

# The Risks of User-Supplied Content Online

Rónán Kennedy

National University of Ireland, Galway Law Faculty, [ronan.m.kennedy@nuigalway.ie](mailto:ronan.m.kennedy@nuigalway.ie)

**Abstract** Websites which rely on user-generated or user-supplied content (USC) run a variety of legal risks, as innocent, uninformed or malicious users may post material which infringes copyright, is defamatory, obscene or otherwise illegal. Amongst the strategies which developers might use to mitigate these risks are indemnities, moderation of content and designing systems in order to avail of the various ‘safe harbours’ which have been developed specifically for online service providers. As the first two strategies have a number of legal and practical drawbacks, the primary protection must be the safe harbours. In an increasingly globalised world, it is unsafe to ignore foreign laws and therefore USC sites should employ a robust but measured notice-and-takedown procedure.

## 1 Introduction

### 1.1 The Phenomenon of User-Supplied Content

One particular type of Internet information system which is becoming increasingly prevalent is the website which relies on users to supply a good deal of its content. Notable examples include Wikipedia, which is an attempt to create a free and open encyclopedia, YouTube, which is a video-sharing site, and MySpace, which is a social networking site that also allows users to post images, audio and video for playback and download. Users also provide reviews for the online bookseller Amazon, blog postings on a variety of hosting sites, and commentary on those blogs and many publicly-accessible mailing lists. Here, membership of the user base is open to all. Other sites may restrict membership, perhaps requiring the payment of a fee (e.g. genealogy sites), membership of an organisation (e.g. a distributed non-governmental organization) or participation in a marketplace (e.g. auction sites such as eBay).

This phenomenon is often known as ‘user-generated content’ (UGC) but is often, in fact, simply ‘user-supplied content’ (USC), as it is not the result of the independent creative work of the users but is copied from some other source, such as television broadcasts. Peer-to-peer file-sharing services for audio and video content, such as Napster, Grokster and KaZaa, have become well known, even infamous, as although they do carry legitimate content, much of what is provided by

users for download is, in fact, copyrighted material and as a result, many have been shut down.

Information systems developers who are taking advantage of new business and content provision models, such as UGC/USC, need proper awareness of the legal pitfalls involved and how to avoid these where possible. Although the legal liabilities of online service providers (OSPs), particularly Internet service providers (ISPs), have received significant consideration in recent years and legislation has been enacted in order to clarify their position, much of this discussion has proceeded on the basis that they are simple conduits, indifferent to and unaware of the content which flows through their systems. USC sites are different as they actively encourage users to provide particular types of content, often as the foundation of their business model. They must therefore take care to ensure that they fit properly into the existing models. This paper considers some of the legal risks which information systems developers should consider when designing these types of systems. It makes some suggestions for reducing or minimising the risks involved, particularly how to ensure that the system fits into the various 'safe harbours' in American and European law.

## 2 Possible Legal Issues

### 2.1 Copyright Infringement

In general, if content has been genuinely generated by individual users of the site, then they will have the right to upload it to a public website for distribution. However, in many cases, the content will have been created by a third party and simply appropriated by the user, perhaps with either no understanding or a mistaken understanding of any risk of copyright infringement, and often with no malicious intent. Sometimes, also, UGC will contain both original work and content copyrighted by third parties.

Nonetheless, even if the purpose of the user is innocent, the legal liability remains the same. Therefore, perhaps the most important risk which operators of a user-supplied site must manage is from copyright infringement. A prominent current example is Viacom's allegation that copyrighted material often appears on the video-sharing site, YouTube (Computer and Telecommunications Law Review 2007), but this is an issue which pre-dates the widespread use of the Internet.

In *Playboy v. Frena*, a bulletin board system operator was held liable for the copying of images from the plaintiff's magazines although the uploading and downloading was in fact carried out by users. However, later courts refused to follow this precedent and in *Religious Technology Centre v. Netcom*, the Church of Scientology was unable to obtain damages from an ISP for infringing copies uploaded to USENET by a customer of the ISP (Reed 2004, pp. 96–97).

In these types of situation, there is little doubt that the user of the site is liable for copying the copyrighted work and making it available to the public (Clark and

Smyth 2005, pp. 333–337). The liability of the administrators of the site is less clear (Clark et al. 2005, p. 339). The most significant precedent on the issue in these islands is *CBS v. Amstrad*, where the defendant sold dual-tape cassette systems with an advertising campaign that emphasised how they facilitated copying of tapes through high-speed dubbing. The House of Lords held that they could not be held responsible for what consumers did with their equipment after purchase.

