CREW Project - Legal and Ethical Issues

Nikki Rogers (CREW Project) & Andrew Charlesworth (Centre for IT & Law), University of Bristol.

Version 1.0 (13 February 2009)

Contents

Collaborative Research Events on the Web (CREW*)*
JISC Virtual Research Environments Programme

Start Date: 1 March 2007
End Date: 28 February 2009
Lead Institution: University of Manchester
Partner Institutions: University of Bristol

Co-Investigators: Michael Daw, Nikki Rogers, Rob Procter, Caroline Williams, Andy Hall
Project Manager: Michael Daw   e-mail: michael.daw@manchester.ac.uk

Project Web URL: http://www.crew-vre.net

Executive Summary

The Collaborative Research Events on the Web (CREW) project aims to improve access to research event content, by creating an architecture for capturing and publishing the scholarly communication that occurs at events like conferences and workshops. The Repository of AG Collaborative Events (RACE) project aims to build a digital repository service of collaborative research events, such as seminars, conferences, workshops, and training and teaching events, by building on the CREW architecture in order to record and annotate Access Grid (AG) events.

A review of the current literature, carried out by the authors, surrounding the use of both videoconferencing and the AG, suggests that, to date, little or no work has been published which directly assesses the social, legal and ethical issues relevant to either the development and use of the CREW architecture generally, or the specific functionality envisaged by the RACE project. Consideration of such issues will be a necessary step in the wider deployment and use of the CREW architecture by the stakeholder groups: events services, event organisers, and researchers.

While a specific social, legal and ethical literature for the work undertaken by CREW and RACE is not currently available, more general literature provides some indicators of issues that will need to be considered. In the legal arena, key legal areas will probably be:

- intellectual property law, notably copyright and related rights, possibly patent law and trade secrets;
- data protection law, privacy and confidentiality law;
- content liability laws, notably defamation law;
- freedom of information law.

The legal issues are likely to run in tandem with, and be influenced by, normative and ethical considerations particular to the cultural understandings prevalent within each of the range of subject disciplines represented in the broad UK research community.

Incorporating the CREW architecture into discipline-specific events is likely to raise more issues of 'culture shock' in conservative disciplines (e.g. law) than in disciplines already open to, or engaged in the use of, increasingly sophisticated mechanisms for providing wider access to, and sharing of, research data and outputs (e.g. computer science). Such 'culture shock' may be expressed as opposition grounded in existing norms (e.g. "That's not how things are done in this discipline because…"), and/or by recourse to arguments claiming legal justifications for non-engagement (e.g. "You can't do that, it breaches data protection laws"). Stakeholders seeking to incorporate the CREW architecture into their processes will need to consider how to structure their approaches so such normative/ legal objections can be avoided, or their effect ameliorated.

Developing such approaches will require stakeholders of all kinds to engage in risk assessment processes. They will need to:

- identify the issues that may hinder adoption or use of the CREW architecture, legal or normative;
- assess the degree of risk inherent in those issues in the context in which they are operating;
- where the risks suggest it to be necessary, develop options for effective compliance with particular legal obligations, or research community norms.

Legal issues are rarely insurmountable if dealt with in a timely and structured fashion, but Lack of a risk assessment usually results in poor strategies or processes for addressing particular issues, and failure to allocate sufficient resources to effectively address problems. A strategy of encouraging CREW stakeholders to discuss (and document) good practice in the practical handling of legal risks in the use of CREW technology will be an essential part of ingraining effective legal compliance processes into a rapidly developing field.

Glossary and Abbreviations

AG	Access Grid. An advanced videoconferencing application that uses audio and video tools, allowing people in different locations worldwide to meet in a virtual venue (virtual meeting room).
CDPA 1988	Copyright, Designs and Patents Act 1988
CREW	Collaborative Research Events on the Web (JISC). The project aims to improve access to research event content by capturing and publishing the scholarly communication that occurs at events like conferences and workshops. The project is developing tools to enable presentations and similar sessions to be recorded and annotated and enable powerful searches across distributed conference and related research data.
DPA 1998	Data Protection Act 1998
EU	European Union
FOIA 2000	Freedom of Information Act 2000
NDA	Non-Disclosure Agreement. Legally binding agreement between parties to a discussion or event, that some or all elements of that discussion or event are to be treated as confidential Often used in circumstances where a party wishes to discuss potentially patentable material with third parties, without compromising the requirement that the material not be made public prior to patent filing.
IPRs	Intellectual Property Rights. A bundle of exclusive rights over creations of the mind. Intellectual property rights include copyrights, trademarks, patents, design rights and trade secrets.
RACE	Repository of Access Grid Collaborative Events (JISC). The project proposes to build a digital repository service of collaborative research events such as seminars, conferences, workshops, and training and teaching events. This repository service will archive such sessions and allow for its content to be searched, browsed through and retrieved via existing and established repository search services.
VO	Virtual organisation. In this context, a user group that wishes to share resources (including annotations) within their group but not publically.

Section A - Technical Overview of the CREW Project

CREW Stakeholder Groups

An Events Service

The CREW project recognises the following types of organisation may wish to offer a research events service from which “end-users” can access event outputs.

A Virtual Organisation (VO)

A VO may host events – for example a seminar series, or regular conferences, and wish to disseminate event outputs for its members (only) to access. The outputs may include a variety of event-related content, for example, detail about presenters and delegates, the recorded presentations, the papers and informal comments made by attendees (in the form of annotations). This organisation may span several “real-world” organisations, meaning that its end users may have institutional login usernames and passwords managed by different services - for example some of the group members may be from the NHS, some from several different UK Universities.[1]

A National Service

A national service for Higher Education may wish to disseminate information about past and forthcoming research events as an online resource to the UK academic community. This is the case with one of the CREW project partners, Intute. Intute currently employs cataloguers to filter information about forthcoming events relating to several academic disciplines and disseminates this data via its public website.[2] An extended service could harvest fuller data from Event Providers and/or allow Event providers to enter data to their service via a Web Form for event entry. It could support Web 2.0 technologies to allow researchers to annotate events and recordings of events. It could potentially link its national service with a Video Archive service,[3] and thus operate in a distributed architectural setting. In such a scenario, core events content is drawn from a central events service, video content is linked to and streamed “on demand” from a video archive service, and annotations are securely stored in an annotations service. How these components interoperate is discussed further below in relation to ***Diagram 1***. As well as openly listing ‘public’ information about research events, this national service could also support the requirements of a VO by allowing some events only to be listed for logged-in users only, where they are verified to possess the necessary VO membership credentials.

An Event Organiser

An event organiser may wish to disseminate content relating to its event(s) via a national service or VO website, as discussed in the previous paragraphs.

Researchers

A researcher (or anyone who has an interest in research event outputs) may wish to access event information following an event they have attended; perhaps to replay a recording of a presentation they were not able to attend during parallel sessions, or to replay a recorded excerpt to a research colleague

[1] E.g. the CREW project’s Institute for Health Studies (IHS) stakeholder group based at Manchester University.

[2] See, for example, Intute: Social Sciences: Seminars and Events http://www.intute.ac.uk/socialsciences/events.html

[3] As is under investigation in the current JISC-funded RACE project - Repository of AG Collaborative Events (RACE) http://www.rcs.manchester.ac.uk/research/race

back at the office. Those who have not attended events in person may still wish to look at event content. A researcher may want to search or browse for future events in their field, or a related field of research; to review what other researchers have commented about various presentations; to add their own comments to seminars of interest; or to link flickr photos, or blog items, to events they were present at, and so on.

When a researcher makes a comment – we call this an annotation - on an event page in the CREW Events website they must be logged in so that the CREW application can track their comment. They may wish to mark their annotation as destined for private, VO or public consumption. If private, then they only will be able to view the annotation when logged in. If for a VO. then all VO. members will be able to view the annotation when logged in. If for public consumption then all will be able to view the annotation whether logged in or not.

Presenters

A presenter at a event may be recorded by the Crew Access Grid Recorder and, if they are using a PC or laptop, say for a PowerPoint presentation or demonstration of some kind then CREW can automatically record what is taking place on the screen displayed to the audience. At the same time, if the Live Annotations tool is being used, audience members may make informal comments about the content of the presentation. All this content is time-synced and fully integrated using CREW applications and will become replayable from the online website for Events after the speaker's presentation has taken place.

CREW High Level Architecture Diagram

The CREW architecture diagram given in ***Diagram 1*** is a high level, conceptual diagram, not intended to conform to any standard technical specification. The physical distances and proportions of particular items in the diagram are not necessarily relative. Its components are discussed below. The 'green' area represents the view layer through which some information may be captured from as well as offered to end users. For example, users are able to access information about events, including the ability to replay AG event recordings, and via the same user interfaces to contribute user annotations (whether "live" – i.e. during an event, or post event, to event pages displayed on the events website). The blue are is a middleware layer, with the dark blue area containing specifically CREW software applications.

Components in the View Layer

Search/Browse Events Website

The events website could be offered as a national service with a default, public view as well as a login option. It could alternatively be a VO-only website, only viewable by members of that VO.

The events website is coupled with the CREW Events service in technical terms, as the Events website is delivered as part of a web application with a JSP-based view layer and backed by a relational database – *database B* in ***Diagram 1***. *Database B* contains core data about events (e.g. titles, locations, organisations, delegate lists where available, names of speakers, session listings, links to online academic papers). It identifies all these types of resource with unique identifiers. Hence an annotation, stored in the Annotations service in *database D*, is stored with its link to the logged in user who made the annotation and the event page or the event recording the annotation relates to. Similarly for Access Grid video content, which is linked to events and stored in *database C.* The Authorisation service plays a key role in determining whether or not content from *databases B or C or D* should be "allowed" through to the view layer, depending on whether content is marked as for private, public or VO consumption, and also on the credentials of the logged in user. This is discussed in more detail for each of the 'middleware' layer components below.

Institutional Research Portal with event portlet

In this scenario, a portlet within an institutional portal delivers event content, most likely in a service oriented architecture whereby the portlet queries the CREW Events service in order to deliver content through the portal. At the time of writing, the CREW Project is trialling different approaches to delivering the range of functionality offered by the Search/browse Events Website via a portlet. The institutional portal would be typically offered to institutional members only and security built in to the portal framework and trust therefore delegated through the portal to the events service.

