Suzanne's posts: '*My chosen method is potassium cyanide....I've stopped eating so my tummy will be nice and acidic*'. It also quotes her father's accusation against the newsgroup: '*The knowledge, the tools, and their psychological encouragement. ... She was led to her death*'[52]. Undesirable content includes a host of other content including: videos containing violence, suicides, beheadings; and information on illegal activities such as how to make bombs. In the future, as the number on online users increases, there will also be an increase in undesirable content, bringing more challenges to the regulators.

5. Regulation of UGC: Limitations of Law

An important concern is the effectiveness of the law in dealing with the challenges discussed above. The legal dilemmas presented by UGC are not new in the context of Internet Law, and many of the same problems are faced in other social contexts. What is new with UGC is the lack of control over the content which has lead to an increase in opportunity for illegal activities; the difficulty in monitoring and effectively policing such content; and the potential difficulty in identifying content providers. Hence there are a number of difficulties which present themselves when attempting to take legal action against publishers of UGC.

5.1 Discovering a User's Identity

Discovering the identify of an online publisher (who has committed an illegal act) can sometimes be difficult. Many people use pseudonyms when posting material on the Internet, making it hard to trace them. It is not impossible, however, to trace an online publisher, and some cases have shown that this kind of anonymity is only temporary. One such case in the UK involved the Motley Fool forum in which a certain Jeremy Benjamin had posted serious defamatory statements about Terry Smith, chief executive of Collins Stewart Tullett. Mr Benjamin had made his postings under a nickname, but Motley Fool was forced to reveal the poster's identity through a court order obtained by Mr. Smith. Mr Benjamin's IP address was consequently traced to his employees, Kyte Fund Management.[53] Mark Weston, technology law specialist at MAB[54] Law, says that '*Just as in the offline world, as long as someone knows who you are, they can be forced to reveal your identity'*. [55] However, it is submitted that this is not always the case; there may be situations where an IP address cannot be traced to an individual, such as where a person logs on using a roaming IP, or where a person logs on from an Internet Café. In the latter case, the owner of the Café will most likely not have the possibility of identifying who the user of a particular machine was at a particular time.

5.2 Jurisdiction and Applicable Law

Due to the global accessibility of UGC, legal issues regarding jurisdiction and applicable law can pose difficulties when attempting to address online illegal activity. The Internet essentially crosses traditional geographic and jurisdictional boundaries making the implementation of jurisdiction-specific laws difficult to implement. An activity which may cause one party in his/her jurisdiction to feel aggrieved may not be illegal in the other party's jurisdiction. The Brussels Regulation sets out rules for determining jurisdiction within the European Union (and a few other signatories), however, online content originating from countries that are not a party to the Brussels Regulation can pose difficulties for the law. One such example is hate speech – US law and European law differ on this issue, with the US leaning towards freedom of speech (a cornerstone of the US constitution), while European law is more restrictive. Hence a posting

which is clearly illegal under European law may not be considered illegal in a US jurisdiction. Likewise, the US concept of 'fair use' for intellectual property issues is wider than the concept of 'fair dealing' in Europe. The result with such contradictory definitions of illegality is that a person (say A) who deems himself aggrieved by another person's (say B) activities on the Internet may take action against such person B in that B's jurisdiction, only to find that the laws of B's jurisdiction state that no illegality has occurred. The aggrieved person A may of course choose to take action in his own jurisdiction, if he can claim that the effect was felt there, but he may then be faced with the impossibility of enforcing the judgment. Contradictions between laws may arise not only in substantive, but also in procedural matters: taking the above example of a court order being used to reveal identity: the circumstances under which this is issued may vary from jurisdiction to jurisdiction and a complainant in a case may find that the procedural laws in a foreign jurisdiction do not lend him a hand, leaving him without a sufficient case to be made out due, for instance, to the lack of being able to obtain evidence.

5.3 Regulation of 'Undesirable Content'

As mentioned earlier, activities on the Internet may be not be illegal but may be largely undesirable. This poses even greater difficulty, because the law can be ineffective in such cases. Yet an activity which is not illegal can still be tremendously harmful. The suicide newsgroup mentioned in Section 4.6 presents an illustration of this – it will be hard to curb these kinds of blogs by presenting them as illegal. One may possibly argue that the posting of such content amounts to aiding and abetting, or instigation to commit, a suicide. However this is a criminal offence and as such carries a high standard of proof 'beyond reasonable doubt', as well as the requisite 'mens rea'[56] on the part of the aider/instigator. Jurisdictions are likely to differ even more widely in their treatment of such a situation, and in the case of multiple postings from different users one would have to consider who is responsible for the alleged crime.

Pornographic content represents another kind of 'not illegal but undesirable' content (at least to some!). Whilst the possession and distribution of child pornography is illegal in most jurisdictions, many other types of pornography are widely accepted as not being illegal. The distribution of such material may be criminal if it is distributed to minors; however once again many hurdles exist when attempting to prove criminality since in most jurisdictions, one would need to prove that the pornography material in question corrupted an otherwise innocent minor.

Although there are other forms of Internet regulation such as social norms, code (software) and markets (price) according to Lessig's modalities of regulation[57]. These regulatory modalities are largely ineffective in many situations. Social norms are not universally shared (across jurisdictions) and can vary with culture, geographic region and customs among other factors. Software used to regulate can be subjected to hacking and circumvention. Markets as regulators can also be ineffective because UGC is based on sharing and collaboration amongst users, rather then a commercial venture.