In the US, the recent Supreme Court decision in the *Grokster* case clarified that although the *Sony* rule which protects technology with both infringing and significant non-infringing purposes still stands, indirect liability for copyright infringement may attach to a defendant who actively induces users of technology to infringe.

Elsewhere, the Australian Federal Court found the operators of the Kazaa file-sharing network liable for facilitating copyright infringement (Williams and Seet 2006), while the Supreme Court of Holland upheld a decision of the Court of Appeals that Kazaa were not liable because the network operated independently of the company, it was not possible to identify copyrighted content, the company was not responsible for the acts of its users and some of the files shared were legitimate (Akester 2005).

## 2.2 Defamation

Defamation is ‘the wrongful publication of a false statement about a person, which tends to lower that person in the eyes of right-thinking members of society or tends to hold that person up to hatred, ridicule or contempt, or causes that person to be shunned or avoided by right-thinking members of society’ (McMahon and Binchy 2000, p. 882). The potential for such statements on a website that allows the general public to post information and commentary is obvious, although proving where and when publication took place can be difficult (McGonagle 2003, p. 74).

There is a defence of innocent dissemination, open to (for example) newspaper vendors and booksellers, but as it only applies to those who neither knew nor ought to have known of the defamation, it will only rarely apply to those administering UGC sites, particularly if the subject matter is contentious.

One notable recent Irish example of possibly defamatory USC involved the Rate-Your-Solicitor.com website. A barrister claimed that material posted on the website about her was defamatory and the President of the High Court threatened to jail the person who was alleged to have made the comments in question. The defendant claimed that he had not made these comments and had no control over the content of the website, which was hosted in the US. However, the material was removed before the deadline set by the judge (Carolan 2006; Collins 2006).

## 2.3 Other Contentious Forms of Speech

While these forms of conduct should be the primary concern of the administrators of a USC site, users may also post material that is pornographic or obscene, or that

is prohibited on political grounds, perhaps as hate speech or sedition. However, these are probably less important in practice. In Ireland, there are few prosecutions for the publication of indecent and obscene material, even in print, and less under the Prohibition of Incitement to Hatred Act 1989 (McGonagle 2003, pp. 281–282), although prosecutions for obscene sexual material do occur in the US (Reed 2004, p. 106). Prosecutions for blasphemy are almost unknown (McGonagle 2003, p. 303).

However, Yahoo! was ordered by a court in France to remove all Nazi memorabilia from its auction website and, although it obtained a declaration from an American court that the French order was unenforceable in the US, it did ban all such material (Reed 2004, p. 95). Child pornography may be a particular concern (Reed 2004, p. 107) and so administrators should take care to remove it immediately if it is discovered on their systems. Finally, there may be concerns about users posting material which breaches the privacy of others (Holmes and Ganley 2007, 343).

### **3 Minimizing the Risks**

When planning and designing an information system that uses USC, either as a main or subsidiary source of content, developers will want to reduce or remove the risk of legal difficulties. There are a number of strategies which they might adopt.

#### ***3.1 Indemnities from Users***

The first possible line of defense is to require users to provide some form of indemnity. This will take the form of a legal agreement which users have to agree to before they upload content, either when they apply for membership of the site or each time they add more content, wherein they warrant that the material uploaded does not infringe copyright or contravene any other law (Miles and Caunt 2007, p. 25). Sometimes, these agreements go so far as to transfer legal ownership of any intellectual property in the uploaded content to the operator of the site (Holmes et al. 2007, p. 338). This can be controversial – the musician Billy Bragg removed all of his music from MySpace when he discovered that he was transferring all rights in the process (Levine 2006), forcing a revision of the terms and conditions (Orlowski 2006) and it may not be wise to go so far.

Indemnities can be useful, if only as a way of focusing the minds of users on whether they are willing to take responsibility for the content they are making public, and some sites go so far as to outline what those responsibilities are (Miles et al. 2007, p. 25). However, they have limitations, both legal and practical.

From a legal point of view, a point of controversy in the early days of contracting online was whether what are known as ‘click-wrap’ contracts are valid. These are generally licences for the use of software which the user agrees to when an application is used for the first time. Indemnities would present similar issues. Although their validity is not entirely clear, a clear and reasonable contract will

probably be accepted by the courts (Johnson 2003). However, consumers still do not seem to regard them as constituting a valid contract (Gatt 2002), which raises the question of how carefully they will be read and whether they will act as a proper deterrent to risky or illegal conduct.

