

Online Content: Risks and Rewards



► **Inside**

Introduction

Overview

Legal Risks of User Generated Content

Maintaining legal defences

Tips on minimising the risks



Introduction

With digital content becoming ever more popular and users becoming more sophisticated, all those involved in the online publishing industry need to be aware of the risks that come with the rewards of digital content.

As user generated content (“UGC”) appears on more and more websites, operators of those websites have to decide how to deal with such content. Setting up procedures to remove undesirable or illegal content from a website may seem the obvious choice but the desire to protect a brand in this way can create legal problems for the operator of the relevant website.

Overview

It is clear enough to a brand owner that if they publish content on a website there will be a variety of rules with which to comply ranging from intellectual property and data laws to the more recent consumer protection legislation. However, many companies want to take advantage of the creativity and honesty that comes from UGC. As this type of content is not created by the operator of the website, does the operator have to take responsibility for that content? This inbrief sets out an overview of the legal risks of UGC and the related legal defences.

Legal risks of Online Content

Intellectual property rights infringement UGC is likely to attract copyright protection. If the contributor is the author, they will own the copyright and this content will need to be licensed to the operator if the operator intends to make any use of the content. The website operator should include suitable licence terms in the conditions of use of the site and ensure that a user agrees to these before the content is posted.

There is always a significant likelihood that UGC will incorporate content that is not owned by the person uploading that content which then gives rise to a risk that third party intellectual property rights (“IPR”) may be infringed.

A film clip posted online for example will contain a number of different rights held by one or more third parties. Permission may be required from the owners of the copyright in the film recording itself, scriptwriters, actors, brand owners, owners of the film location, the soundtrack and the underlying composition. Unless the relevant rights have been obtained, uploading such content will infringe third party IPR.

When UGC of any kind is uploaded by users, the user should be asked to confirm that the material does not infringe any third party rights and that the user owns the material or has permission to upload it. However, such contractual remedies for the website operator may have limited benefit if the user has no financial means or cannot be readily identified.

Defamation

Any person who repeats or republishes a defamatory statement, or who is in any way involved in its publication, is also potentially liable in a defamation claim. The law of defamation recently underwent a major shake-up, the implications of which are still rattling through the courts. A statement is defamatory if it causes or is likely to cause “serious harm”. In relation to businesses, that means economic loss.

In the context of UGC, the operator of the website is more at risk because it will be easier for a claimant to identify the operator and may choose to pursue the operator of the site rather than the actual author of the defamatory statement. Despite the statement being made by a user rather than the operator of the site, liability could still arise if the operator is involved in its publication and aware of the content.

Unfair Commercial Practices

Recent consumer protection legislation raises additional legal risks. The Consumer Protection from Unfair Trading Regulations 2008 (“CPRs”) prohibit unfair commercial practices generally and 31 practices are specifically listed as prohibited including the offence of “falsely representing oneself as a consumer”. Websites which include product reviews run the risk of breaching the CPRs. For example, a user from one company posing as a consumer to post a review of a competitor’s products will be a prohibited practice. The risk for the website operator is if the enforcing agency decides the publication of the review on the site creates the impression that the trader is a consumer. And don’t forget, if brands adopt and incorporate UGC into their marketing materials, it may fall within the ASA’s remit and the CAP Code will apply. Examples of what can constitute ‘adopting and incorporating’ include placing UGC on a brand’s YouTube channel (regardless of whether it directly promotes the brand or not) and removing only negative comments from an online ratings and review section.

The CPRs do contain a “due diligence defence” which may enable a website operator to avoid the commission of the offence. This applies if the misleading material is posted by another person and the operator took reasonable precautions to avoid the offence. The operator should:

- ask users to confirm they are consumers



and to declare any relevant interest in the product before submitting their review;

- monitor the information provided by the user for anything that raises suspicion, such as a reviewer with an email address “@nike.com” posting a poor review of an adidas product; and
- check the content for any other indications it is not a genuine consumer (which will depend on the particular subject matter and circumstances).

Privacy

Where users are asked to register with the website prior to submitting UGC, personal data will be collected and the website operator will need to have a privacy policy detailing what it intends to do with the data submitted. Users should be asked to confirm they agree with the privacy policy before submitting any UGC.