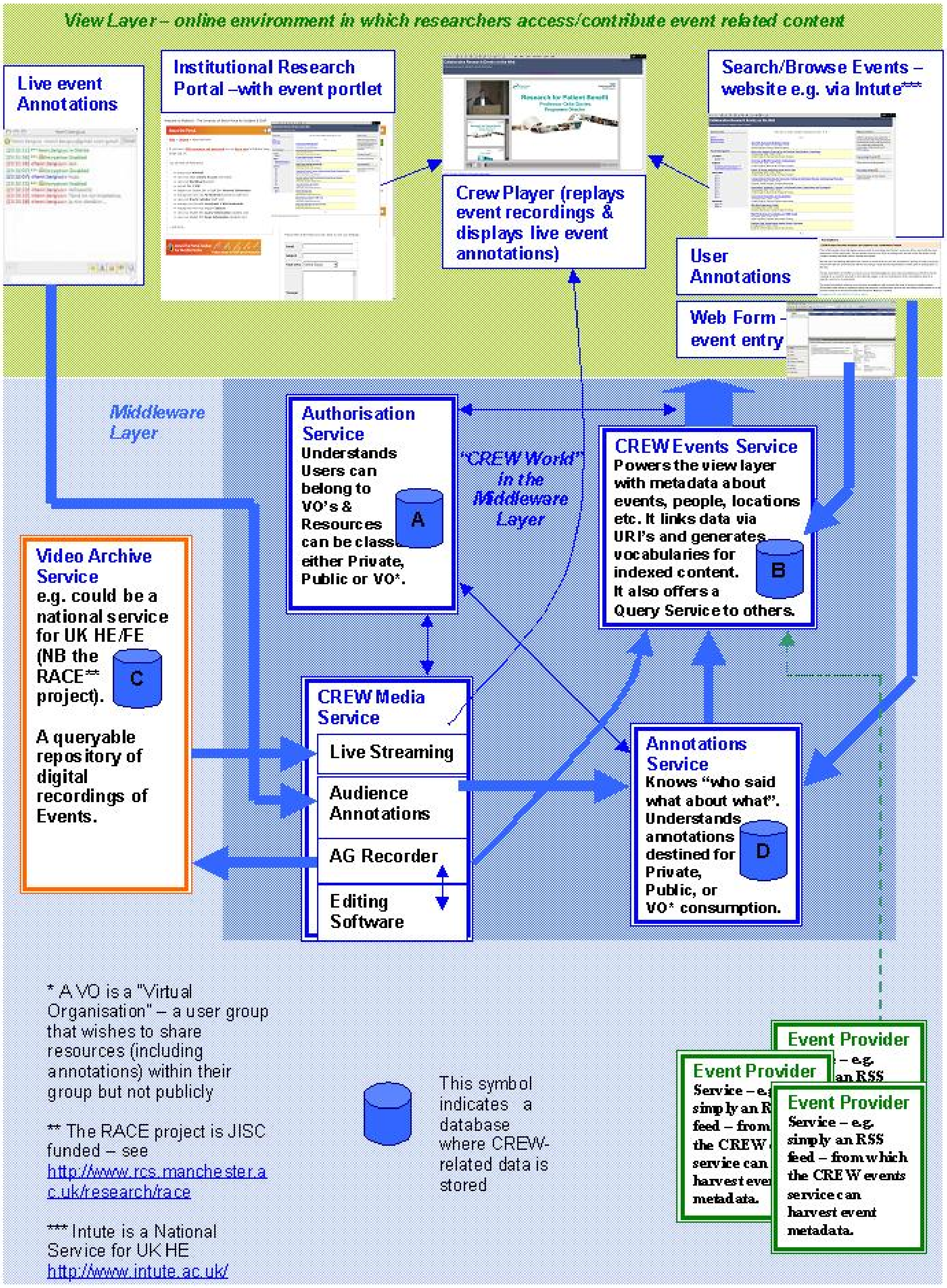

View Layer – online environment in which researchers access/contribute event related content
Live event Annotations
Institutional Research Portal –with event portlet
Crew Player (replays event recordings & displays live event annotations)
Search/Browse Events – website e.g. via Intute***
User Annotations
Web Form - event entry
Middleware Layer
Authorisation Service
Understands Users can belong to VO's & Resources can be classed either Private, Public or VO*.
A
"CREW World" in the Middleware Layer
CREW Events Service
Powers the view layer with metadata about events, people, locations etc. It links data via URI's and generates vocabularies for indexed content.
B
It also offers a Query Service to others.
Video Archive Service
e.g. could be a national service for UK HE/FE (NB the RACE** project).
C
A queryable repository of digital recordings of Events.
CREW Media Service
Live Streaming
Audience Annotations
AG Recorder
Editing Software
Annotations Service
Knows "who said what about what". Understands annotations destined for Private, Public, or VO* consumption.
D
* A VO is a "Virtual Organisation" – a user group that wishes to share resources (including annotations) within their group but not publicly
** The RACE project is JISC funded – see http://www.rcs.manchester.ac.uk/research/race
*** Intute is a National Service for UK HE http://www.intute.ac.uk/
This symbol indicates a database where CREW-related data is stored
Event Provider – e.g. an RSS
Event Provider Service – e.g. simply an R feed – from the CREW service can harvest even metadata.
Event Provider Service – e.g. simply an RSS feed – from which the CREW events service can harvest event metadata.

Diagram 1: Overview CREW Architecture

CREW Player

The CREW Player streams content from the video archive service and may only be launched from within the event portlet or the events website.

In this way, access to recorded content is only possible through the view layer. In the case that a user is not permitted to view a recording because of its availability only to a certain VO, then the link to the recording will not appear to the user in the event portlet or the event website, meaning they will not be able to access it. It is through the view layer, then, that security for recordings is enforced. The CREW player is coupled with the CREW Events Service and launches event recordings using their session identifiers. Session identifiers are stored in the CREW events service where they are protected by the authorisation service, and also in the video archive service. The video archive service is potentially “open” to other services in the online environment so we recognise that these session identifiers must not be “guessable” by other applications (for example they must not be obviously based on the event name or session they relate to).

Live Event Annotations

This component is offered as a website, with functionality similar to a Jabber chat room for example. It is made available to event audiences. Once logged in audience members are able to make annotations relating to a speaker’s presentation. This may be simply to record, textually, questions asked and answers given. Or it may be to link the topic under discussion to online references (people, projects, blogs and so on).

If the CREW recording toolkit is being used to capture an Access Grid session then all annotations made in this way will be time-synced to the recording. Later they will be displayed in the CREW player and made searchable from within the Search/Browse Events Website.

Live annotations are made only by logged in end-users and may be flagged for virtual organisation or public consumption.

Components in the Middleware Layer

CREW Events Service

The CREW Events service is the key component that offers core data to the view layer, as shown in ***Diagram 1***. It links data (e.g. people to events to organisations to presentations to recordings) via unique identifiers. The demonstrator CREW events service is currently online.[4] A default view will list all events available to a public audience. Login is provided for users who wish to make an annotation relating to an event, and for users who have VO membership and wish to see additional events classified only for VO members to access. The CREW Events Service acquires annotations from the Annotations Service via a query mechanism. Where events have been recorded using the AG Recorder, the event listing will have been passed as metadata to the CREW Events Service via the AG Recorder upload function. Via a similar upload function, any live annotations made during the recording of the event will have been uploaded to the Annotations service. For recorded events the view layer component (whether an institutional portal or Events website) will display a clickable link via which to launch the replay of that recording.

The linked data is stored in *database B*. *Database B* holds interlinked metadata about events and links to where additional content is held elsewhere online. *Database B* may also harvest data from remote Event provider services hosted elsewhere on the network.

[4] CREW Demonstrator
http://crew.rcs.manchester.ac.uk/Crew/

Whenever a request for that data is triggered by a view layer application such as the Events website, the CREW Events Service retrieves the appropriate data from *database B* and then performs a check using the Authorisation Service. The Authorisation service will check the user's logged in credentials (if indeed they are logged in) against the permissions attached to the event data requested. If the Authorisation Service finds that the user is not permitted to view that particular event information (either because it is private or available only to a particular VO) it denies access and the CREW Events Service will not deliver the requested information to the view layer. It will instead display an appropriate explanation to the end-user.

Video Archive Service and CREW Media Service

The Video Archive Service is not included in the darker blue area of the architectural diagram above – it is a remote service and is hence not in the "CREW world". Nonetheless it must be configured to respond to incoming requests for multimedia content which will have been triggered in the CREW case by an end-user launching the view layer CREW Player tool. The CREW Player tool receives streamed video content via the CREW Media Service. If the Video Archive service has been configured to "trust" an instance of the CREW Media Service, if it then receives a request for content from that service it will allow it to stream content to the CREW Player. As we have said earlier, the security of these requests for content is enforced in the view layer – and links to recorded content will not be provided in the view layer if they have not been authorised first by the Authorisation Service.

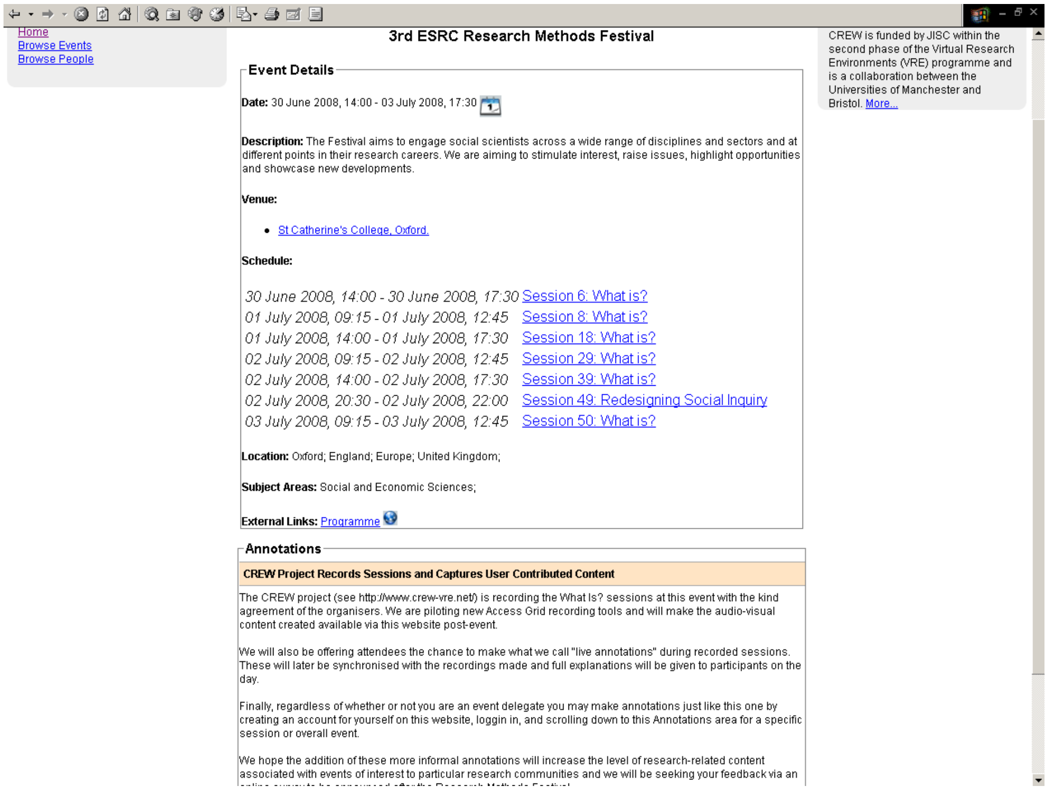
Authorisation Service

As shown in the architecture diagram above, this service is backed by *database A. Database A* stores the names of all users who may log in to the CREW Events Service, their unique identifiers, their email addresses, and any VO membership details. It also stores the unique identifiers of event resources stored in database B of the CREW Events Service and annotations in *database D* of the Annotations Service. It stores the access permissions relating to these resources: event information may be classified as for public or VO consumption, and annotations may be classified as for private, public or VO consumption.

In technical terms, the CREW authorisation service is being implemented using the Java Swing framework support for Access Control Lists and some additional logic provided by a bespoke Gatekeeper Java component. Authentication information is stored in a relational database accessed by JDBC in the CREW events service J2EE web application.

Annotations Service

The annotations service acquires its data from two applications in the view layer – the User Annotations part of the Events Website (see ***Diagram 2***) and also live audience annotations submitted via the CREW AG Recording Toolkit. The Annotations Service records user names and identifiers, linked to annotations and whether annotations are destined for private, public or VO access. The CREW Events Service may query it for data to pass through to the view layer and these two components are in the "CREW World" of the middleware layer, meaning that they have a trust relationship and can securely exchange data. Annotations will only make it through to the view layer after the appropriate security checks have been performed by the Authorisation Service, as described above.