In addition, if the user is under the age of 18, the contract may not be enforceable. For adult users, the Unfair Contract Terms Directive (Directive 93/13/EEC) provides that unfair terms in standard form contracts involving consumers will not be binding on the consumer. A term will be held to be unfair if 'it causes a significant imbalance in the parties' rights and obligations arising under the contract, to the detriment of the consumer' (Article 3(2)). An indemnity which imposes too much liability on a consumer might be challenged on this basis.

From a practical point of view, the user may not be easily traceable. They may not provide sufficient or accurate information on their identity or location. They may, of course, be traceable by IP address, but this is a slow and cumbersome process which may involve protracted negotiations or litigation with their ISP (McIntyre 2004). Even if they can be located, they may be located in another jurisdiction, making enforcing the indemnity difficult, or they may not have very many assets, making enforcing the indemnity pointless.

### **3.2 Moderation of Content**

Another potential defence is to employ humans to moderate content which is posted by users. However, in addition to the obvious resource implications, this may be a bad rather than a good idea from the perspective of legal liability. Early American cases involving online defamation made bulletin boards that exercised editorial control over content liable for defamatory content (*Stratton Oakmont v. Prodigy*), whereas those that did not were treated as a common carrier and thus immune from suit (*Cubby v. Compuserve*). While these cases have been superseded by the Communications Decency Act (CDA), which we will consider shortly, the risk is clear: operating a moderation system may, in fact, remove the immunities enjoyed by the ignorant and opens the service provider to liability if it fails.

Automated moderation, or filtering, is touted as an appropriate solution, particularly for copyrighted content, but despite asides to this effect in the US Supreme Court's decision in the *Grokster* case, difficulties in implementing, updating and mandating the use of such technology on a global scale make it impractical (Samuelson 2006).

### **3.3 Issues of International Jurisdiction**

The Internet is, of course, international in scope. Those operating websites will often focus solely on legal liability under their local laws and will not be concerned about possible breaches of foreign laws. However, this may prove to be a short-sighted policy. The rhetoric of the Web as an untameable new frontier for the

human mind is giving way to the more prosaic realisation that Internet traffic and content can be controlled (Goldsmith and Wu 2006). With increased globalization, the notion that individuals can ignore the laws of major world powers and trading powers, particularly the US, becomes increasingly untenable. This is perhaps most clearly illustrated by the impact which an American crackdown on Internet gambling has had on the industry worldwide, including the recent arrests of foreign CEOs of gambling websites for alleged breaches of American law while transiting through the US (Timmons and Pfanner 2006).

### *3.4 Availing of Safe Harbours*

As the Internet developed, so did the understanding that OSPs were a new type of content provider and that applying the existing models of liability to them risked stunting or stifling a new industry. Many jurisdictions enacted legislation to give OSPs legal immunity for content which they carried on behalf of their users, on the basis that they could not realistically monitor or control the flow of information which governments wanted to facilitate. The shape of these 'safe harbours' differs; we will consider only the two most important, the American and the European, each of which is informed by different freedom of speech traditions.

American legislation creates two primary safe harbours for OSPs. One is § 512 of the Digital Millennium Copyright Act, 17 U.S.C. § 512, which provides that service providers shall not be liable to pay damages or be subject to an injunction for copyright infringement if the infringement occurs due to routing of material through their systems, caching, storage of information on their systems by users or providing links to infringing material. These immunities apply

'only if the service provider—

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures' (in other words, digital rights management systems).

In addition, to benefit from § 512 (c), which provides immunity for '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,' the service provider must '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 'upon notification of claimed infringement ... respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.' This is commonly called a 'notice-and-takedown' procedure; there is provision for a counter-notification which allows the user to rebut the claim of infringement.

In *Ellison v. AOL*, a user posted copies of the plaintiff author's books on USENET without authorization. Copies were stored on AOL's servers for 14 days, as was their standard policy. The author's email complaint to AOL went unanswered, probably because AOL changed its copyright notification email address without registering the change with the US Copyright Office and without automatically forwarding email from the old address. When he began a legal action, AOL blocked access to the USENET group. On appeal, the Ninth Circuit held that the confusion regarding copyright notifications probably made it impossible for AOL to benefit from the safe harbour and remanded the matter for further consideration.

In *CoStar v. LoopNet*, the plaintiff provided commercial real estate information. LoopNet allowed real estate brokers to post listings on its website. Users warranted that they had all necessary 'rights and authorizations' to post material. LoopNet employees cursorily reviewed photographs. Photographs copyrighted by CoStar were posted on LoopNet's website. The Fourth Circuit concluded that even if LoopNet could not benefit from the DMCA safe harbour, it could still benefit from the *Netcom* ruling and the screening of photographs by LoopNet was not significant enough to make them liable for copyright infringement.

