

1.3: Web 2.0 and Legal Issues Factsheet

Naomi Korn and Professor Charles Oppenheim, March 2009

Context

This resource is based upon the IPR Toolkit created by the JISC-funded Web2Rights Project (www.web2rights.org.uk) and adapted for SCA sponsors and other organisations across the public sector. It is intended to form part of a toolkit, which can be further adapted to suit specific requirements and issued to content creators and content users across the public sector who are responsible for rights management and rights clearances. This paper provides a brief overview of some of the other types of legal issues that public-sector bodies may encounter when engaging with e-content.

General

There are many legal ramifications that need to be addressed by public-sector bodies when dealing with e-content, the risk of which increase with Web 2.0 engagement. These issues include defamatory, race hate, terrorist-encouraging and pornographic materials being posted, identity theft and privacy/data protection. The overview below provides a brief summary of some of the key issues.

Data Protection

If you are dealing with information about individuals then you will need to consider the Data Protection Act 1998. This Act applies to personal data about living, identifiable individuals. Thus, if you collate information about users (for instance people contributing to a wiki), which might include personal details such as name and email address, then the Data Protection Act will apply.

The Act imposes obligations on the data controller. A data controller is the organisation that makes the decisions as to how and why personal data is to be processed. Processing data includes reading, using, amending, storing and deleting the data. Even where the information is passed to a third party to be processed, the data controller will remain liable for the obligations under the Data Protection Act where the controller is the entity that specifies what should be done with the data during processing. If you use, store and/or delete information about the users then it is likely you fall under the definition of data controller.

Data Protection Principles

The Act requires the data controller to act in accordance with eight principles:

- Personal data shall be processed fairly and lawfully
- Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
- Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
- Personal data shall be accurate and, where necessary, kept up to date

- Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
- Personal data shall be processed in accordance with the rights of data subjects under this Act
- Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
- Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Sensitive Personal Data

Where personal data is 'sensitive', then the data controller has additional responsibilities. Data becomes sensitive if it includes any of the following types of information about an identifiable, living individual:

- Racial or ethnic origin
- Political opinions
- Religious beliefs
- Trade union membership
- Physical or mental health
- Sexual life
- Commission of offences or alleged offences

In general, consent to processing such data can only be granted with explicit written consent of contributors obtained before processing the data.

Any plan developed for the purposes of defining the organisation's copyright strategy can be used to define a data protection strategy. For a most useful Data Protection Compliance Check List, see: www.ico.gov.uk/upload/documents/pia_handbook_html/files/DP_checklist_final.doc

Retrieved from: www.web2rights.org.uk/team/wiki/index.php/Copyright_strategy

Freedom of Information

Public-sector bodies are subject to the Freedom of Information Act 2000 (or, for Scottish-based institutions, the Freedom of Information (Scotland) Act 2002). This requires institutions to have adopted a publications scheme, giving details of routinely produced information and how it may be obtained, and it requires institutions to supply information upon request (subject to certain exceptions).

Further information on the Freedom of Information legislation is available in the JISC Legal Freedom of Information Act 2000 Overview paper (www.jisclegal.ac.uk/freedomofinformation/freedomofinformation.htm) and the JISC Legal The Freedom of Information 2000 Essentials paper (www.jisclegal.ac.uk/freedomofinformation/FOIEssentials.htm).

Accessibility

Accessibility laws are in place to ensure that services are accessible by users with disabilities. The Disability Discrimination Act 1995 (as amended by the Special Educational Needs and Disability Act 2001) requires service providers (including those offering education services) to ensure the accessibility of their services by users with disabilities. This includes a proactive duty to consider accessibility, and a requirement to make reasonable adjustments where necessary to allow access. Although the legal duty applies in relation to users with disabilities, accessibility should be seen in a positive light as benefiting all.

Prevention of Terrorism

The Terrorism Act 2006 aims to outlaw incitement to terrorist activities and will include incitement through websites and email communications and is of relevance to the educational sector. The Terrorism Act 2006 contains a comprehensive package of measures designed to ensure that the police, intelligence agencies and courts have the tools they require to tackle terrorism and bring perpetrators to justice. Although not specifically information technology related, new criminal offences have been created including:

- Acts Preparatory to Terrorism
- Encouragement to Terrorism
- Dissemination of Terrorist Publications
- Terrorist training offences

Many of these crimes may be committed or facilitated by computer use and public-sector bodies should play their part in ensuring that such crimes are not committed or facilitated on their computer systems. Reporting suspicious activity to the police is essential.

Universities and colleges are being urged by the UK government to take seriously the problem of extremism on their campuses. Practical guidance has been issued, which points out universities and colleges responsibilities within the law and clarifies the legal position (www.dfes.gov.uk/pns/DisplayPN.cgi?pn_id=2006_0170).