Home
Browse Events
Browse People

3rd ESRC Research Methods Festival

CREW is funded by JISC within the second phase of the Virtual Research Environments (VRE) programme and is a collaboration between the Universities of Manchester and Bristol. More...

Event Details

Date: 30 June 2008, 14:00 - 03 July 2008, 17:30

Description: The Festival aims to engage social scientists across a wide range of disciplines and sectors and at different points in their research careers. We are aiming to stimulate interest, raise issues, highlight opportunities and showcase new developments.

Venue:

- St Catherine's College, Oxford.

Schedule:

30 June 2008, 14:00 - 30 June 2008, 17:30	Session 6: What is?
01 July 2008, 09:15 - 01 July 2008, 12:45	Session 8: What is?
01 July 2008, 14:00 - 01 July 2008, 17:30	Session 18: What is?
02 July 2008, 09:15 - 02 July 2008, 12:45	Session 29: What is?
02 July 2008, 14:00 - 02 July 2008, 17:30	Session 39: What is?
02 July 2008, 20:30 - 02 July 2008, 22:00	Session 49: Redesigning Social Inquiry
03 July 2008, 09:15 - 03 July 2008, 12:45	Session 50: What is?

Location: Oxford; England; Europe; United Kingdom;

Subject Areas: Social and Economic Sciences;

External Links: Programme

Annotations

CREW Project Records Sessions and Captures User Contributed Content

The CREW project (see http://www.crew-vre.net/) is recording the What Is? sessions at this event with the kind agreement of the organisers. We are piloting new Access Grid recording tools and will make the audio-visual content created available via this website post-event.

We will also be offering attendees the chance to make what we call "live annotations" during recorded sessions. These will later be synchronised with the recordings made and full explanations will be given to participants on the day.

Finally, regardless of whether or not you are an event delegate you may make annotations just like this one by creating an account for yourself on this website, loggin in, and scrolling down to this Annotations area for a specific session or overall event.

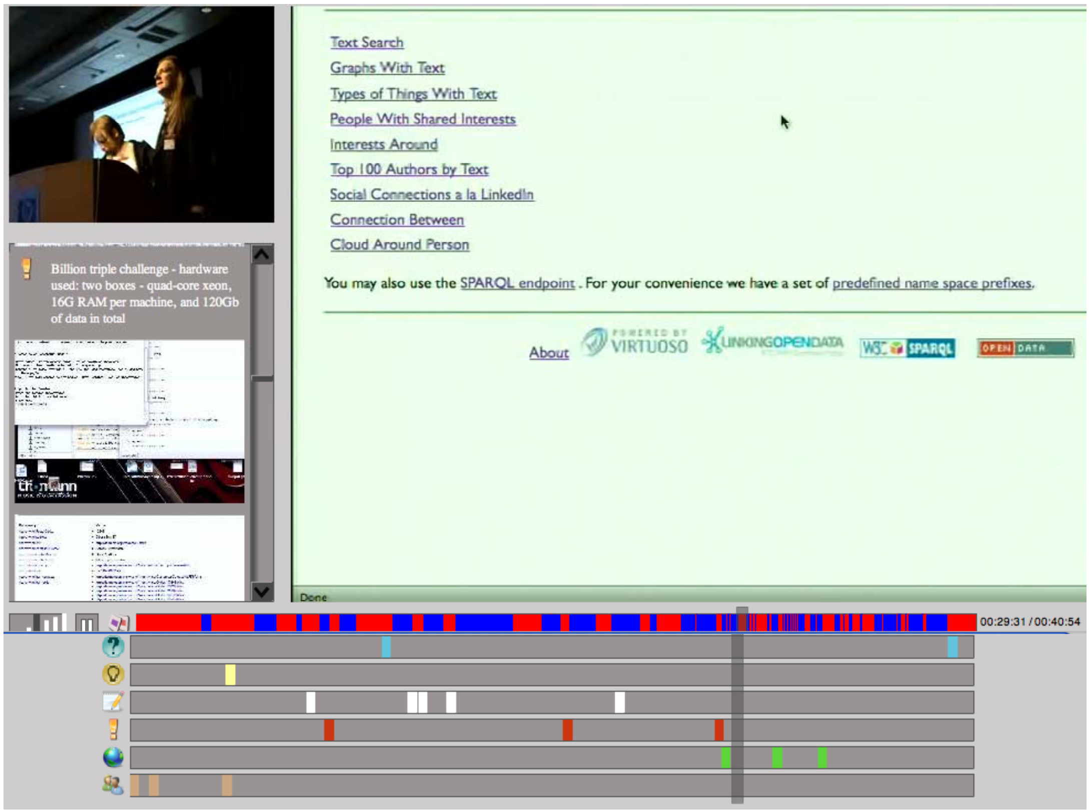
We hope the addition of these more informal annotations will increase the level of research-related content associated with events of interest to particular research communities and we will be seeking your feedback via an online survey to be announced after the Research Methods Festival

Diagram 2: Annotations Service

Recording Toolkit

The portable AG recording toolkit includes an editing application that allows an editor to edit out sections of recordings if required (among other functionality such as selecting camera views and so on). The toolkit includes screen capture for PowerPoint slides when used in speaker presentations – indeed with the CREW toolkit a hardware component is used to record wholly what takes place on a presenter's laptop from the audience perspective throughout a presentation and this could include a presenter's "tour" of datasets they have access to, computer code they are developing on a remote machine, demos and multimedia clips they wish to play to the audience and so on. The recordings are integrated with Live Event Annotations made by audience members, which are also automatically time-synced with the event video recordings. When a recording is complete, its video file is uploaded to the Video Archive Service and the session identifier for this plus some brief metadata is sent to the CREW Events Service. Annotations made are uploaded to the Annotations Service with associated metadata. **Diagram 3** illustrates this range of recorded and integrated information as it is made available to the end-user for replay (the markers on the timelines at the bottom of the screen shot indicate where live annotations were made – the annotations appear among the PowerPoint slides on the left hand side and also when the cursor is positioned over a marker):

Diagram 3: CREW AG Recording Toolkit



Text Search
Graphs With Text
Types of Things With Text
People With Shared Interests
Interests Around
Top 100 Authors by Text
Social Connections a la LinkedIn
Connection Between
Cloud Around Person

You may also use the SPARQL endpoint . For your convenience we have a set of predefined name space prefixes.

Billion triple challenge - hardware used: two boxes - quad-core xeon, 16G RAM per machine, and 120Gb of data in total

Administrative Interfaces

These are provided to the CREW Events Service to support editor control over annotations and recorded content – to allow retraction of comments if needed for example.

Section B - Legal and Ethical issues

Law and Ethics

In the academic literature dealing with law and ethics, legal issues are usually regarded as a sub-set of ethical issues. Thus, the combined rules found in data protection law and privacy and confidentiality law fall to be considered under general privacy issues[5] and intellectual property law, notably copyright, under ownership issues.[6] However, laws clearly differ from other ethical issues in that they are mandatory, their scope and application are derived from legislation; interpretations by regulatory bodies, e.g. the UK Information Commissioner; and ultimately by judicial decisions. Legal requirements form the baseline of ethical requirements; they set a standard below which the actions of individuals and organisations may not fall. However, in some areas of academic endeavour, it is arguable that existing legal requirements may fail to provide adequate protection in all circumstances and that an ethical academic should aspire to, or actively provide, more stringent safeguards. The vital component of both these elements – knowing where proposed research activities will cross from legality into illegality; and identifying where the mere observance of laws is insufficient to meet ethical standards – is an adequate understanding of the letter and spirit of those laws, and their applicability to particular forms of research.[7] This will be the case for the CREW project's capture and publishing of scholarly communication that occurs at events like conferences and workshops, and the RACE project's proposed digital repository service of collaborative research events.

Having undertaken a literature review as part of the process of developing this report, the authors have uncovered little material of direct relevance to the use of both videoconferencing and the AG in the fashion envisaged by the CREW project – there appears to have been no significant analysis of the legal and ethical issues that might be raised by the collection, annotation and preservation of scholarly communication in this fashion. This is perhaps not unsurprising, given the developmental nature of the technologies involved, even though videoconferencing as a technology has a long history, and IP (Internet Protocol) based videoconferencing has existed since the early 1990s.

There are, of course, other related fields of work from which lessons can be drawn. Oral historians and other researchers collect interviews, focus group discussions and other presentations using audio and audio-video media, and as a result have developed useful expertise and materials on the legal and ethical issues involved in capturing, archiving and using/disseminating the words of others.[8] Privacy and confidentiality, copyright issues, and defamation law appear repeatedly in those materials, as does the concern for ensuring that participants are capable of providing, and have given, informed consent to being recorded. More specialist literature, such as that produced by copyright lawyers, adds further weight to the argument that those using the CREW architecture and tools should be aware of the legal requirements that will need to be observed, if

[5] Eynon, R. Fry, J. & Schroeder, R. 'The Ethics of Internet Research'. in *The SAGE Handbook of Online Research Methods*. eds. Fielding, N. Lee, R. & Blank, G. (Sage Publications, pp. 23-41).

[6] Kastman, L.-A. M. & Gurak, L. J. (1999). Conducting Technical Communication Research via the Internet: Guidelines for Privacy, Permissions, and Ownership in Educational Research. *Technical Communication* 46(4): 460-469.

[7] Charlesworth, A. (2008) 'Understanding and Managing Legal Issues in Internet Research'. in *The SAGE Handbook of Online Research Methods*. eds. Fielding, N. Lee, R. & Blank, G. (Sage Publications, pp.42-57).

[8] See, for example, Linda Shopes, L. (2006) 'Legal and Ethical Issues in Oral History' in Charlton, T.L.; Myers, L.E & Sharpless, R. *Handbook of Oral History*, AltaMira Press at 135-169; Neuenschwander, J. H. *Oral History and the Law*, (3rd ed.) Oral History Association, 2002; Ward, A. (undated) Is your oral history legal and ethical? Oral History Society website, http://www.ohs.org.uk/ethics/index.php

recorded content is to be capable of reuse to its fullest extent.[9] The archivist community has also spent considerable time evaluating the potential impact of legal and ethical issues upon the collection, preservation and reuse of digital objects.[10] As well as reiterating the importance of the issues of privacy and confidentiality, copyright and defamation law, archivists have also identified further issues. These include international initiatives/pressure to promote access to archives,[11] and the impact of the Freedom of Information Act 2000 (FOIA 2000) upon the ability of archives that are, or are part of, 'public authorities', to control public access to material they hold.[12] Finally, the practices of current Internet and Web 2.0 commercial entities provide some guidance as to risk amelioration, particularly with regard to user-generated content.[13] From these surrounding literatures, it is possible to derive both a set of legal issues that are most likely to affect use of the CREW architecture and tools, as well as a set of strategies for addressing them.

Assessing the Environment

The CREW architecture is designed to capture and publish a range of elements relating to the scholarly communication that occurs at events like conferences and workshops. It is thus important to understand and work with the expectations and understandings of those participating in such events, and those interacting with the materials generated. Those expectations and understandings will be relevant both to the legal and ethical issues raised, the extent to which those are likely to pose problems/risks for use of the CREW architecture and tools, and the ways in which those problems/risks can be addressed.