In particular, if a user uploads a photograph this may constitute personal data (including personal data of third parties if the photo shows someone other than the user) and the user will need to consent to the photograph being used by the website operator in the same way as other personal data.

Other unlawful content

Online content will also be unlawful if it is sexually explicit, obscene, incites racism, hatred or terrorism and or is otherwise offensive to a certain section of society.

Maintaining Legal Defences

The law provides a number of defences to the possible claims identified above and the operator of a website needs to assess these defences against the commercial benefit of maintaining the particular content on its website. It is possible that by choosing to take a more active interest in the content of the website (for example by taking responsibility for moderating that content) an operator may lose its right to rely on these defences and will become liable for content which it did not itself create.

Where websites contain UGC, the decision as to whether or not to moderate the website can be challenging one and requires careful balancing of

the commercial and legal risks. For further tips, see our sister inbrief on Website Moderation.

Safe Harbour Defences

Website operators who simply host websites in the EU may be able to take advantage of the defences in the E-Commerce Regulations 2002 which provide protection from liability provided that the operators:

- have no actual knowledge of unlawful activity or information;
- are not aware of facts or circumstances from which it would have been apparent that activity or information was unlawful;
- on becoming aware, act expeditiously to remove or disable access to information; and
- the recipient of the material is not acting under the authority or control of the operator.

An operator who does not check content before it is displayed on the page is likely to be able to take advantage of the above defence. The site should have a “notify and take down” policy to ensure it acts “expeditiously” to remove or disable access to any problematic material. As soon as the operator has notice of the alleged infringement it should then remove the material. Whilst the E-Commerce Regulations don’t explain what is meant by “expeditiously”, section 3 of the Terrorism Act 2006 requires material published electronically to be removed within two working days of a notice under that Act requiring its removal. Although this Act will not apply to all publications it gives a clear reference point. Liability arises from the point at which the operator becomes aware or could reasonably have been aware from the surrounding facts so it is likely to be safer to take down the material first and ask questions later.

Innocent Dissemination

The Defamation Act 1996 contains a similar “internet defence” specific to defamatory statements, provided that the website operator acts with “reasonable care”. This defence is in addition to the general defences of proving the truth of the statement or that it is objectively fair comment on proven facts). If the relevant website operator is not the author, editor or publisher of

the defamatory statement and takes reasonable care in relation to its publication and does not know or have reason to believe that it caused or contributed to the publication of the defamatory statement, then the operator will avoid liability.

A website operator will not come within the definitions of “author”, “editor” or “publisher” in the Defamation Act if all they do is provide access or make available a system which transmits the statement but have no effective control over that system. In such cases, the website operator will be classed as an “innocent disseminator” of the information and will be able to rely on the legal defence to avoid liability.

The Act does not explain what is meant by “reasonable care”. However, in a recent case, Google (on appeal) was held not to have acted quickly enough in removing material (it took Google five weeks to act after first being contacted). However, Google was not ultimately liable as the Claimant lost on another point. Nevertheless, the lesson to learn is that acting quickly is the safest choice.

The Defamation Act 2013 has introduced a further line of defence designed specifically for website operators, based upon a “notice and take-down” procedure. If the website operator fulfils the requirements of that procedure, it has a complete defence to a claim.

Tips on Minimising the Risks

This area of law is continually developing as ongoing cases in the US (which will no doubt have ramifications for the UK and other European-based operators) attempt to establish the extent of liability of an internet service provider for the content of their websites.

Websites’ terms of use for sites which allow UGC should always include:

- suitable warranties and indemnities from the user in relation to the content which is uploaded (although operators should bear in mind these will only be of benefit if the user can pay);
- a mechanism enabling users to complain about a particular posting (i.e. a hyperlink such as “Complain about this content” or

“Report abuse”);

- clear complaints procedure which enables the operator of the site to deal with the complaint quickly and explains the procedure for complaints;
- clear “notice and take down” policy which permits the site operator to remove or block access to material once an allegation of problematic content is received; and
- separate privacy policy explaining what will happen to any data provided to the website operator.

**For further information
on this subject please contact:**

Jo Farmer

Partner

+ 44 (0)20 7074 8111

jo.farmer@lewissilkin.com