E-Security

This is generally taken to mean the laws and technologies involved in keeping information secure. Issues that may arise and their relationship to specific legal regulations include:

- The lawful interception of data under controlled conditions (The Regulation of Investigatory Powers Act (2000) and Regulation of Investigatory Powers (Scotland) Act (2000) (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (Lawful Business Regulations))
- Security of personal data (Data Protection Act 1998)
- Regulating the information to be made available via cookies and other tracking devices (The Privacy and Electronic Communications (EC Directive) Regulations 2003 (the Anti-Terrorism Crime and Security Act 2001))
- Also of relevance are the Prevention of Terrorism Act 2005 and the Terrorism Act 1996 (which permit orders to be made in specified circumstances prohibiting the use of inter alia the internet), and the Human Rights Act 1998.

Incitement of Racial Hatred

Inciting either racial or religious hatred is a criminal offence. Publishing and disseminating online materials that are likely to incite such hatred is also a criminal offence. As corporate entities, public-sector bodies have a responsibility not to publish and disseminate racist materials in any format including electronically. As well as the likely reputational damage, public-sector bodies have a general statutory duty under the Race Relations Act 1976 (as amended) in carrying out their functions, to consider the need to eliminate unlawful discrimination and to promote equality of opportunity and good relations between people of different racial groups. Incitement to racial hatred is governed by section 21 of the Public Order Act 1986, whilst the Racial and Religious Hatred Act 2006 makes it illegal to threaten people because of their religion, or to stir up hatred against a person because of their faith. It is designed to fill gaps in the current laws, which makes it illegal to threaten people on the basis of race or ethnic background. This Act extends to England and Wales only.

Retrieved from "www.web2rights.org.uk/team/wiki/index.php/Obscenity%2C_Libel_etc"

Retrieved from "www.web2rights.org.uk/team/wiki/index.php/General_Issues_Paper_%28this_information_is_based_upon_resources_created_by_JISC_Legal%29"

Defamatory, Obscene and other Unlawful Content

Of particular concern to the providers of next-generation technologies may be the potential liability for hosting infringing material (for example if contributors post defamatory or obscene material or works which infringe copyright). The E-commerce Directive and Regulations provide for some immunity against liability for a service provider that hosts, caches or acts as a conduit for unlawful content so long as certain criteria are met. Broadly the service provider who hosts or caches unlawful information will not be liable for damages or for any other pecuniary remedy or for any criminal sanction so long as they do not have actual knowledge of the unlawful activity or information and is not aware of facts or circumstances from which it would have been apparent that the activity or information was unlawful. Neither should the service provider have had a hand in transmitting or in any way altering the information. Please note that the E-Commerce Directive and Regulations do not apply to ISPs located outside the European Union. So if the plan is to use an ISP located in the USA, make sure that the service complies with USA legislation.

Although the rules are somewhat complex (for instance they do not state what is meant by expeditiously, nor how actual knowledge is obtained by a service provider), in general service providers have sought to mitigate liability that might arise by putting into place a notice and take-down procedure and by making the service subject to specific terms and conditions (which usually exclude liability of the service provider). Such terms and conditions can be found on the website of the service provider. Most notice and take-down procedures provide that when a service provider receives notice that allegedly infringing material is on the site and/or on the equipment operated by the service provider, then the material is removed. While instituting such a procedure is good practice, there are factors that providers of Web 2.0 technologies within the public sector might like to consider:

- The procedure for taking down allegedly infringing material. Will any investigation be made as to the identity and provenance of the complainer prior to removing the material?
- Put-back procedure. Will the service provider consider instituting a 'put-back' procedure whereby the material is automatically re-instated should it be found to be non-infringing?

A number of jurisdictions are starting to require service providers to install filtering software (dealing notably with material that infringes copyright) in order to maintain immunity from suit. Whereas liability in these cases tends to arise where the provider of the next-generation technology is profiting from a business model that infringes copyright belonging to third parties (such as a service that makes clips of videos available whilst profiting from advertising revenue), some thought might be given to the possibility of building filtering tools in educational Web 2.0 technologies.

Contempt of Court

Although perhaps less likely to arise than the other issues with regards to the legal issues arising from engagement with next-generation technologies, disregard for the authority of the courts of justice, eg ignoring a court order, is a criminal offence.

Whilst we hope you find the contents of the SCA IPR Toolkit useful and informative, the contents are for general advice and best practice purposes only and do not constitute legal advice. Although we believe the contents are up to date and accurate as well as a true representation of best practice advice, we can give no assurances or warranty regarding the accuracy, currency or applicability of any of the contents in relation to specific situations and particular circumstances. In such circumstances, appropriate professional legal advice should always be sought.

© HEFCE, on behalf of JISC. The contents of this IPR Toolkit are licensed for use under a Creative Commons Attribution-Non-Commercial 2.0 UK: England & Wales Licence.