User Generated Content – Risks, Prevention & Protection for Service Providers in the UK: Part 2

Anthony Misquitta | April 2011

This is the second part of our two-part note on User Generated Content. Our **first note** discussed what UGC is, what the risks of UGC for internet and website service providers are, the ownership of UGC, copyright infringement and defamation. In this note we discuss **hatred**, **data protection and infringement of privacy and the impact of the Digital Economy Act 2010**.

6. Hatred

In the UK it is a criminal offence to incite hatred on the grounds of religion, race or sexual orientation, or to incite others to commit criminal acts.[1] Sites which allow users to upload their own content, however, may inadvertently create a forum for the publication and dissemination of materials which are intended or likely to stir up such hatred.

Previously, UK legislation incriminated service providers who allowed the publication of material that incited and provoked hatred, which was punishable by fine or imprisonment. However, the draft Electronic Commerce Directive (Hatred against Persons on Religious Grounds or on the Grounds of Sexual Orientation) Regulations 2010, which were published earlier this year, contain proposals to revise this stance. Service providers will be afforded greater protection from liability under the draft Regulations, as long as they do not select the recipient; or create, or monitor the offending material. Therefore, if service providers merely provide users with a means of storing information with the sole purpose of onward transmission, they will not be held to have committed an offence.

Under draft Regulation 7, a service provider who stores information will only be liable if it:

- knew that the information was intended to stir up religious hatred or hatred on the grounds of sexual orientation; or
- failed to expeditiously remove the information or disable access to it when he had actual knowledge that the material was threatening or intended to incite hatred.

Risk Prevention

In reality, the necessity of knowledge and intention as component parts of an offence mean that a service provider is now far less likely to face liability. However, by way of suggested methods of prevention:

- Where possible do not store information for longer than is reasonably necessary;
- Do not modify the uploaded content in any way;
- Put in the written T&Cs of use of the website that any abusive material which it is reasonable to believe is intended to incite hatred on the above grounds, will not be tolerated;
- Enforce strict measures against any known offending individuals, such as disabling their access to upload content, if capacity is available.

7. Data Protection and Infringement of Privacy

Privacy law entitles an individual in the UK to a legitimate expectation of privacy. In addition, the EU's Data Protection Directive 95/46 and the UK's Data Protection Act 1998 ("the DPA") govern data protection of an individual's details in the public domain. However, given that the foundation of many social networking sites is to enable users to share their own, and potentially others', personal details (which may include sensitive personal data such as date of birth, family names, address, updated movements and whereabouts and so on), the websites sit uncomfortably within the current legislative framework. The question therefore becomes: what is a "legitimate" level of privacy and data protection that UGC website users can expect a service provider to provide?

The inherent risks involved are the misuse and abuse of the uploaded personal information. This may be by other users, which at worst results in identity fraud; or indeed by service providers themselves through the facilitation of, for example, behavioural advertising to which the users have not consented. Behavioural advertising / targeting can be used by online publishers or internet marketers to increase the effectiveness of campaigns by collecting data on an internet user's behaviour such as browsing habits, search queries, and web site history. This information is then used to serve more targeted advertisements to the user – the goal is to increase relevancy based on the collected data and foster a better conversion rate.

Commentators have suggested that the data protection framework under the DPA is inappropriate in a UGC social networking environment. As yet, there are very few cases involving liability for UGC that have reached trial, which would certainly help to clarify the parameters of the Act for service providers. However, Applause Store Productions Ltd v Raphael[2] sets a current precedent suggesting that courts should hold to account not only the individual who posted the infringing material but also the service provider. The decision inadvertently labelled the service provider as a "data controller" even though it is the user who "controls" the uploaded data. This case is therefore a warning to service providers to err on the side of caution as regards data protection.

Risk Prevention:

- Obtain consents for the issuing of a user's personal information (perhaps including more restrictive data fields for those under 18). This cannot be written in as a default term of the user T&Cs, but could be achieved by way of, for example, a specific "tick-box" indicating consent to a third party's use of the personal data for specified purposes, such as advertising;
- Obtain further consent and / or issue warnings at the point at which a user proposes to upload material which describes a third party;
- Provide default privacy settings before a user has tailored their own settings;
- Create advanced technological means by which users can define their own privacy settings;
- Create age-sensitive sections which are only accessible on confirmation that a user is over 18 to reduce the possibility that minors disclose inappropriate levels of their personal data to other users;
- Place clear and accessible Acceptable Use and User Etiquette policies on the website informing users of privacy risks and consequences of uploading information about others which has not been consented to; and
- Ensure users can control their personal data and uploaded content by way of deletion and updating.

8. The Impact of the Digital Economy Act 2010

The effects of the new Digital Economy Act 2010 ("the DEA") have yet to be seen, however, it is expected to update the IP and data protection framework to be better suited to service providers in the UGC context. Please refer to our **Watered down Digital Economy Act 2010 passed in "wash up" procedure** briefing for further information on this legislation.

The greatest impact of the DEA upon UGC service providers will be in relation to online copyright infringement which envisages service providers taking a more active and perhaps more onerous role in monitoring and policing their websites for persistent offenders of copyright infringement, by implementing a set of monitoring and reporting obligations, the final form of which will be prepared by OFCOM early in 2011. These obligations, for which some service providers will have to contribute 25% of the cost of actioning, may include:

- Compiling Copyright Infringement Reports of users who have committed copyright infringement and about which the service provider has been alerted;
- Issuing a Notification to a user who exceeds a certain infringement threshold, as defined by OFCOM, warning them to refrain from further infringements; and
- Taking appropriate action against a user who has exceeded the threshold by, for example, suspending the subscriber's access to the website.

The DEA implements the penalties for service providers who fail to adequately adhere to these obligations which can include a fine of up to £250,000, issued by OFCOM, and Court-ordered blocking injunctions (at the service provider's expense). The recent draft of OFCOM's "Initial Obligations Code" indicates that the above obligations will only apply to service providers with more than 400,000 subscribers such as BT, Post Office, Sky, Talk Talk, Virgin Media, O_2 and Orange. This means that small ISP, mobile operators and wi-fi providers such as hotels and coffee shops will be initially exempt.

Service providers should however be aware that, in deciding whether to grant an injunction, the court will have to consider the extent to which the service provider has attempted to comply with the DEA and prevent copyright infringement on its site. Therefore, it is advisable as a method of both prevention and protection against such penalties for service providers to adopt a conscientious approach and the risk prevention suggestions above.

If you require further information on anything covered in this bulletin please contact **Anthony Misquitta** or your usual contact at the firm on 020 3375 7000.

This publication is a general summary of the law. It should not replace legal advice tailored to your specific circumstances.

1 [2008] EWHC 1781 (QB)
2 Relevant legislation includes: the Crime and Disorder Act 1998, Criminal Justice Act 2003, Racial and Religious Hatred Act 2006 and the Criminal Justice and Immigration Act 2008.