5.4 Practical Issues in Instituting a Lawsuit

Taking legal action as a means of enforcing rights which have been allegedly infringed by UGC may involve issuing take-down notices [58] or instituting legal proceedings. The institution of proceedings is a complicated matter when it involves UGC. The difficulties outlined in Sections 5.1-5.3 indicate that legal proceedings can be a very expensive option, especially where there are multiple defendants located in different jurisdictions. The fact that a number of defamation cases have been mentioned above may appear to contradict this argument; however it is argued that in a defamation case, a complainant may have a more personal incentive to ensure that action is taken and defamation laws tend to be more clearly defined than laws dealing with the other illegal acts. Also, action will usually be taken against one specific

defendant, and if successful will have the desired result – the removal of a particular posting. This cannot be said for more general material such as pornography, for example, as the removal of one posting will not solve the problem and seems hardly worth the ordeal. With regard to copyright issues, a copyright owner may be concerned by a particular posting but may have lost track of the number of infringers which can multiply within seconds if published online.

The above considerations inevitably lead one to the conclusion that the law and other modalities of regulation may not be effective in regulating this 'Wild Web' effectively!

6. The Role of Intermediaries: Web Hosts and ISPs

Given the situation described in the foregoing sections, it is not surprising that in attempting to regulate UGC the focus has turned on the intermediaries (Web hosts and Internet Service Providers - ISPs) rather than the perpetrators. A website host or ISP is a far easier target to institute proceedings against. A successful lawsuit against a large commercial entity like YouTube may result in an extraordinary amount of damages. Hence in the recent past a barrage of lawsuits have been filed against ISPs, website owners, managers and web hosts, alleging illegal conduct such as copyright infringement, defamation, and even sexual assault.[59] Indeed it is reported that upon acquisition of YouTube, Google 'set aside over $200 million to cover losses and damages stemming from copyright infringement lawsuits brought against the video sites'[60].

The idea of turning to the intermediaries is not without merit: certainly they are the ones in the best position to carry out what little control can be exercised in this 'ungovernable' environment. However, it is not practical for intermediaries to monitor and control UGC due to the large volume of content and fast rate at which it is published. Indeed the law (e.g. Directive 2000/31/EC Section 4) has recognised this and shields intermediaries from liability unless they have notice of infringing content and fail to act on such notice[61].

6.1 Contracts: A Form of Control?

There are a few things which an intermediary can and should do. One of them is to exercise some form of 'policing' role in the initial stages of the user joining the site, mainly by providing two functions: the first is by providing a proper form of identity verification; the second is by creating awareness in the user. Whether either of these two functions is carried out effectively on these sites is debatable.

6.1.1 Identity Verification

The concept of identity verification is of particular importance and should be taken seriously by a website hosting content. It is therefore surprising that on most websites hosting UGC no real form of identity verification is exists. In many cases may websites do not even require any identification whatsoever to view their content. The matter is different when a user wants to join as a member or upload content. In this case, a user is required to register and give various details, such as name, address, date of birth, username, password, and a valid email address.[62] Most of these are 'required fields', and a user will not be able to register unless these details are entered. This form of registration is quite useless as an attempt at identity verification since it is easy to enter false data. It is also very easy to create an email address of the web-based kind such as a 'hotmail' address, using false information. This renders the requirement of a 'valid' email address also futile. None of the information is verified in any way, and the sites are consequently 'open to all', hence users with pseudo identities are free to join and view/upload content uninhibited. Some kind of constraint exists with sites such as Facebook, where a person

must be 'invited' as a 'friend' in order to be able to interact with another user. However most of these sites make a user part of the 'community' upon registration without identity verification.

This lack of identity verification has led to some of these site getting into trouble. For example MySpace was sued for negligence for the lack of age verification on its site after a number of minors who used the site were sexually assaulted by other MySpace members. One such case is that of Pete Solis who assaulted a fourteen-year old Texan girl whom he met on this site. Solis and his victim had exchanged contact details on MySpace and agreed to meet. The meeting led to the victim joining Solis at his apartment, where the assault occurred.[63] Consequently MySpace started working on developing software, codenamed 'Zephyr', which will 'alert parents of name, age and location data which teens enter into their profile or alter'.[64] The information is logged onto a file on the parent's computer and can be accessed remotely by the parent. It is argued that the best effect of such an activity is the deterrent qualities it may have for a young person who knows about this system. When a parent is alerted, it may be too late and also the software will not track a teenager's profile status when using other computers. MySpace have claimed that in spite of their efforts, they have 'not yet found a firm or technology that can reliably verify the age of [their] members under 18'. [65]

6.1.2 Creating Awareness

The other important matter is ensuring that users know what they can and cannot do on a site, so that when posting content on a website they are specifically told that they are not allowed to upload material which is subject to another person's intellectual property rights, or which is defamatory or obscene. Creating this kind of awareness in the user is especially vital when one considers that a large number of such users are young 'carefree' people. Although ignorance of the law is no excuse, it seems only right to alert young people to the fact that an activity which they think is inconsequential may actually carry severe consequences. As an example, YouTube is riddled with video clips consisting of various photos of celebrities shown together with accompanying music in the background. Users posting such clips may be infringing copyright in both the photographs and the music; but because this is being done on such a large scale, the fact that is illegal may not occur to users.