Another safe harbour is the Communications Decency Act, 47 U.S.C. § 230, which gives providers and users of an 'interactive computer service' nigh-complete immunity for the re-publication of the content provided by others. For example, in *Zeran v. AOL*, an advertisement for tasteless t-shirts was posted on AOL with the plaintiff's telephone number and he received threatening calls as a result. AOL eventually removed the advertisement but Zeran filed suit, claiming that there was unreasonable delay in removing defamatory material. AOL successfully pleaded § 230 of the CDA as a defense. The court felt that the intention of Congress was to free OSPs from the impossible burden of having to check each individual message.

In *Batzel v. Cremers*, an email which was alleged to contain defamatory statements about the plaintiff was sent to the defendant by a third party. The defendant modified it slightly and forwarded it to a mailing list, something which was not intended by the original author. When the plaintiff sued for defamation, the defendant raised § 230 as a defence. However, the court held that this would only apply if the defendant had reason to believe that the original author was submitting the message in order to have it published online; otherwise, the protection would spread too widely.

What this means, then, is that in the US, the level of protection which an OSP has is relatively high. In general, there is no obligation to read and investigate every piece of information distributed or published through a website. Even if the information is edited and redistributed, such as through a mailing list, § 230 may still apply. Thus, for example, a blogger is not subject to liability for comments on their blog – although they remain liable for what they themselves publish on the blog.

In Europe, the relevant legislation is the Electronic Commerce Directive (Directive 2000/31/EC). This applies to those providing an 'Information Society service,' defined in Directive 98/48/EC as 'any service normally provided for remuneration, at a



distance, by electronic means and at the individual request of a recipient of services,' a definition that is sufficiently broad to encompass most, if not all, USC sites.

Article 12 of the Directive exempts OSPs from liability when they act as a 'mere conduit':

'Where an information society service is provided that consists of the transmission in a communication network of information provided by a recipient of the service, or the provision of access to a communication network, Member States shall ensure that the service provider is not liable for the information transmitted, on condition that the provider:

- (a) does not initiate the transmission;
- (b) does not select the receiver of the transmission; and
- (c) does not select or modify the information contained in the transmission.'

Article 14 exempts service providers from liability for hosting content:

'Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

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

In light of the *Godfrey v. Demon* case, where an ISP was unable to plead the defence of innocent dissemination (which is on a statutory basis in the UK) because they had not acted in response to a complaint from the plaintiff, there remains uncertainty about what constitutes acting 'expeditiously to remove or to disable access to the information' complained of (Lloyd 2004, pp. 692–699). Unfortunately, there is a dearth of case law on the Directive which makes it difficult, as yet, to see how far it differs from the American situation.

Similar to the US position, Article 15 makes it clear that there is no obligation on service providers to monitor content on their systems:

'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity.'

If one does choose to monitor, while *Batzel* makes it clear that the level of intervention which one may undertake while retaining protection under American law is high, the risk of losing immunity under Articles 12 and 14 of the Electronic



Commerce Directive is obvious. This is a strong argument against monitoring content posted by users.

Internationally, the general trend is that intermediaries are not absolutely liable for the actions of users unless they know or should know of illegal activity or they derive a direct benefit from it, although some jurisdictions, such as Singapore, do not extend this as far as hosted content (Reed 2004, Chapter 4). In order to avail of immunity, the OSP must have some procedure for dealing with complaints regarding material available on their systems and that this should operate without undue delay.

A solid notice-and-takedown procedure is therefore essential. This compromise between monitoring and lack of control is good for OSPs but it should be balanced with an awareness of the risks of overuse. The norm for UK ISPs seems to be automatic removal of material complained of (Lloyd 2004, 695–696), even though this is likely to lead to further difficulties with the user who posted the original content, who may be able to sue for breach of contract. From a broader perspective, abuse of notice-and-takedown procedures can have a chilling effect on speech on a global scale (Urban and Quilter 2006).

## 4 Conclusion

User-supplied or UGC websites are another iteration in the continued and always surprising development of the Internet as a global communications medium. As this technology develops, information systems developers should be conscious of the legal risks involved. This raises different challenges for different members of the ISD community. Educators must ensure that their students have a proper awareness of the interaction between laws and new technologies and the gaps that can be created by the pace of change. Practitioners must bear the legal framework within which their finished product will be used in mind when designing it. Researchers must attempt to bridge the gap between the worlds of law and technology so that each can communicate with the other.