In many circumstances, the primary objective of both those using a CREW-based system to capture and publish event materials, and those participating in the events and in later discussions, will be to ensure the widest possible dissemination of the subject matter of the event. In such circumstances, while the legal issues still need to be assessed and, where necessary, action taken to address them, the risks in areas such as privacy and data protection, copyright law and freedom of information are likely to be significantly reduced. This type of 'open access' consensus can be effectively reinforced by use of simple waiver/permission forms relating to these areas of law (e.g. copyright and related rights waivers, or use of permissive Creative Commons licences; simple DP agreements etc.)

However, it is important to remember that expectations across subject disciplines will not be homogenous. For example, in a relatively conservative discipline like Law, expectations about open access to event materials may be different to those found in the Science subjects, which are traditionally more willing to explore new means of dissemination and interaction. Legal print publishers may, for example, refuse to publish academic work that has already seen significant exposure in other media, or in digital preprint. Equally, digital publication and dissemination is still, in mainstream legal academia, regarded very much as second best to publication in established legal print journals, regardless of the potential value of widespread dissemination and increased interaction available through digital channels.

[9] E.g. Brennan D. & Christie, A. (2000). 'Spoken Words and Copyright Subsistence in Anglo-American Law'. *Intellectual Property Quarterly* (No.4):309-349; MacQueen, H. L. (2005). `My tongue is mine ain': Copyright, the Spoken Word and Privacy. *Modern Law Review* 68(3): 349-377.

[10] E.g. Behrnd-Klodt, M.L (2008). *Navigating Legal Issues in Archives*, Society of American Archivists; Charlesworth, A. (2003) *Legal issues relating to the archiving of internet resources in the UK, EU, USA and Australia*, JISC and The Wellcome Trust http://library.wellcome.ac.uk/assets/WTL039230.pdf and the JISC-funded Personal Archives Accessible in Digital Media (PARADIGM) project http://www.paradigm.ac.uk/index.html

[11] Council of Europe Draft Recommendation: A European Policy on access to archives (2000).

[12] Freedom of Information Act 2000: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1

[13] See, for example, Amazon's Conditions of Use & Sale - Section 6 "Your conduct" & Section 7 "Reviews, comments, communications and other content." http://www.amazon.co.uk/gp/help/customer/display.html?ie=UTF8&nodeId=1040616

Deployment of CREW-based systems in such circumstances is thus likely to meet with a degree of opposition, which may be expressed in terms of existing norms (e.g. "That's not how things are done in this discipline because…"), and/or by recourse to arguments claiming legal justifications for non-engagement (e.g. "You can't do that, it breaches data protection laws"). Stakeholders seeking to incorporate the CREW architecture into their processes can thus gain a double advantage from consideration of the legal and ethical issues inasmuch as such consideration will lead both to a greater understanding of the potential risks, and provide a means by which normative/legal objections can be avoided, or their effect ameliorated.

Other environments may also require greater strategic and operational understanding of the legal issues in play. For example, while scientific disciplines may be more open to exploring new means of dissemination and interaction, the outputs of scientific research may on occasion be highly sensitive. Research outputs that may have intellectual property implications (e.g. research that may lead to patent applications); research which is ethically sensitive (e.g. research involving human/animal subjects, research into genetically modified crops); or politically sensitive (e.g. research with military application, research into encryption/decryption technologies), may all carry greater legal risks for stakeholders seeking to use CREW-based systems.

Each deployment of a CREW-based system to capture and publish event-oriented scholarly communication will thus require some thought about the legal issues relevant to the particular environment in which that communication takes place. That analysis, and any actions following from it, will, in many, or even most, circumstances be relatively simple, and the development of generic event checklists and documentation will be of value in reducing the time and cost overhead of undertaking it.

Key Legal/Ethical Issues

This section lays out, in very brief form, information about the areas of law which will be relevant to use of the CREW architecture and tools, in order to provide a background for discussing risk assessment and risk amelioration. It also notes where ethical considerations may impact upon responses to legal requirements. Finally, it provides some examples to demonstrate how the CREW system and the various legal provisions/ ethical considerations might interface. This is not a comprehensive treatment, and those wishing to implement a CREW-based service are advised to seek further advice on the legal issues from their institution, as appropriate.

The law referred to is UK law, unless otherwise indicated, although reader should note that there are often differences between the law of England and Wales, and that of Scotland (e.g. in the areas of defamation law and freedom of information).

Data Protection

The *Data Protection Act 1998* (DPA 1998)[14] provides individuals with certain rights regarding information held about them. It places obligations on those who are responsible for processing personal data (***data controllers***) and gives rights to those who are the subject of that data (***data subjects***). Processing of personal data for research purposes falls under the general provisions of the Act, but some specific research-related exemptions are provided.

Definitions

The DPA 1998 addresses the lawful processing of ***personal data***. It defines personal data as any information relating to an identified/identifiable living person, or which in combination with other information held by or available to the data controller, would permit their identification. Fully anonymised data is outside the Act,

[14] Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

but pseudonymised or coded data is covered, as a pseudonym or code can be linked back to an identifiable individual. Additionally, for the Act to apply, the personal data must be, or intended to be, processed by computer or other equipment, or included in certain types of structured manual records.

Some types of personal data are given greater protection. These are labelled as ***sensitive personal data***. Personal data relating to racial or ethnic origin, political opinions, religious beliefs, membership of trade union organisations, physical or mental health, sexual life, offences or alleged offences fall under this heading.

Data ***processing*** is defined in the Act as 'obtaining, recording or holding the data or carrying out any operation or set of operations on the data.' This includes collection, recording, organization, storage, adaptation/alteration, retrieval, consultation, use, disclosure by transmission/dissemination, alignment/combination, blocking, erasure or destruction. The breadth of the definition essentially means that from its collection, to its destruction or full anonymisation, personal data is being 'processed' and thus the Act applies.

Obligations of a Data Controller

The DPA 1998 places a set of obligations upon data controllers: failure to observe these obligations will breach the Act and can result in legal sanctions, including fines and prohibitions on processing. While large fines are rare, such breaches may bring significant bad publicity. From the point of view of those working in academic institutions, publicised breaches may result in other negative consequences e.g. disciplinary action by employers, future difficulty in obtaining research and development funding, and unwillingness of potential data subjects to engage with institutional projects.

For all personal data, at least one of the following conditions must be met for personal information to be 'fairly processed':

- the individual has consented to the processing

or that the processing is:

- necessary for the performance of a contract with the individual
- required under a legal obligation (non-contractual)
- necessary to protect the individual's vital interests
- necessary to carry out public functions, e.g. administration of justice
- necessary in order to pursue the data controller's or a third party's legitimate interests and not unfair to the individual

Under UK data protection law, consent is thus not an absolute requirement for processing; a data controller may process non-sensitive personal data under another condition. However, data controllers must still provide information to data subjects about the purpose of the processing, and possible third party recipients of the personal data.

The processing of sensitive personal data is subject to more stringent conditions. The conditions for processing sensitive data are that one of the above conditions has been met **AND** the data subject has given her explicit consent to the processing, **OR** that the processing is necessary for a further set of specified reasons, including that it is:

- required by law for employment purposes
- needed to protect the individual's, or another person's, vital interests
- needed in connection with the administration of justice or legal proceedings

The meanings of "consent" and "explicit consent" are not defined, although the latter is often perceived as meaning "in writing" (it need not be). If no consent is forthcoming and the purpose of particular processing is not otherwise on the list of permissible reasons, it will be illegal.

The Data Protection Principles

All personal data processing, unless exempted, must conform to 8 Data Protection Principles. These require that data must be:

1. fairly and lawfully processed
2. processed for limited purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with the individual's rights
7. kept securely
8. not transferred to countries outside European Economic Area unless the country in question has adequate protection for individual privacy.

There are specific exemptions from some of the Principles for personal data processed for research purposes.

Rights of Data Subjects

The Act gives rights to individuals over their personal data held by data controllers. Failure to respect these rights may result in civil or criminal actions. Most data subject rights are linked to, and/or depend for their usefulness upon, the availability of an effective right of subject access. Subject access means that a data subject is entitled to be told by a data controller whether personal data about them is being processed by, or on behalf of, that data controller, and to be given access to a copy of that data. The rights include the ability to:

- make subject access requests
- prevent processing likely to cause damage or distress
- prevent processing for direct marketing purposes
- take action for compensation if they suffer damage caused by breach of the Act
- take action to rectify, block, erase or destroy inaccurate data,
- request the Information Commissioner to assess whether the Act has been breached

As with the Data Protection Principles, there are specific exemptions from data subjects' rights for personal data processed for research purposes.

Research Exemptions in UK Data Protection Law

The DPA 1998 provides exemptions for 'research purposes' including statistical or historical purposes. Where processing for research purposes is not used to support measures or decisions targeted at particular individuals, and will not cause substantial distress or damage to a data subject, it is exempt from:

- The Second Principle - *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 purposes* - personal data can be processed for research purposes other than for which they were originally obtained
- The Fifth Principle - *personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes* – personal data processed for research purposes can effectively be held indefinitely

Additionally, where:

- personal data is not processed to support measures or decisions with respect to particular individuals;
- personal data is not processed in a way that substantial damage or distress is likely to be caused to any individual;
- the research results, or any resulting statistics, are effectively anonymised;

there is an exemption from the data subject's right of access. The data controller may still choose to disclose the information to the data subject, unless by doing so they would breach another individual's data protection rights.

In addition to the legitimate purposes for processing of sensitive personal data contained in the DPA 1998 (e.g. explicit consent, medical research by a health professional), the *Data Protection (Processing of Sensitive Personal Data) Order 2000*[15] expressly permits processing for research purposes 'in the substantial public interest' where the data are not used to support measures or decisions targeted at particular individuals without their explicit consent; and no substantial damage or distress is caused, or is likely to be caused, to any person by the keeping of those data.

While some exemptions are granted for use of personal data for research purposes; there is no blanket exemption from the Data Protection Principles. Thus:

- Research data subjects should be informed of any new data processing purposes, the identity of the data controller, and any disclosures that may be made.
- Research data subjects must be able to meaningfully exercise their right to object to the data processing because it would cause/has caused, them significant damage or distress.
- Requirements for appropriate security of data must be respected, including appropriate levels of security for sensitive data
- Data may not be transferred to researchers in a non-EEA country, unless that country provides adequate data privacy protections, the data subject's explicit consent has been obtained, or there is an appropriate data protection contract with the data recipient.

The legislation recognises that the value of access to personal data in research may outweigh a data subject's desire to exercise a high level of control over the use of their data. As a result, even researchers wishing to use sensitive personal data should be able to do so, if they can demonstrate a significant public interest, and they adhere to the procedural safeguards required by law.

Ethical considerations

It is increasingly the case that research institutions,[16] professional organisations[17] and funding bodies[18] have specific ethical procedures for research involving human subjects. This includes any research which involves interviews and/or questionnaires, as well as other methods of collecting data that relate to identifiable individuals. Usually such procedures require that those collecting data about individuals obtain informed

[15] The Data Protection (Processing of Sensitive Personal Data) Order 2000 http://www.opsi.gov.uk/si/si2000/20000417.htm

[16] E.g. University of Bristol, University Research Ethics - Policy and Procedure http://www.bristol.ac.uk/research/support/governance/ethics/ethics.html

[17] E.g. Socio-Legal Studies Association - First Re-statement of Research Ethics. http://www.kent.ac.uk/nslsa/images/slsadownloads/ethicalstatement/ethics_drft2.pdf

[18] E.g. ESRC, Research Ethics Framework http://www.esrc.ac.uk/ESRCInfoCentre/Images/ESRC_Re_Ethics_Frame_tcm6-11291.pdf

consent to such collection. This may mean that internal institutional procedures require the use of stricter controls on the use of personal data than are required under the DPA 1998, including for events where the CREW system is used to capture personal data.