Creating awareness in the user is supposedly carried out through the 'click-wrap' contract method which accompanies the entry details on the registration page. This generally appears as a link at the bottom of the page saying 'terms of use'. A little box appears near the link and has to be 'ticked' by clicking on it before registration is complete – therefore one cannot register unless the 'terms of use' have been agreed to. Legally this should have the effect of creating a contract between the user and the website owner, binding the user to abide by all terms and conditions imposed by the website. Indeed it has been largely held that this kind of 'click-wrap' agreement is a valid contract where the user knows that by continued use of the site he/she has accepted such terms of use[66]. The fact that registration cannot be completed without ticking the box satisfies this requirement of knowledge.

The contract entered into with YouTube, to take an example, thus mentions all the requisite elements and actually includes the following clause in bold type:

> 'In connection with User Submissions, you further agree that you will not: (i) submit material that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including privacy and publicity rights, unless you are the owner of such rights or have permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein; (ii) publish

> falsehoods or misrepresentations that could damage YouTube or any third party; (iii) submit material that is unlawful, obscene, defamatory, libelous, threatening, pornographic, harassing, hateful, racially or ethnically offensive, or encourages conduct that would be considered a criminal offense, give rise to civil liability, violate any law, or is otherwise inappropriate; (iv) post advertisements or solicitations of business: (v) impersonate another person'.[67]

Likewise, similar provisions will be found on all websites allowing UGC. Terms of use for MySpace also include the following clause:

> 'Use of and Membership in the MySpace Services is void where prohibited. By using the MySpace Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the MySpace Services does not violate any applicable law or regulation. Your profile may be deleted and your Membership may be terminated without warning, if we believe that you are under 14 years of age'.[68]

As far as creating awareness goes, these 'contracts' do not go very far. Whilst we have established that 'click-wrap' is a valid method of creating a legal contract, it certainly has its limitations for the purpose under discussion. The fact that this contract exists as a separate link, and that it is so easy to give consent, does not promote the actual reading of the contract, and it can be safely presumed that an alarmingly low percentage of the users of these sites have actually clicked on this link before ticking the acceptance box. Even if a user actually did click on the link, it is not certain whether the user has actually read the entire long, tiresome legal clauses. The average user will be far too enthusiastic to sign up and enter, and will likely tick anything he/she finds in his way without a second thought.

Unfortunately, not much thought about users' psychology has gone into these contracts. It would have been far better to have clear, straight-to-the-point sentences popping up on a separate screen, with each individual clause having to be explicitly accepted (e.g. by a being ticked). That may actually slow down the user enough for him to give some thought to what he is accepting. It may also help if one of these sites actually took action against a user for infringing the terms of such contracts. That may send a message that these contracts do have some validity after all, and should be taken into account. However this is not necessarily a message which these sites want to pass on.

Evidence of the fact that the said contracts are of little help can be found simply by browsing through any of these sites, which are laden with material prohibited by the terms and conditions of use. Notwithstanding the 'Terms of Use' quoted above, pornography is found freely and in great quantity and variety on YouTube. Moreover, according to an investigation by 'Think and Ask', YouTube does not seem to take great pains to remove content which infringes their own 'Terms of Use'.[69]

It is argued in accordance with the above, that the 'contracts' created between many websites allowing UGC and their users serve little purpose other than to create a disclaimer for the benefit of the website owner.

6.2 Intermediaries and the Law

In the defence of intermediaries (ISPs), it must be said that the law sometimes actually gives intermediaries an incentive to be as little involved as possible in what goes on their web servers. Examples of legislation in this area are the: UK Electronic Commerce (EC Directive) Regulations, 2002; UK Defamation Act 1996; United States 47 USC Section 230; DMCA 1998 safe harbour provisions.

6.2.1 The Electronic Commerce (EC Directive) Regulations 2002

Under the UK Electronic Commerce (EC Directive) Regulations 2002, service providers that host content are not liable for damages or any criminal sanction as a result of the storage of content where:

> "(a) the service provider
>
> (i) does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful; or
>
> (ii) upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information, and
>
> (b) the recipient of the service was not acting under the authority or the control of the service provider."[70]

Protection under the UK Electronic Commerce (EC Directive) Regulations 2002 covers all types of unlawful activity including defamation, copyright infringement and pornography. In addition other laws such as the UK Defamation Act 1996 also give protection to ISPs.

6.2.2 UK Defamation Act 1996

In the UK, Section 1 of the Defamation Act 1996 states that a person will have a defence to an allegation if:

> (a) he was not the author, editor or publisher of the statement complained of,
> (b) he took reasonable care in relation to its publication, and
> (c) he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement.

Moreover, Section 1(3)(e) further states that an ISP will not be considered to be the 'author, editor, or publisher' of a defamatory statement: 'if [the ISP] is only involved as the operator of or provider of access to a communication system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.'

Likewise, in the US, it has been commonly held that vendors and distributors of defamatory publications are not liable if they neither know nor have reason to know of the defamation.