The immediate challenge is dealing with the reality that users may post material which infringes copyright, is defamatory or otherwise objectionable. Relying solely on indemnities or ignoring risks by complying only with local laws are probably inadequate strategies in the long term. Moderating content is too resource-intensive and filtering technologies are not yet, and may never be, practical.

Developers should therefore ensure that new sites and services can avail of the safe harbours in the countries which are their primary focus. This will generally involve a robust but balanced notice-and-takedown procedure.

## References

- Akester, P. (2005). Copyright and the P2P Challenge. *European Intellectual Property Review* 27, 106–112.
- Batzel v. Kremers* 333 F.3d 1018 (9th Cir. 2003).
- Carolan, M. (2006) Man avoids jail after material about barrister removed from website. *Irish Times*, November 24, 2006.
- CBS Songs v. Amstrad Consumer Electronics* [1988] AC 1013.
- Clark, R. and Smyth, S. (2005) *Intellectual Property Law in Ireland*. Tottel, Haywards Heath.
- Collins, J. (2006) When online gets out of line. *Irish Times*, November 25, 2006.
- Computer and Telecommunications Law Review (2007). Case Comment. Computer and Telecommunications Law Review 13, N115.
- fCubby Inc. v. CompuServe Inc.* 776 F Suppl. 135 (SDNY 1991).
- Gatt, A. (2002) Electronic Commerce — Click-Wrap Agreements. Computer Law and Security Report 18, 404–410.
- Godfrey v. Demon* (1999) EMLR 542.
- Goldsmith, J. and Wu, T. (2006) *Who Controls the Internet? Illusions of a Borderless World*. Oxford University Press, Oxford.
- Holmes, S. and Ganley, P. (2007) User-generated Content and the Law. *Journal of Intellectual Property Law and Practice* 2, 338–344.
- Johnson, P. (2003) All Wrapped Up? A Review Of The Enforceability Of “Shrink-Wrap” and “Click-Wrap” Licences in the United Kingdom and the United States. *European Intellectual Property Review* 25, 98–102.
- Levine, R. (2006) Billy Bragg’s MySpace Protest Movement. *New York Times*, July 31, 2006.
- Lloyd, I. (2004) *Information Technology Law*. Oxford University Press, Oxford.
- McGonagle, M. (2003) *Media Law*. Round Hall, Dublin.
- McIntyre, T.J. (2004) Online Anonymity: Some Legal Issues. *Commercial Law Practitioner* 11, 90–95.
- McMahon, B. and Binchy, W. (2000) *Law of Torts*. LexisNexis, Dublin.
- Metro-Goldwyn-Mayer Inc. v. Grokster Inc.* 545 U.S. 913 (2005).
- Miles, J. and Caunt, D. (2007) Brave New World. *Copyright World* 168, 24–26.
- Orlowski, A. (2006) Billy Bragg prompts Myspace rethink. *The Register*, June 8, 2006, available at [http://www.theregister.co.uk/2006/06/08/billy\\_bragg\\_myspace/](http://www.theregister.co.uk/2006/06/08/billy_bragg_myspace/).
- Playboy v. Frena* 839 F Suppl 1552 (MD FL, 1993).
- Reed, C. (2004) *Internet Law*. Cambridge University Press, Cambridge.
- Religious Technology Centre v. Netcom On-line Communications Services Inc.* 907 F Suppl. 1361 (ND Cal.1995).
- Samuelson, P. (2006). Three Reactions to *MGM v. Grokster*. *Michigan Telecommunications Technology Law Review*, 13, 177–196.
- Sony Corporation of America v. Universal Studios* 464 U.S. 417 (1984).
- Stratton Oakmont Inc. v. Prodigy Services Co.* 23 Media Law Reports 1794 (NY Sup. Ct. 1995).
- Timmons, H. and Pfanner, E. (2006) U.S. Law Causing Turmoil in Online Gambling Industry. *New York Times*, November 1, 2006.
- Urban, J.M. and Quilter, L. (2006). Efficient Process or “Chilling Effects”? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer and High Technology Law Journal*, 22, 621–693.
- Williams, M. and Seet, S. (2006) Authorisation in the Digital Age: Copyright Liability in Australia after *Cooper* and *Kazaa*. *Computer and Telecommunications Law Review* 12, 74–77.
- Zeran v. America Online Inc.* 129 F.3d 327 (4th Cir. 1997).

Information Systems Development  
Challenges in Practice, Theory, and Education Volume 2  
Barry, C.; Conboy, K.; Lang, M.; Wojtkowski, G.;  
Wojtkowski, W. (Eds.)  
2009, VIII, 560 p., Hardcover  
ISBN: 978-0-387-78577-6