Additionally, some individuals may wish to contribute anonymously to discussions or via annotation. This may not be technically possible using a CREW-based system, or desirable in the light of other considerations.

Relevance to the use of the CREW System

Example 1 - An Event Organiser (EO) organises an academic conference at which a number of speakers are to give papers. The EO wishes to collect a variety of event-related content, for example, detail about presenters and delegates, the recorded presentations, the papers and informal comments made by attendees (in the form of annotations) and make these available to other researchers. The EO plans to use the CREW System to do so.

In this example, the EO will be collecting personal data from and about a range of individuals, including the speakers, whose personal details will be captured as part of the programme, and whose talks will be recorded. The CREW system also captures information about individuals attending the conference who make annotations, and potentially can capture information about individuals who add annotations at a later date.
All these individuals should be provided with details about:

- the purpose of the personal data collection;
- what personal data the system will hold, and how long it is to be held;
- to whom the personal data within the system will be accessible.

While their consent to the processing of their personal data is not necessarily required by the DPA 1998 – it could be justified by virtue of the fact that it is necessary in order to pursue the data controller's or a third party's legitimate interests (i.e. the EO's interest in creating a publically accessible virtual record of the event) and is not unfair to the individual - both the 'belt and braces' approach adopted by some organisations towards their DP obligations, and, potentially, institutional ethical requirements, may mean that the EO will wish to obtain consent from speakers, delegates and other users.

Personal data processed in the CREW system will have to be held in accordance with the 8 Data Protection Principles.

Copyright and Related Rights

Copyright is a property right vested in the owner of a protected work, and is essentially a bundle of economic and moral rights. In the UK the basic legal framework is contained in the *Copyright, Designs and Patents Act 1988* (CDPA 1988), as amended by later primary and secondary legislation.[19]

Copyright provisions

Copyright comes into being when a work is created, and no formal registration process is required, or available, in the UK. For a work to attract copyright protection the CDPA 1998 requires that it must be 'original'. It need not be especially imaginative, but its creation must involve some effort and it cannot be just a copy of another work.

Copyright only exists for a limited period - the term of copyright – and all works eventually emerge from copyright protection. Under UK law, different types of work have different terms of copyright protection. Also, despite the harmonising role played by international agreements, different countries apply different terms of copyright protection to works. Thus, the basic term of copyright in the EU is author's life + 70 years, but in the UK the term of copyright for sound recordings is 50 years from the end of year in which they are made or published.

Copyright covers many types of creative effort. It protects specific classes of works, but not ideas. The following works will be important in on-line research:

- *Literary Works*: Popular understanding of literary works includes fiction and non-fiction books, journals and newspapers/magazines, but the category is much wider. The basic criteria are that the literary work is original and 'fixed' in some medium. This means that letters, e-mail messages, and webpages can all be the subject of copyright. A work's 'literary merit' is unimportant. The CDPA 1988 brought the spoken word within the scope of 'literary works', but requires spoken or sung words be 'recorded, in writing or otherwise ...' before a copyright can exist.[20]
- *Artistic Works*: Includes graphic works, photographs, sculptures, collages, maps, charts and plans. These are protected regardless of artistic merit.
- *Sound Recordings*: Includes every type of sound recording on any type of medium from which sounds can be reproduced.
- *Films*: this includes any medium from which a moving image may be reproduced.
- *Broadcasts*: this includes any transmission capable of lawfully being received by members of the public.

Several copyrights may subsist simultaneously in a single item, such as a book or a webpage..

Ownership of copyright

Ownership of copyright in a work can change hands after its initial creation, and like any property, can be bought, sold or inherited. It is important to remember that copyright in a work is separate from physical ownership of the work. Ownership of copyright in a work belongs, initially, to the person who created it. This is subject to exceptions, which differ between countries, e.g. under UK law, copyright in works created in the course of employment does not vest in the employee, but in their employer, and thus the employer is the first owner. This exception does not apply to contractors.

[19] UK Copyright, Designs and Patents Act 1988: http://www.ipo.gov.uk/cdpact1988.pdf

[20] Phillips, J. (1989). Copyright in Spoken Words - Some Potential Problems. *European Intellectual Property Review* (No.7) 231-234.

Copyright in the spoken word is slightly more complicated. For example, if a person is talking about a subject and the discussions is not recorded in any way, then there is no copyright in the spoken word – the talk has not been 'fixed'. However, if a third party records that talk on a tape recorder, at that moment the work is 'fixed' and a copyright crystallises. In such circumstances, it appears that the speaker will have a copyright in their words, and the third party (technically, the 'producer' of the sound recording under the CDPA 1988) in the recording of those words. Thus, in order to use the recording, it will be necessary to secure permissions from both the speaker and the individual who 'produced' the recording. The same will be true of an audiovisual recording (technically, a 'film' under the CDPA 1988) of the talk, where both the speaker and the third party (technically, the producer and the principal director under the CDPA 1988) will own copyrights in the resulting recording.[21] If the speaker is reading from a written script or paper, there will be a copyright in the text, which is already 'fixed', and a joint copyright owned by the speaker and the individual who 'produced' the recording, in the recording.

A copyright owner has the right to prevent third parties from, without permission:

- copying the work;
- issuing copies of the work to the public;
- performing or broadcasting the work;
- adapting, or amending the work.

Copying is defined as reproducing the work in a material form, including storing the work in any medium. If someone carries out these 'restricted acts' on a work without the owner's permission, or authorises someone else to do so, they are infringing the copyright in the work.

Where a third party collects material in which another person holds a copyright (e.g. a recording of a presentation in which the interviewee holds a copyright in their spoken words), and wants to use that material in another work, such as an article, a book, or event proceedings etc, they have a number of options. The third party could obtain an outright transfer of the copyright from the copyright holder (***assignment*** - which must be in writing); they could obtain the copyright holder's permission do some of the things reserved to the copyright holder (***licence*** - which need not be in writing), or they could investigate whether any national copyright exemptions or defences would cover their proposed use.

Moral rights

The CDPA 1988 also introduced the concept of "moral rights" into UK legislation. These are distinct and separate from property rights and include:

- The right of the author of a work to be acknowledged as author or creator
- The right not to have their work subjected to 'derogatory' treatment
- The right of an individual to refuse to be associated with something they did not create.

Moral rights cannot be transferred, but can be waived. They do not apply to computer programs; works reporting current events; works that have appeared in newspapers, magazines, learned journals, or other collective works; actions required by law or by a Court, and to most employee created materials. An individual might, for example, wish to be identified as the author of their spoken words, as recorded by a third party.

[21] It is worth noting that the CDPA 1988 does not appear to have caught up with the concept of 'user created content' or that individuals other than professionals will make sound recordings or 'films' ('film' means a recording on any medium from which a moving image may by any means be produced) .

Relevance to the use of the CREW Architecture and Tools

Example 2 - An Event Organiser (EO) organises an academic conference at which a number of speakers are to give papers. The EO wishes to collect a variety of event-related content, for example, detail about presenters and delegates, the recorded presentations, the papers and informal comments made by attendees (in the form of annotations) and make these available to other researchers. The EO plans to use the CREW System to do so.

In this example, the EO wishes to collect and make available a range of works in which copyright subsists. The recorded presentations will probably be a joint copyright of the speaker, and the producer /principal director of the recording. This means that the EO will need to obtain either an assignment or licence of copyright from the speaker, and may, if the people who are making the recording are not employees of the EO, also need to obtain either an assignment or licence of copyright from them, in order to use the recording within the CREW system (i.e. allowing other users to view and make copies of the presentation).

Assignment of copyright would be the easiest way to effect this - i.e. transferring all rights to the EO - but while such assignments are common in contracts with producer/principal directors, they might not be acceptable to speakers, who may fear that this would restrict their ability to further disseminate their work. In such cases, a non-exclusive licence from the speaker permitting the EO to use the recording would be an alternative approach; however the EO is going to have to have a clear idea of what activities the licence will cover, as using the recording outside the terms of the licence will be a breach of copyright.

Use of other copyright works, including the papers from the conference and the annotations made by the attendees (and future users) will also require the EO to arrange terms on which they can be used. This could again be by assignment (in writing), or by licence. With regard to the annotations, for example, the EO might make access to the service, or the ability to enter annotations conditional upon the grant to the EO of a non-exclusive licence to reuse the annotations within the CREW Service. Lessons may be derived here from the licence conditions found in social networking sites.[22]

[22] E.g Yahoo! Terms of Service (on the Flickr site)

"With respect to all other Content you elect to post to other publicly accessible areas of the Service, you grant Yahoo! the royalty-free, perpetual, irrevocable, non-exclusive and fully sub-licensable right and licence to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, perform and display such Content (in whole or part) worldwide and/or to incorporate it in other works in any form, media, or technology now known or later developed." http://uk.docs.yahoo.com/info/terms.html

Defamation

Defamation law is the communication of a statement that makes a false claim, expressly stated or implied to be factual, that diminishes the public stating of a living natural or legal person.

In most jurisdictions, therefore defamation liability is based on three criteria:

- publication of untrue information about an identified individual, or clearly defined small class of people;
- dissemination of that information to other people than the author;
- damage to the reputation of the person referred to.

The key legislation in this area in the UK is the *Defamation Act 1996*, which was designed to simplify and modernise the law of defamation, in particular with regard to determining who could be sued in a given action.[23] However, national defamation laws vary widely, e.g. Scots law differs in important respects from English law. This is important when considering international Internet interactions, as individuals who believe they have been defamed may be able to choose a favourable jurisdiction in which to sue e.g. where the author of the statement is based, or where the statement was received by others. Thus, a individual defamed on a Usenet news group by a mailing sent by someone in Australia, which is available to users in the UK and US, could potentially choose any of those countries in which to sue.[24]

Under English law, a defamatory statement, or representation, in permanent form is a libel. Statements in books, articles, newspapers, letters, e-mails and webpages are libels, as are statements recorded on tape or other media. For a statement to be libellous, it must:

- be untrue and lower the opinion of the person defamed in the eyes of others – merely abusive statements are not libellous e.g. stating "Respondent B is a moron" is unlikely to be defamatory; falsely claiming that "Respondent B is a creator of child pornography" will be defamatory.
- refer to the person defamed in a way that they are clearly identified
- be made known to others or 'published' – e.g. the statement is disseminated to people other than its author and the person defamed.

Any living individual can sue for defamation; the dead cannot. A company can sue if the defamatory statement is in connection with its business or trading reputation.

Current interpretation of the law following the Defamation Act 1996 suggests that in respect of a CREW-based archive:

- the display of false information damaging to the reputation of the person referred to in that information, via a publically accessible system, will be considered by the courts to be 'published', and thus libellous;
- the author of a libellous statement captured in a CREW recording, or written in an annotation, that is accessible to third parties may be sued for damages, unless they did not intend their statement to be published at all;
- if the statement is published within a publically accessible system, such as a CREW-based archive, which is edited (or moderated), i.e. some other person than the author has control over the content of the statement, or the decision to publish it, that "editor" may be sued for damages;

[23] Defamation Act 1996: http://www.opsi.gov.uk/Acts/acts1996/ukpga_19960031_en_1

[24] See further, Collins, M. (2005). *The Law of Defamation and the Internet* (2nd ed.), Oxford University Press.