Thus in the case of *Cubby, Inc. vs. CompuServe Inc*.[71] the plaintiff, Cubby, Inc. claimed damages due to one of CompuServe's self operated forums 'Rumorville', which had an electronic gossip magazine called 'Skuttlebut'. Defamatory statements were posted about Cubby in 'Skuttlebut'; but CompuServe held that it does not review the contents of publications prior to postings. The court likened the role of CompuServe to that of an electronic bookstore or library and hence did not find CompuServe liable as a publisher. This finding is based on the court case of *Smith v. California*[72], in which the United States Supreme Court held that a distributor must have demonstrable knowledge of defamatory content of a publication prior to dissemination in order to be held liable for releasing that content. On the other hand, in *Stratton Oakmont vs. Prodigy*[73] which was also in respect of defamatory material posted on a online forum, the network provider Prodigy was held liable because since it claimed that it ensured a 'family' atmosphere online, a certain amount of editorial control was exercised over the content, thus Prodigy could not claim to have no knowledge of the defamatory posting.

Of course, the intermediary will have to affect take-down immediately if he is notified of any material which is likely to be libelous on his site, since once he actually has knowledge of such material, the defense of ignorance ceases to exist. In the UK case of *Godfrey v Demon*[74], the defendant (Demon, an ISP) was notified of libelous material hosted on its Internet news server. Demon failed to take down the libelous material and eventually it was overwritten by the system. The Court held that Demon could not be protected under Section 1 (Defamation Act 1996) and hence use of a Section 1 defence was 'hopeless in law'.

This position clearly places the intermediary in a peculiar position. Robin Hamman[75], in discussing the ISP's liability in this sort of situation, states that the intermediary has three options: pre-moderation, which would entail checking all the material before it is posted; post-moderation, where the ISP keeps an eye on material posted and removes that which he deems inappropriate; and reactive/alert only moderation, whereby the ISP is only involved in removing material which he is notified of. Hamman says that a dilemma ensues because 'publication risk' is least likely when using the pre-moderation model, and yet, this is the one which will be most detrimental to his defence in the event that some libelous material escapes his watchful eye, for he can no longer claim to be a mere distributor. The middle option (watching over content already published) would be an ideal solution from a practical point of view as it allows for fast publication (a characteristic of UGC), whilst ensuring that some form of supervision is exercised. However, this once again places the intermediary in an editorial role, thereby cancelling his defense. In a scenario such as that of UGC, publication happens too fast for an intermediary to be able to exercise one-hundred per cent control. As the law stands, therefore, the intermediary is placed in a position whereby he either chooses the extreme and impossible task of ensuring that nothing dubious at all will ever exist on his site, or the other extreme where he exercises no control at all, as long as he effects take-down immediately if notified.

6.2.3 United States: 47 USC Section 230

Following on from the earlier US cases discussed above (on defamation), the US Congress tried to tackle the dilemma of ISP liability by introducing 47 USC Section 230 of the Telecommunications Act 1996[76]. Section 230 listed Congress' 'findings' and 'policy', whereby it is recognised that the activities upon the Internet have '*flourished, to the benefit of all Americans*', and that '*the continued development of the Internet and other interactive computer services*' should be preserved. It also recognised, however, the need for some form of control (especially by intermediaries). Hence, Section 230 lists the following, amongst its policies (Section 230(b)):

- ‘to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services’

- ‘to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material’

The intention in the U.S. is therefore to encourage ‘self-regulation’ and the exercise of control by the intermediary through the inclusion of the following protections for ‘good samaritan’ blocking and screening of offensive material (Section 230 (c)):

- ‘Treatment of publisher or speaker**.** 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.

- Civil liability**.** No provider or user of an interactive computer service shall be held liable on account of - any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)’.

Section 230 also imposes the following obligation:

> ‘A provider of interactive computer service shall, at the time of entering an agreement with a customer for the provision of interactive computer service and in a manner deemed appropriate by the provider, notify such customer that parental control protections (such as computer hardware, software, or filtering services) are commercially available that may assist the customer in limiting access to material that is harmful to minors. Such notice shall identify, or provide the customer with access to information identifying, current providers of such protections.’

An important question is whether the provision of Section 230 had the required effect. Whilst this section has certainly been used widely to defend the intermediaries’ liability, as will be seen below, it is doubtful whether it will have had the effect of inducing self-regulation. An intermediary will always be exempted from liability only until it has been given notice of infringing material, at which point it must effect take-down procedures. In *Zeran v. America Online, Inc.*[77] the court equated the action of screening material in the manner hoped for by Section 230 as amounting to notice, stating ‘similarly, notice-based liability would deter service providers from regulating the dissemination of offensive material over their own services. Any efforts by a service provider to investigate and screen material posted on its service would only lead to notice of potentially defamatory material more frequently and thereby create a stronger basis for liability. Instead of subjecting themselves to further possible lawsuits, service providers would likely eschew any attempts at self-regulation.’

6.2.4 Section 230 and expanding immunity

Section 230 has been widely used with continuous success as a defence by intermediaries against liability for defamatory statements posted on their sites. Indeed a recent article discussing website immunity stated that ‘*It is fairly well established now that interactive computer service providers are not liable for information transmitted over their service by*

another. In the plain vanilla case of a person suing a website or ISP for defamation based on a message board posting by a third party, judges hardly even finish reading the complaint before granting judgment for the defendant'.[78]

What is interesting, however, is that the immunity offered by Section 230 has been expanded far beyond this scope. By virtue of *Barrett v Rosenthal* [79] it was established that a person who posts defamatory material on a website without being the actual author of that material can still be spared from liability by the Section 230 defence. In this case, the defendant had posted the content of an email containing defamatory material onto a website without verifying its contents. The important fact in this case is that the website was not owned or managed by the defendant and she was merely a 'user' of this site. The Court placed emphasis on the wording of Section 230 which 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.*'[80] The Court first defined 'user' as anyone using an interactive computer service, therefore anyone using the Internet would fall under this definition. Secondly, the Court chose not to accept the Plaintiff's plea stating that one must distinguish between 'active' and 'passive' use, and stated simply that we conclude there is no basis for deriving a special meaning for the term 'user' in Section 230(c)(1), or any operative distinctions between 'active' and 'passive' Internet use. By declaring that no 'user' may be treated as a 'publisher' of third party content, Congress has comprehensively immunized republication by Individual Internet users'. As Eric Goldman states on his blog dated 20th November 2006, '*presumptively, everyone online is eligible for 47 USC 230 immunization*.'[81]

Section 230 has also been applied in the case of *Universal Communication Systems, Inc. v. Lycos, Inc.*[82], in favour of the Raging Bull website: a financial messaging board operated by Lycos. The complainants (plaintiffs) sued Lycos, stating that under Florida securities law Lycos was the publisher of information posted on this kind of site by third-parties. The Court dismissed this claim stating:

> 'We have no trouble finding that Lycos's conduct in operating the Raging Bull web site fits comfortably within the immunity intended by Congress. In particular: (1) web site operators, such as Lycos, are "provider[s] ... of an interactive computer service"; (2) message board postings do not cease to be "information provided by another information content provider" merely because the "construct and operation" of the web site might have some influence on the content of the postings; and (3) immunity extends beyond publisher liability in defamation law to cover any claim that would treat Lycos "as the publisher'.[83]

The complainant (plaintiff) also tried to claim active inducement on the part of Lycos, basing such claim on the previous Grokster case (*MGM Studios, Inc. v. Grokster, Ltd.*) [84] and stating that 'active inducement' destroys a Section 230 defence; however the Court felt that this was a standard messaging board and no inducement was deemed to have occurred.

An even more significant broadening of the Section 230 defence is to be found in the US case of *Doe v. MySpace*[85]**.** This case was in regard to an allegation of negligence against MySpace and consequent liability for the sexual assault on a minor member of MySpace by another member of MySpace, Peter Solis, as mentioned above. In this case, the Court stated that '*nothing on the fact of the statute support's …narrow interpretation that the CDA's immunity applies only to cases involving defamation and defamation-related claims*.' The Court then went on to list a number of cases where the Section 230 immunity was applied to non-defamation claims. One of the cases referred to was *Doe v Bates*[86] concerning a lawsuit against an e-group hosted by Yahoo! Inc. for the publication of pornographic pictures of a child. In that

case, the Court applied Section 230 and found that Yahoo was not liable, even though the complainant (plaintiff) did not allege that there was anything defamatory about the posting. The Court went on to reject the complainant's (plaintiff) claim that Section 230 was not applicable due to the fact that it was not brought against MySpace in its capacity as publisher. The Court stated that '*no matter how artfuly Plaintiffs seek to plead their claim, the Court views Plaintiff's claims as directed toward MySpace in its publishing, editorial and/or screening capacity'*. The Court therefore applied Section 230 immunity to this case. Whilst this is merely a district court and may not be followed in future decisions, it does give an idea as to the breadth of activities to which the Section 230 immunity may apply.

It must be noted that Section 230 does not provide immunity from federal criminal law and infringement of intellectual property law (e.g. copyright, trademark infringement)[87]. With regard to its effect, Section 230(d) states: '(1) NO EFFECT ON CRIMINAL LAW- Nothing in this section shall be construed to impair the enforcement of section 223 of this Act, chapter 71 (relating to obscenity) or 110 (relating to sexual exploitation of children) of title 18, United States Code, or any other Federal criminal statute. (2) NO EFFECT ON INTELLECTUAL PROPERTY LAW- Nothing in this section shall be construed to limit or expand any law pertaining to intellectual property.'

6.2.5 DMCA 1998, Section 512

In the US, ISPs can avoid liability for copyright infringement from the actions of website users by virtue of Section 512 of The Digital Millennium Copyright Act ("DMCA") 1996, known as the 'safe habor' provisions.

The DMCA Section 512(c)(1) states that: 'A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider -

(A)

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) Does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.'

Eligibility for protection under Section 512 is subject to certain conditions given in Section 512(c)(2) namely that the website owner must have:

(a) designated an agent to receive notifications of claimed infringement
(b) make its agent available through its service, including on its website in a location accessible to the public
(c) provide the copyright office with the contact details (name, address, phone, email) of the agent and other information it may deem necessary.