- if the statement is published within a publically accessible system, such as a CREW-based archive, by a "commercial publisher" (defined as a person whose business is issuing material to the public, or a section of the public,[25] i.e. there is no requirement of payment by the public) that "commercial publisher" may be sued for damages;
- if the person 'publishing' the statement within a publically accessible system is not an author, editor or publisher, as defined in the Act,[26] or because they are merely involved in "processing, making copies of, distributing or selling any electronic medium in or on which the statement is recorded, or in operating or providing any equipment, system or service by means of which the statement is retrieved, copied, distributed or made available in electronic form" or acting "as the operator of or provider of access to a communications system by means of which the statement is transmitted, or made available, by a person over whom he has no effective control"[27] they may not be sued for damages UNLESS
- they failed to take reasonable care in relation to its publication, or knew, or had reason to believe, that what they did caused or contributed to the publication of a defamatory statement,[28] in which case they too can be sued.

It is also worth noting that while s.4A of the Limitation Act 1980 provides that:

> *no action for libel or slander, slander of title, slander of goods or other malicious falsehood shall be brought after the expiration of one year from the date on which the cause of action accrued.*

as far as the courts are concerned, for the purposes of s.4A of the Limitation Act 1980, on-line archives are in effect being continuously republished each time they are accessed. As such, defamatory material made accessible via a CREW archive or repository could be the subject of legal action in England long after the original date of publication, as republication lays the publishers open to legal action every time that the defamatory statement appears.[29]

[25] s.1(2) Defamation Act 1996.

[26] s.1(1)(a) Defamation Act 1996.

[27] s.1(3) Defamation Act 1996.

[28] s.(1)(b) and s.1(1)(c) Defamation Act 1996.

[29] See *Loutchansky v Times Newspapers Ltd and Others (No 2)* [2002] 1 All ER 652.(CA)

Relevance to the use of the CREW Architecture and Tools

Example 3 - An Event Organiser (EO) organises an academic conference at which a number of speakers are to give papers, and records it using a CREW-based system. During their presentation, Speaker A makes a potentially defamatory comment about another person in their field, Academic X, suggesting that Academic X's recent work is plagiarised from other sources, and some of his research results have been falsified. A number of attendees add annotations to the recording which make further allegations about improprieties in Academic X and his research. Still further allegations of plagiarism are made, in public annotations to the recording, by users of the CREW-based system after the events, as the recording of the presentation and attendees' allegations are publically available. Academic X has been investigated by their University and other authorities and the allegations proven to be groundless.

In this example, it appears that Academic X has been defamed by Speaker A, i.e. a false claim has been made about him, which has been made known to others, and which is likely to cause damage to his reputation. If Speaker A's comment was made at the conference and not recorded, it would be slanderous. However, as the EO has recorded the presentation, it will be treated as libellous. The comments made by the attendees and users entered into the CREW system as annotations will also be libellous. As such, it is likely that Academic X has a cause of action against Speaker A, and the attendees and users who made the libellous annotations, as authors' of a libel.

The question then arises as to whether the EO would also face possible liability by virtue of:

- its role as creator/owner of the event output,
- its archiving of the libellous statements within the EO's CREW system implementation, and
- its making accessible the event output to other researchers/users.

The EO might reduce its potential liability for the recording, archiving and dissemination of the statement, if it refrained from actively editing/moderating the presentations/annotations, i.e. from reviewing each presentation and checking each annotation before making it available to others on the CREW-based system. However, such a 'hands-off' approach might not be considered reasonable, if there was a significant risk of libellous statements being made.

If the EO does engage in active editing/moderation it would probably be regarded as a 'publisher'[30] of the libel, being in a position to effectively exercise editorial control to prevent its release. Absent active editing/moderation, the key issue is the effective handling of archiving and dissemination of the libellous statements, once their presence is known. The EO will be liable for 'publishing' the libellous presentation and annotations if:

- it knew of their content; e.g. by listening to/reading them, or following a complaint from Academic X; and,
- it did not take reasonable steps to prevent further access to the libellous statements.[31]

The EO would need to consider its role regarding the collection of the information in question and its archiving within the CREW-based system. It might decide to actively review and edit all recordings/annotations prior to making them accessible to prevent potentially libellous statements from being archived and disseminated, or decide not to edit and claim no 'editorial' role. Much would depend upon the potential of the event for generating potentially libellous statements – i.e. would a reasonable person have expected that the event might generate contentious statements, or was there knowledge of previous public clashes/bad blood between Speaker A and Academic X.

Active moderation would protect speakers and annotators, but pose higher legal risk for the EO if it missed a

[30] 'Publication' in defamation law simply means 'making available to parties other than the author and subject of the libel'.

[31] See, for example, *Godfrey v. Demon Internet Ltd* [1999] 4 All ER 342 (QBD).

libellous statement. Exercising no moderation would expose speakers and annotators to higher personal risk; this could be reduced by advance provision of information about good practice when making a recorded presentation, or when adding annotations to the CREW-based system.

When archiving material, it is sensible to have in place an effective and quick procedure, for accepting notice from third parties complaining they have been defamed; and for removal of material from archival access until they are confirmed as defamatory or otherwise. This process could be part of a wider set of moderation and 'notice and take down' procedures within a CREW-based system for other types of contentious material, e.g. material infringing third party copyrights.

Freedom of Information

The *Freedom of Information Act 2000* (FOIA 2000)[32] gives a general right of public access to all types of recorded information held by 'public authorities', sets out exemptions from that general right, and places a number of obligations on public authorities.

Public authorities and access rights

'Public authorities' are broadly defined in the Act, and include not only Government Departments and local authorities, but a long list of other public bodies, including colleges and universities, as well as wholly owned 'spin-off' organisations.

Public authorities have two main responsibilities under the Act.

- They must produce a 'publication scheme', in essence, a guide to the information they hold which is already publicly available. This must be approved by the Information Commissioner.
- They must deal with individual requests for information. Individuals already have the right to access their personal data, held on computer, and in some paper files, under the DPA 1998. The FOIA 2000 permits individuals to access all other types of non-personal information that public authorities hold, subject to specific exemptions in the Act.

Information requests

Any individual can make a request to a public authority for information. The individual does not have to be the subject of that information, or be affected by its holding or use. For example, the FOIA 2000 is widely used by the media to obtain information for use in material for broadcast or publication.

The Act gives applicants two related rights:

- to be told whether the information is held by the institution
- to receive the information, where possible in the manner requested, e.g. as a copy or summary, or in paper or electronic format. An individual may also request to inspect records in person

Requests for information must be dealt with promptly, and the Act sets a maximum time frame for response of 20 working days. A fee may be charged for provision of requested information.

Where an applicant specifically requests information about a third party, or where responding to a request would involve the disclosure of personal information about a third party, the public authority must apply the Data Protection Principles when considering the disclosure of information. An authority must not disclose third party information, if to do so would mean breaching one of the Principles. Where the disclosure would not breach the principles, the authority may release the information.

Exemptions

The Act creates a general right of access to information held by public bodies, but also sets out 23 exemptions where that right is either disapplied or qualified. These relate to issues such as national security, law enforcement, commercial interests, and data protection. In particular, information is exempt from the Act if it is accessible to the applicant by other means.

There are two general categories of exemption: those where, even though an exemption exists, an institution has a duty to consider whether disclosure is required in the public interest and those where there is no duty

[32] Freedom of Information Act 2000: http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1

This Act applies to England & Wales; there is a separate, but broadly similar, Freedom of Information Act for Scotland.

to consider the public interest. The public interest test requires an institution to consider whether the public interest in withholding the exempt information outweighs the public interest in releasing it. This public interest test involves considering the circumstances of each particular case and the exemption that covers the information. The balance will lie in favour of disclosure, in that information may only be withheld if the public interest in withholding it is greater than the public interest in releasing it.

Exemptions where the public interest test applies are wide ranging,[33] but include:

- Information intended for future publication by the public authority, or third party;
- Health and safety;
- Personal information;[34]
- Commercial interests.

Where an institution considers that the public interest in withholding the information requested outweighs the public interest in releasing it, the institution must inform the applicant of its reasons, unless providing the reasoning would effectively mean releasing the exempt information.

'Absolute Exemptions'[35] include:

- Information accessible to applicant by other means;
- Personal information;[36]
- Information provided in confidence.

Only the information to which an exemption applies can be withheld, e.g. if a particular material is requested which contains some exempt information, only those specific pieces of exempt information can be withheld. The rest of the material has to be released. Where an institution decides an exemption applies and withholds information, it must give reasons for its decision and inform the applicant of his right to complain to the Information Commissioner. Where an exemption applies, but an institution is then required to release the information by the Information Commissioner, because it is in the public interest to do so, it must disclose the information requested 'within a reasonable time'.

[33] See s.22, s24, s27-31, s.33, s.35-40 FOIA 2000.

[34] if the institution believes that disclosure would not breach any of the data protection principles, but the individual who is the subject of the information has properly served notice under s.10 DPA 1998 that disclosure would cause unwarranted substantial damage or distress, or the individual who is the subject of the information would not have a right to know about it or a right of access to it under the DPA 1998, there is no absolute exemption and the institution should consider the public interest in deciding whether to release the information.

[35] See s.21, s.23, s.32, s.34, s.36, s.40-41, s.44 FOIA 2000.

[36] There is an absolute exemption from the provisions of the FOIA if an applicant making a request for information under the FOIA is the subject of the information requested and they already have the right of 'subject access' under the Data Protection Act 1998. There is also an exemption from the provisions of the FOIA if the information requested under the FOIA concerns a third party and disclosure by the institution would breach one of the Data Protection Principles

Relevance to the use of the CREW Architecture and Tools

Example 4 – A Virtual Organisation (VO) spanning several UK-based "real-world" academic institutions organises a conference at which a number of speakers are to give papers, and records it using a CREW-based system. The EO wishes to collect a variety of event-related content, for example, detail about presenters and delegates, the recorded presentations, the papers and informal annotations made by attendees, and make these available only to logged-in members of the academic institutions, who will be able to add further annotations. The conference covers a topic that is controversial and is receiving considerable media coverage. Shortly after the event, the VO (or one of its constituent institutions) receives an information request from a journalist who wishes to have access to the event materials, including all comments made by attendees and other users.

In this example, the first issue to address is whether the information request is being directed to a 'public authority'. It is likely that in such circumstances, the VO will not have an independent existence from the "real-world" academic institutions involved, and that as a result, the material in question would be deemed to be held individually or jointly by a public authority or authorities. Projects of this nature often have a 'lead institution' which would be responsible for operating and maintaining the CREW-based archive. If this is the case, then the institution, as a public authority, has an obligation to inform the journalist that they are holding the information, and to disclose the material requested, or to grant access to it.

The obligation to disclose may be overridden in circumstances where there is an exemption on which the institution(s) can rely. However, the number of exemptions potentially applicable to this situation may be limited, e.g. :

- where the recorded presentations are to be published in the future, there might be grounds for arguing that, subject to the application of the public interest test, that disclosure could be refused until after that publication.
- if the recorded event involved subject matter where either the disclosure of information contained within it, or identification of the speakers or other participants, might expose individuals at the institution(s) to harm, a health and safety exemption (e.g. for individuals working on animal experiments at a participating institution who might be targeted as a result), or data protection exemption, might be claimed. The former would be subject to the public interest test, the latter might be, depending upon which data protection exemption was at issue.
- if the recorded event involved subject matter falling within the commercial interests exemption, e.g. if the information requested contained material that was commercially sensitive, e.g. releasing it would damage the possibility of commercial exploitation of scientific data by the institutions
- if the recorded event involved subject matter subject to a duty of confidence, e.g. if the participants in the event were required to sign a Non-Disclosure Agreement (NDA) before participating in the event, or being allowed access to the CREW-based records. In such circumstances, the institutions would have to show that the use of the NDA or other confidentiality mechanisms were justified, given the nature of the material covered.

Those arranging the event would need to be aware of their institutions' obligations under the FOIA 2000, and to consider:

- the nature of the material they will be collecting;
- the information provided to participants in, and users of material derived from, the event; and
- the necessary documentation to be completed by those participants and users, in order to protect their interests and those of the institutions.

Section C - Risk Analysis and Risk Strategies

Why carry out a Risk Analysis?

Academic projects involved in the collection, archiving and reuse of digital materials, which experience serious legal difficulties, usually do so because of a failure to assess, at an early stage, the strategic and operational legal risks inherent in:

- the environment in which the project is taking place, and the nature of the materials;
- the methods used to collect and archive the materials;
- the ways in which the materials are to be used and reused.

This failure to develop a clear understanding of the legal risks leads, in turn, to such projects neglecting to:

- seek advice on issues/problems with which they have little or no prior experience
- document the types of issues/problems which analysis would have suggested required attention;
- identify and document consistent strategies or processes for avoiding or ameliorating those legal issues/problems;
- allocate sufficient time and resources to support those strategies or processes, as required;
- train staff to identify legal issues/problems as they arise; to adopt the appropriate process for handling them; and to allocate responsibility for ensuing that those processes are followed.

This means that when legal issues/problems do arise, that projects are all too often unable to deal with them in an effective, timely and financially viable manner. This may result in loss of functionality (e.g. the inability to use certain functions of the CREW architecture), loss of material (e.g. material has to be withdrawn from a CREW-based event resource due to failure to obtain appropriate copyright clearances), or project failure. Developing a clear understanding of the legal issues relating to the project, and implementing a strategy for managing them are thus key project management skills. An effectively managed project may still face legal risks, but will do so armed with adequate documentation, appropriate processes and an informed staff.

When should a Risk Analysis be undertaken?

EOs seeking to utilise CREW-based systems in capturing and publishing event-oriented scholarly communication should incorporate a legal risk assessment at an early stage in their initial methodology/planning. This will identify the legal risks involved in the use of particular technologies and tools, as well as in particular collection, archiving and dissemination practices. If carried out early enough, the risk assessment can be useful as a means of providing input into project choices in those areas. It may also examine, as appropriate, options for:

- effective compliance with particular legal obligations, e.g. how best to accommodate the rights of data subjects under data protection law, how data will be kept secure;
- aggregating important project-related information e.g. a 'copyright register' for copyright permissions relating to archiving and use of event material;
- effective administration of the use of CREW-based tools and practices, e.g. ensuring the legal risks are understood by both EO staff, event participants, and future users of the event resource; that legal liability for content is appropriately allocated and explained, and that there are adequate processes in place to limit all stakeholders' liability.

By performing a risk assessment early in the process, an EO will avoid problems being discovered at a later stage, when changes are likely to be more difficult, time consuming and costly. The process of articulation of a project's objectives, the organisation's requirements, and the justifications for particular design features required for risk assessment purposes will also have important benefits for general project management.

However, a legal risk assessment should not be treated simply as a start of project 'box ticking' exercise, as over time the legal issues may change. New risks may appear, particularly if there are changes in the technologies used, or in the EO's practices, processes and goals. Initial strategies for previously identified risks may also require evaluation as to their effectiveness in practice.

At the end of each event, the EO should consider documenting the legal issues encountered during the process, whether these were anticipated in the risk assessment, and how they were handled. A strategy of encouraging EOs to discuss good practice in the practical handling of legal risks observed in the used of CREW-based services will be an essential part of ingraining effective legal compliance processes into a rapidly developing field.

What should be analysed?

There are a range of potential issues that could be covered by a risk analysis. As already noted above, in any given case, the environment in which the EO is seeking to operate may have significant implications for the nature and extent of legal risk. As a starting point, EOs should identify:

- the other parties/stakeholders with an interest in the development of the event resource;
- what the other parties/stakeholders' needs, aims and objectives are likely to be (e.g. by consultation);
- reliable sources of relevant legal information (e.g. data protection officers, copyright clearance officers, JISC Legal, consultants, and lawyers);
- the legal issues relevant to the particular event to be captured, archived and disseminated;
- how those legal issues may impact upon elements of both operational and strategic planning;
- where legal (and ethical) compliance mechanisms may be needed (e.g. a 'copyright register'), and whether internal or external formalities need to be observed (e.g. data protection audit or ethics committee clearance);
- how the legal issues could be communicated to those affected by them (e.g. data protection notices, user terms and conditions);
- how and where information about the legal issues relevant to the development of the event resource could be most effectively recorded and archived;
- the estimated time and resource allocation required to develop and maintain the necessary documentation and processes to address the legal issues identified.

Risk Strategy

Once the risk assessment is completed, it will be possible for the EO to prioritise the legal risks and to determine and document how the key risks are to be addressed, who is to address them, and when this is to happen. Experience suggests that the temptation for staff of EOs will be to concentrate solely on the technical issues involved with utilising CREW-based systems, at the expense of matters that are often viewed as rather mundane and boring. It is thus helpful to have a clear roadmap and timescale for addressing the legal issues raised. It also means that it is harder for work required to address legal risks to simply 'fall off the agenda' in the event of time or resource constraints (a common problem with JISC projects). This information should be contained in the EO's risk strategy document.

Section D - Problem Areas and Technical/Non-Technical Solutions

Finding Solutions

It will be clear from Section B that the key legal problem areas facing EOs/CREW user groups are likely to be copyright, data protection, defamation and freedom of information. There are also a range of other legal issues which are much less likely to occur on a regular basis, but which may still surface in particular environments, or when dealing with particular topics, such as confidentiality, trade secrets and the use of NDAs in academic/commercial settings; or content liability for collection, archiving and dissemination of material that might be considered obscene, indecent, or to fall into the 'extreme pornography' category, which might appear in the context of discussion of art.[37] Where EOs/CREW user groups have conducted a risk analysis, they will be in a position to decide how to deal with such issues in an appropriate fashion in a given scenario.

Information

In all circumstances, a key element of problem avoidance will be effective communication of the aims and objectives of, and legal issues relevant to, the event that the EOs/CREW user group proposes to capture. These need to be communicated to those undertaking the event capture, those whose work/paper is being captured, participants in the event, and those using/adding to the resource that results. It will be important to consider how that information can be most appropriately communicated to relevant parties, both in terms of making the information accessible at appropriate times, and providing information in user-friendly form.

The concept of communication/information 'layering' envisages a set of explanations which cover the same issues, but which are targeted at particular sub-sets of audience, in terms of technicality of explanation, length of explanation and often both. It is a technique increasingly used in data protection circles for privacy policies, and also by the Creative Commons for its licence scheme.

In data protection terms, privacy policies are often aimed at lay readers, interested parties and experts. The lay readers are assumed to be simply interested in a very basic explanation of what the policy means for them. The interested parties are assumed to want to know more about the wider implications of the policy and how it affects them in detail. The experts are assumed to want chapter and verse on the precise nature of the policy and how it relates to the Data Protection Act 1998.[38]

The layered licences used by the Creative Commons take a slightly different approach. When you create a licence using the Creative Commons licence generator, the program produces three versions of the licence:

- *Commons Deed*. A plain-language summary of the licence, complete with the relevant icons.
- *Legal Code*. The fine print that you need to be sure the licence will stand up in court.
- *Digital Code*. A machine-readable translation of the licence that helps search engines and other applications identify your work by its terms of use.[39]

A layered approach, if both accurate and well designed, is thus an effective way of ensuring that an appropriate level of information is imparted to each participant in the process. In terms of the use of CREW-based systems:

[37] See, for example, the work of American artist and photographer, Robert Mapplethorpe, which has been the subject of several references to the UK police and CPS.

[38] See, for example, *The Center for Information Policy Leadership, Ten steps to develop a multilayered privacy notice* http://www.hunton.com/files/tbl_s47details%5Cfileupload265%5C1405%5Cten_steps_whitepaper.pdf

[39] Creative Commons, License Your Work http://creativecommons.org/about/license/

- those capturing an event will need a detailed overview of the aims and objectives of, and legal issues relevant to, that event, not least because they may be called upon to explain those issues to others. They may also need guidance as to when it is appropriate/acceptable/necessary to remove/redact event data from the CREW-based system to avoid legal liability.
- those presenting at an event will need information about:
    - what data (including personal data) will be collected by the system, to whom it may be made available, how it may be used and reused, and any implications for them arising from collection, use and reuse;
    - what permissions (including copyright assignments or licences) will be required from them for the data to be used for those purposes, and the implications of their granting those permissions, as well as any right they have to refuse or retract permissions;
    - appropriate content and commentary, particularly where the event recording is likely to be publically available, as the implications of this wide dissemination of conference outputs may not be immediately apparent to presenters.
- those interacting with a CREW-based system during (or after) an event, e.g. annotating presentations, will need information about:
    - what data will be collected about them, e.g. ID information, and how this may be used;
    - what permissions might be required of them in order for them to be able to interact with the system, e.g. interaction with the CREW-based system might be conditional on the EO/CREW user group being granted a non-exclusive licence to use/reuse/make publically available user-generated annotations;
    - appropriate content and commentary, including information about circumstances that might lead to material placed on the system being removed/redacted.

Communication of at least some generic layered information for CREW-recorded events could be incorporated within the CREW system, although it is likely that for presenters and attendees at events such information might have to be presented in advance and outside the CREW technology framework.

Ownership

When dealing with a potentially complex event capture system, such as a CREW-based system, it is important to be clear about ownership rights in the material generated from an event, and in the light of those rights, to understand what can be legitimately done with that material by the EO/CREW user group and by third parties. Where it is proposed to include material generated at an event in a larger repository, such as that envisaged by the RACE project, provision of clear and concise IPR information, presented in a uniform and simple fashion, becomes vitally important to the usability of the repository by third parties and, where applicable, to the development of consistency of practice between repositories seeking to permit the sharing and reuse of material.[40] For users, a clear understanding of the legal issues relating to their use of materials from a particular repository is often key to their willingness to utilise it, and to their effective and non-infringing use of items and metadata from it.

Dealing consistently and effectively with the IPR issues raised by use of a CREW-based system both at start-up and during operation, will require the clear allocation of responsibility for those determining and addressing those issues within the EO's management team/CREW user group. Where event materials are to be included

[40] See further, Charlesworth, A. *et al.* (2008) *Feasibility study into approaches to improve the consistency with which repositories share material* Project Report, JISC, 7 November 2008. http://ie-repository.jisc.ac.uk/256/1/jisc-clax-final-report-repocon.pdf

in a wider repository of such materials, it will be important that processes are in place to ensure that risk management is an ongoing issue, and that responsibility for undertaking such assessment, as well as developing and administrating methods of handling any risks identified, is clearly located within the staffing structure of the repository. Effective IPR risk management is key to establishing and maintaining both depositor and user trust in the reliability of a repository. In short, building a flexible copyright/IPR policy framework, based on an initial background and risk assessment, which contains clear and documented processes for deposit and access management, policy and process audit and risk amelioration, and which incorporates the ability to effect coherent change management in the light of shifts in environmental factors, will be essential for long-term repository sustainability.

At an event level it would, wherever possible, be an effective approach to seek a uniform set of IPR permissions from all contributors by use of standard licences or assignments, which are made known and agreed to by all parties before the event. A standard licence could be created specifically for each event, but in general in the academic environment, it would seem that adopting the Creative Commons' (CC) simple system of licences could be an effective way forward, inasmuch as it is a system with high existing recognition, and has a simple set of user-friendly icons to identify licence types.