The extent to which the safe habor provisions under the DMCA are effective for ISPs and UGC, have been tested by a US$1Billion dollar lawsuit filed on March 13th, 2007, by Viacom against YouTube and Google for copyright infringement[88]. Among other complaints, Viacom alleged that over 150,000 Viacom clips have been illegally uploaded onto Youtube totalling more than 1.5 billion views[89]. In its defence Youtube claims protection under the DMCA safe habor provisions and Fair use. At the time of writing testimonies are being collected for trial, and any judicial ruling will possibly have wide ranging implications for ISP liability, UCG and intellectual property law.

In spite of the DMCA safe harbor provisions, YouTube have been taking precautions to limit copyright infringement. For example in 2006, YouTube signed an agreement with Universal Music Group (UMG) and to licence users who posted videos on the YouTube to allow them to use music owned by Universal as a soundtrack[90]. Indeed it is unfair to impose too much responsibility on ISPs, however, an ISP is a business entity whose aim is to maximise profits, and therefore its business success cannot be at the expense of others (e.g. copyright owners).

7. Conclusions

The issues raised by UGC are indeed serious, and need to be addressed by the combined effort of individuals and organisations. Among many players: users need to take responsibility for their activities; parents need to ensure that their children are protected from dangers associated with use of the Internet, legislators need to create new laws to address new types of illegal activities, software developers need to consider ethical and legal issues when developing new products; and service providers need to adhere to their contractual and legal obligations.

ISPs are perhaps the most effective players who can exercise some form of ‘gate-keeping’ to regulate UGC. An important question is whether ISPs can be more proactive without subjecting themselves to liability since monitoring may subject them to actual knowledge of illegal content. Indeed, as discussed earlier, the current state of the law does not impose an obligation on ISPs to monitor information transmitted or stored and actually provides them with immunity if they have no actual knowledge of infringing content. This gives little incentive for ISPs to monitor activities on websites.

We submit that ISPs can make more effective use of technology as a regulator, and of their position at the gateway of the Internet, by actively monitoring and removing infringing content as far as it is practicable to do so, subject to cost. We argue that generally greater use needs to be made of technology to regulate illegal content. Indeed MySpace recently announced a new copyright technology, called "Take Down Stay Down" which prevents users from uploading previously removed infringing video clips[91].

Other forms of online patrol such as e.g. Internet Watch Foundation[92] also need to play a greater role in policing the Internet, by creating greater awareness of their presence and activities. More endeavours of this kind need to be undertaken to protect the values of society.

There is also a need for strict identity verification protocols to be put in place when registering for online services such as email addresses, or membership of various websites. Such protocols could enable a service provider to uniquely identify any individual registering for a service, and hence make him/her accountable, which may also act as a deterrent. Identity verification can include the requirement to have registration data such as a social security number (in the US) or credit card details, and a method of verifying that the person producing such details is genuine. New legislation can also be adopted to enforce correct procedures for online identity verification.

UGC, enabled by the revolution in digital technologies has undoubtedly raised many issues regarding the distribution and sharing of online content. On hand one it has empowered ordinary citizens and enhanced a sense of freedom and democracy. Ordinary citizens are able to send and receive information on a previously unimaginable scale. They are able to potentially exercise 'legitimate power' to influence change (e.g. social, political, cultural or economic) by the ability to communicate and network with a global audience. On the other hand, many online activities are illegal or undesirable akin to a new frontier like the 'Wild West' . We reiterate the need for a concerted effort to address such illegal and undesirable activities. Hopefully this will produce a relatively safe and lawful online environment, allowing citizens to enjoy the beneficial aspects of UGC.

Endnotes

[1] This paper is a revised and extended version of a paper presented at BILETA 2007.
[2] Tim O'Reilly is the founder and CEO of O'Reilly Media, Inc., publishers of high quality computer books and organisers of technology-related conferences. He is also an activist for open standards. See: http://www.oreillynet.com/pub/au/27
[3] http://radar.oreilly.com/archives/2005/10/web_20_compact_definition.html
[4] T. 'OReilly (2005), What is Web 2.0: Design Patterns and Business Models for the Next generation of Software: http://www.oreillynet.com/pub/a/oreilly/tim/news/2005/09/30/what-is-web-20.html
[5] Y. Zhang (2006). Wiki means More: Hyperreading in Wikipedia, Sixteenth ACM Conference on Hypertext and Hypermedia, August 22-25, 2006, Odense, Denmark
[6] http://meta.wikimedia.org/wiki/List_of_Wikipedias#All_Wikipedias_ordered_by_number_of_articles
[7] TiVo is a service that amongst other things can automatically find and digitally records all of someone's favourite shows, every time they're on. It also enables various online services (e.g. podcasts, traffic, movie listings). See: http://www.tivo.com/1.0.asp
[8] Syndication refers to the process of making bits of a website content available for other sites to use (e.g. sharing news headlines). Syndication is usually facilitated by use of an XML application RSS 2.0 which allows bits of content to be placed into a simple text file which can then be read (at specific intervals) by other websites or reader programs. See: http://www.devarticles.com/c/a/XML/Simple-Web-Syndication-with-RSS-2/
[9] P. Anderson (2007), What is Web 2.0? Ideas, technologies and implications for education, JISC technology and Standards, Feb, 2007.
[10] Ibid
[11] Ibid
[12] Ibid
[13] Ibid
[14] Ibid
[15] Ibid
[16] P. Chin (2006), The Value of User Generated Content, Part1, Intranet Journal : http://www.intranetjournal.com/articles/200603/ij_03_07_06a.html
[17] Ibid
[18] http://sfbay.craigslist.org/

[19] http://www.lessig.org/blog/
[20] http://en.wikipedia.org/wiki/Wiki
[21] http://www.amazon.co.uk/
[22] http://www.lowcarbsite.com/forum/viewforum.php?f=2
[23] R. Lemos (2006), Social sites' insecurity increasingly worrisome, The Register, 5th December 2006, http://www.theregister.co.uk/2006/12/05/social_sites_vulnerable/
[24] The Guardian(2007), How the web became a sexists' paradise, Friday April 6, 2007 http://technology.guardian.co.uk/news/story/0,,2051580,00.html
[25] ABC News (2007), Blogger Sued Over Topless Aniston Photo, Feb 21, 2007 http://abcnews.go.com/Entertainment/wireStory?id=2893926
[26] A. Orlowski (2007), Saddam's YouTube Smash, The Register 2nd January 2007, http://www.theregister.co.uk/2007/01/02/saddam_youtube_hit/
[27] http://www.flickr.com/
[28] A. Vance (2006), Secret Service grills MySpace teen, The Register 16th October 2006, http://www.theregister.co.uk/2006/10/16/teen_myspace_protest/
[29] http://www.bebo.com/
[30] J. Kiss (2007), Bloggers force ad boycott on San Fran Radio Station, The Guardian, 16th January 2007, http://blogs.guardian.co.uk/organgrinder/2007/01/bloggers_force_ad_boycott_on_s.html
[31] Copyright is the legal right which the author of an original literary, dramatic, musical or artistic work (among others) has with respect to controlling use and access to his/her work. See: UK Copyright Designs and Patents Act 1988: http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_2.htm#mdiv1
The Convention on Cybercrime (Budapest Nov 2001), agreed on the harmonisation of laws in 43 signatures (including the US, Japan, Canada, S.Africa), to define criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes: security breaches (e.g hacking), fraud and forgery, copyright infringements and child pornography.
[32] DMCA is the US Digital Millennium Copyright Act : See http://www.copyright.gov/legislation/dmca.pdf
[33] Viacom is a media conglomerate which owns many cable and satellite TV networks such as MTV and BET.
[34] E. Brown (2007), Copyright and Online User-Generated Video. 51st Anniversary Conference On Developments in Intellectual Property Law February 23, 2007, Chicago, Illinois
[35] A. Berzon (2007), Scenes from a Tightrope, Red Herring, 2nd April 2007.
[36] Ongoing litigation at the time of writing include: *Io Group, Inc. v. Veoh Networks, Inc.*, No. 06-3926, (N.D. Cal., filed 6/23/2006); *Tur v. YouTube, Inc.*, No. 06-04436 (C.D. Cal., filed 7/14/2006); *UMG Recordings Inc et al v. Grouper Networks, Inc.*, No. 06-6561 (C.D. Cal., filed 10/16/2006); *UMG Recordings Inc et al v. Bolt, Inc.*, No. 06-6577 (C.D. Cal., filed 10/16/2006); *UMG Recordings Inc et al v. MySpace Inc.*, No. 06-7361 (C.D. Cal., filed 11/17/2006). See A. Berzon (2007) above.
[37] See YouTube Terms and Conditions: http://www.youtube.com/t/terms
[38] Brazil orders YouTube shut down over celebrity sex video http://boingboing.net/2007/01/04/brazil_orders_youtub.html
[39] L. Hearn (2006), Tassie YouTube star calls it quits http://www.smh.com.au/news/web/youtube-star-quits/2006/08/28/1156617251368.html
[40] T. Govani & H. Pashley (2005), Student Awareness of the Privacy Implications When Using Facebook http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf
[41] Ibid
[42] An additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems was added to the Convention on cybercrime in Strasbourg, January 2003.
[43] M. Cooper (2005), God I hate Arabs. http://www.welcometotheasylum.com/articles/arabs.htm
[44] Examples include many sites contain anti-Western and pro-terrorist sites.
[45] A. Zaharov-Reutt (2007), Wikipedia entry causes pro-golfer Fuzzy Zoeller to sue http://www.itwire.com.au/content/view/9913/53/
[46] J. Seigenthaler (2005), A false Wikipedia 'biography', USATODAY, 29th November 2005 http://www.usatoday.com/news/opinion/editorials/2005-11-29-wikipedia-edit_x.htm
[47] Statement can be viewed at http://www.mumsnet.com/lw/state.html
[48] Think and Ask (2006). Fetish Videos Land on Family Entertainment Website 'You Tube' http://www.thinkandask.com/2006/022706-youtube.html
[49] A noted earlier, the Convention on Cybercrime (Budapest Nov 2001), agreed on the harmonisation of laws in 43 signatures (including the US, Japan, Canada, S.Africa), to define criminal offenses and sanctions under their domestic laws for four categories of computer-related crimes: security breaches (e.g hacking), fraud and forgery, copyright infringements and child pornography.
[50] What is the best way to kill yourself when you're under 13? http://www.mouchette.org/suicide/answers.php3?cat=experience