Table 1: Creative Commons licences types and icons

CC BY	This license lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you for the original creation.
CC BY NC	This license lets others remix, tweak, and build upon your work non-commercially, and although their new works must also acknowledge you and be non-commercial, they don't have to license their derivative works on the same terms.
CC BY NC ND	This license is the most restrictive of our six main licenses, allowing redistribution. This license is often called the 'free advertising' license because it allows others to download your works and share them with others as long as they mention you and link back to you, but they can't change them in any way or use them commercially.
CC BY NC SA	This license lets others remix, tweak, and build upon your work non-commercially, as long as they credit you and license their new creations under the identical terms.
CC BY ND	This license allows for redistribution, commercial and non-commercial, as long as it is passed along unchanged and in whole, with credit to you.
CC BY SA	This license lets others remix, tweak, and build upon your work even for commercial reasons, if they credit you and license their new creations under identical terms.

Use of CC licences may also facilitate deposit of event materials with repositories, although CC licences are not a panacea for all deposit and access-related copyright issues arising in repositories.[41] Repositories, such as the RACE repository, will need to assess at an early stage if the CC system is an appropriate licensing

[41] Korn, N. & Oppenheim, C. (2006) 'Creative Commons Licences in Higher and Further Education: Do We Care?" *Ariadne*, no. 49. http://www.ariadne.ac.uk/issue49/korn-oppenheim/

mechanism for the type of events it seeks to preserve, and advise EOs/CREW user groups accordingly.[42]

Where a uniform system of copyright licensing is used, this can be combined with other metadata relating to particular events to produce a clear overview of the right holders involved in, and licensed rights applicable to, an event. In principle, such a metadata system could be machine readable, permitting, for example, automated searching by users for materials with particular usage rights, or categorisation of materials for the purposes of an FOIA request (e.g. confidential/non-confidential or prepublication/published).

Technical Solutions

The CREW system permits a significant degree of control over the material that is recorded and stored at an event (and afterwards). This will raise issues with regard to the responsibility of EOs/CREW user groups/repositories for ensuring that only appropriate material is collected, preserved and made available. In certain circumstances, e.g. defamatory statements or breaches of IPRs, recordings may need to be edited, slides removed and annotations rejected. Equally, it may be necessary (or desirable) for EOs/CREW user groups/repositories to be able to identify users of a CREW-based system to determine authorship of particular user-generated material, and/or control their use of the system, e.g. by restricting their ability to make annotations, or by removing annotations where these are inappropriate. Responsibility for taking such actions should be allocated within the EOs/CREW user groups/repositories, and rationales for intervention/deletion/rejection clearly defined to enable effective, efficient and consistent actions. EOs/CREW user groups/repositories will need to consider the extent to which their policy on editing will affect their potential editorial liability for content, e.g. it may be that a policy will state that such editing will only occur in circumstances where the organisation has been properly notified of the defamatory statements or IPR infringements.

Documentation and Records

From a legal perspective, documentary (and electronic) evidence is highly important when seeking to determine if, and to what extent, legal technicalities have been appropriately considered and dealt with. If such documentary evidence is effectively structured, the time and effort required to be dedicated to managing legal risk should be reduced. Examples of systems of documentary evidence include:

- policy and decision documentation – policies for identifying and handling legal issues should always be documented to provide continuity, particularly on projects where personnel may change quite quickly. Equally decisions with regard to handling legal risks, e.g. a decision to remove material from CREW archive, should be recorded with reasons for the decision. This recordkeeping enables consistency in decision-making and provides an audit trail for how policy has developed.
- an IPR register – a collated set of IPR assignments and licences relating to a particular collection of material, which could simply consist of a set of paper licence documents in a ring binder, or a electronic database of scans of such paper documents, or electronically generated and stored agreements within a computer system. An IPR register allows the licensee to identify efficiently the terms on which particular materials are licensed when dealing with third party queries or licensor claims. Information from such a register may be included in the metadata attached to files to allow for automated review of the IPR status of a work or materials.

The extent of documentation and recordkeeping will vary from project to project. However, as with IPR policy, it may be advantageous for repositories to specify the type of documentation and records they would prefer projects using a CREW-based system to provide on deposit of the material collected from an event.

[42] See further, Charlesworth, A. et al. (2008) *Development of Good Practice Guidelines for Repository Owners*, Project Report, BECTA. February 2008, pp. 51-71.

Conclusions and Recommendations

The technical output of the CREW project strongly suggests that there is scope to significantly improve access to, and enhance the value of, research event content by means of information capture from a variety of sources. However, as with other contemporary projects seeking to capture, preserve, aggregate and disseminate digital information, such as web archives, digital repositories for teaching and research materials, social networking services, and other user-generated content forums, users of the CREW system will be faced with a range of potential legal issues that will impact upon their activities. In order to use the CREW system effectively they will thus need to understand the legal issues and concomitant risks, undertake at least some degree of legal risk assessment and, where necessary, develop strategies for handling potential problem areas. Consideration of such issues will be a necessary step in the wider deployment and use of the CREW architecture by the stakeholder groups: events services, event organisers, and researchers.

How users of the CREW system handle legal issues will inevitably be important to projects like the RACE project, which is seeking to develop a digital repository service of collaborative research events derived from recording and annotating Access Grid (AG) events. It is in the long term interests of such repositories to encourage the development of coherent and consistent practices in handling legal issues across EOs/CREW user groups in order to facilitate the smooth deposit of event materials. If different EOs/CREW user groups adopt significantly divergent practices for handling legal issues, this may significantly increase the work of a repository in ensuring that:

- deposited event materials have been appropriately risk assessed;
- necessary information has been collected in the form of documentation or digital metadata to permit effective use/reuse;
- agreements reached with/licences obtained from third parties are adhered to.

It is therefore suggested that as part of the process of building upon the work of the CREW project, it will be necessary for projects such as RACE to consider developing good practice guidelines on handling legal issues for EOs/CREW user groups seeking to produce event materials with the aim/expectation of depositing them with a repository. Outlining a basic set of standards for handling legal issues when collecting event material via CREW-based systems, at an early stage of deployment of the technology, should:

- reduce uncertainty amongst EOs/CREW user groups about legal risks, encouraging uptake of the technology;
- cut the overhead in preparing for, and undertaking, legal risk assessment as EOs/CREW user groups are not required to 're-invent the wheel';
- enable EOs/CREW user groups/repositories to more easily share good practice in the practical handling of legal risks, thus ingraining effective legal compliance processes into a rapidly developing field.

In developing a set of standards for handling legal issues in the collection, aggregation, preservation and dissemination of event material, it will be possible to draw upon examples of good practice in other related fields. While the useful literature that relates specifically to legal issues in the use of both videoconferencing and the AG is currently very thin, much can be learnt from other fields, e.g. web archiving, which involve significant third party data capture. Significant work has also been carried out by JISC and others on good practice in the field of repository development and data deposit, notably in terms of developing effective accession strategies, providing guidance to would-be depositors, and in improving the sharing and reuse of material.

Bibliography

Books

Carey, P. (2004). *Data Protection: A Practical Guide to UK and EU Law*. (2nd ed.), Oxford University Press.

Collins, M. (2005). *The Law of Defamation and the Internet* (2nd ed.), Oxford University Press.

Neuenschwander, J. H. (2002). *Oral History and the Law*, (3rd ed.) Oral History Association **[US law]**

Articles & Reports

Brennan D. & Christie, A. (2000). 'Spoken Words and Copyright Subsistence in Anglo-American Law'. *Intellectual Property Quarterly* (No.4):309-349.

Behrnd-Klodt, M.L & Wosh, P.J. (eds.) (2005). *Privacy & Confidentiality Perspectives: Archivists & Archival Records*, Society of American Archivists. **[US law]**

Behrnd-Klodt, M.L (2008). *Navigating Legal Issues in Archives*, Society of American Archivists. **[US law]**

Charlesworth, A. (2003) Legal issues relating to the archiving of internet resources in the UK, EU, USA and Australia: A study undertaken for the JISC and The Wellcome Trust
http://library.wellcome.ac.uk/assets/WTL039230.pdf

Charlesworth, A. (2008). 'Understanding and Managing Legal Issues in Internet Research'. in *The SAGE Handbook of Online Research Methods*. eds. Fielding, N. Lee, R. & Blank, G. (Sage Publications, pp.42-57).

Charlesworth, A. Ferguson, N. Massart, D. Van Assche, F. Mason J. Radford, A. Smith, N. Tice, R. Collett, M. Schmoller, S. (2008) *Development of Good Practice Guidelines for Repository Owners*, Project Report, BECTA. 14 February 2008.

Charlesworth, A. Ferguson, N. Morgan, E.L. Schmoller, S. Smith, N. & Zeitlyn, D. (2008) *Feasibility study into approaches to improve the consistency with which repositories share material*. Project Report, JISC, 5 November 2008.
http://ie-repository.jisc.ac.uk/256/1/jisc-clax-final-report-repocon.pdf

Eynon, R. Fry, J. & Schroeder, R. (2008). 'The Ethics of Internet Research'. in *The SAGE Handbook of Online Research Methods*. eds. Fielding, N. Lee, R. & Blank, G. (Sage Publications, pp. 23-41).

Fielding, N. & M. Macintyre (2006). 'Access Grid Nodes in Field Research'. *Sociological Research Online* 11(2): http://www.socresonline.org.uk/11/2/fielding.html

MacQueen, H. L. (2005). `My tongue is mine ain': Copyright, the Spoken Word and Privacy. *Modern Law Review* 68(3): 349-377.

Linda Shopes, L. (2006). 'Legal and Ethical Issues in Oral History'. in Charlton, T.L.; Myers, L.E & Sharpless, R. *Handbook of Oral History*, AltaMira Press at 135-169. **[US law]**

Parry, O., Mauthner, N.S. (2004). 'Whose data are they anyway? Practical, legal, and ethical issues in archiving qualitative research data' *Sociology* 38(1): 139-52.

Phillips, J. (1989). Copyright in Spoken Words - Some Potential Problems. *European Intellectual Property Review* (No.7) 231-234.

Ward, A. (undated). Is your oral history legal and ethical? Oral History Society website
http://www.ohs.org.uk/ethics/index.php

Other Materials

NB: UK Acts listed in this section are cited to their originally published form, unless otherwise indicated. To view consequent amendments to UK Acts, please consult the UK Statute Law Database at: http://www.statutelaw.gov.uk/Home.aspx

Council of Europe, Draft Recommendation: A European Policy on access to archives
https://wcd.coe.int/ViewDoc.jsp?Ref=CM(2000)93&Sector=secCM&Language=lanEnglish&Ver

Copyright, Designs and Patents Act 1988 (unofficial consolidated version)
http://www.ipo.gov.uk/cdpact1988.pdf

Defamation Act 1996
http://www.opsi.gov.uk/Acts/acts1996/ukpga_19960031_en_1

Data Protection Act 1998
http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

Freedom of Information Act 2000 (England & Wales)
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000036_en_1

Websites

Collaborative Research Events on the Web (CREW)
http://www.crew-vre.net/

CREW Demonstrator
http://eric.rcs.manchester.ac.uk/Crew/

Intute
http://www.intute.ac.uk/

Intute: Social Sciences: Seminars and Events
http://www.intute.ac.uk/socialsciences/events.html

Repository of AG Collaborative Events (RACE)
http://www.rcs.manchester.ac.uk/research/race