[51] T. Gutierrez & K. McCabe (2005), Parents: Online newsgroup helped daughter commit suicide. CNN, November 11, 2005. http://www.cnn.com/2005/US/11/04/suicide.internet/index.html
[52] Ibid
[53] L. Sherriff (2005), Anonymity no protection for online libellers. (The Register 24th March 2005) http://www.theregister.co.uk/2005/03/24/motley_ruling/
[54] Matthew Arnold & Baldwin Solicitors, Watford and London UK http://www.mablaw.co.uk/
[55] See L. Sherriff (2005) op.cit.
[56] A criminal offence usually consists of two elements which needs to be proved namely the *actus reus* (the act, omission or state of affairs) and the *mens rea* (state of mind or intention of the accused).
[57] L Lessig (1999). Code and other Laws of Cyberspace. Basic Books, US.
[58] A take down notice (under copyright law) involves informing a service provider about conduct (e.g. online content) which is alleged to be an infringement and making demand that such content be removed.
[59] Discussed below
[60] G. Duncan (2006), Google Stashes $200 Mln for YouTube Suits: 16th November 2006 (Digital Trends) http://news.digitaltrends.com/article11763.html
[61] For example the EU Electronic Commerce Directive - Directive 2000/31/EC Section 4 : Liability of Intermediary service providers. Also in the US 47 USC Section 230 gives immunity to ISPs. Further for defamation, The UK Defamation Act 1996 Section 1(3)(e) states that an ISP will not be considered to be the 'author, editor, or publisher' of a defamatory statement: 'if [the ISP] is only involved as the operator of or provider of access to a communication system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control.'
[62] See e.g. registration page for YouTube http://www.youtube.com/signup?next=/my_videos_upload%3F, and MySpace http://signup.myspace.com/index.cfm?fuseaction=join&MyToken=5878a480-a6a0-4ba7-8571-c418920b49e9
[63] E. Bangeman (2006), MySpace sued in wake of sexual assault (20th June 2006): http://arstechnica.com/news.ars/post/20060620-7096.html
[64] C. Williams (2007), MySpace passes age verification buck to parents (17th January 2007) – The Register http://www.theregister.co.uk/2007/01/17/myspace_zephyr/
[65] Ibid quoting the Wall Street Journal
[66] Cairo, Inc. v. CrossMedia Services, Inc.No. C04-04825 (JW) (N.D. Ca., April 1, 2005); Hotmail Corp. v. Van$ Money Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 (N.D. Cal., 1998).
[67] See YouTube Terms of Use: http://www.youtube.com/t/terms
[68] See MySpace Terms of Use: http://www.myspace.com/Modules/Common/Pages/TermsConditions.aspx
[69] Think and Ask: You Tube Pulls some Pornography, Bans Children 'under 13': http://www.thinkandask.com/news/030206-utube2.html
[70] Section 19, The Electronic Commerce (EC Directive) Regulations 2002
[71] 776 F.Supp. 135(S.D.N.Y. 1991)
[72] 361 U.S. 147 (1959)
[73] Stratton Oakmont Inc v Prodigy Services Co (23 Media Law Rep (BNA) 1794 (NY Supreme Court 1995)
[74] QBD, [1999] 4 All ER 342
[75] Robin Hamman: User Generated Content Online and UK Libel Law: a discussion of issues http://www.cybersoc.com/files/cybersoc_libel_discuss_paper.rtf
[76] Title V of the Telecommunications Act 1996 is also known as The Communications Decency Act
[77] (E.D.Va. 1997) 958 F.Supp. 1124.
[78] Kevin Fayle: 'Website immunity spreads with impunity' (The Register - 28th February 2007) http://www.theregister.co.uk/2007/02/28/section_230_website_immunity/
[79] S 122953 (Cal. Sup. Ct., November 20, 2006)
[80] Section 230, (c)(1)
[81] Eric Goldman: Technology and Marketing Law blog: 'California Issues Terrific Defense-Favorable Interpretation of 47 USC 230' 20th November 2006 - http://blog.ericgoldman.org/archives/2006/11/barrett_v_rosen_1.htm
[82] 2007 WL 549111 (1st Cir. Feb. 23, 2007)
[83] http://www.ca1.uscourts.gov/pdf.opinions/06-1826-01A.pdf
[84] MGM Studios, Inc. v. Grokster, Ltd., See: http://fairuse.stanford.edu/MGM_v_Grokster.pdf
[85] Case No. A-06-CA-983-SS
[86] No.5:05-CV-91-DF-CMC, 2006 WL 3818758 (E.D. Tex. Dec.27, 2006)
[87] See the 31st May 2007 amended opinion of *Perfect 10, Inc. v CCBill LLC*, 481 F.3d 751
[88] Viacom's YouTube lawsuit could test limits of DMCA , http://www.theregister.co.uk/2007/03/14/viacom_youtube_lawsuit_dmca/

[89] See: http://news.com.com/pdf/ne/2007/ViacomYouTubeComplaint3-12-07.pdf
[90] Universal sues video sharinig sites.
http://www.theregister.co.uk/2006/10/19/universal_sues_vidoesharers/
[91] R. Francia (2007). MySpace launches Take Down Stay Down copyright protection
http://tech.blorge.com/Structure:%20/2007/05/11/myspace-launches-take-down-stay-down-copyright-protection/
[92] http://www.iwf.org.uk/