Collaborative Applications: IP & Security Implications for Jointly Shared Information

Martin White, Managing Director, Intranet Focus Ltd

martin.white@intranetfocus.com

Working as a consultant I spend my life sharing documents with clients, and of course being sent documents as well. I have been using Basecamp in its original version for many years now as a repository for shared documents and my clients value the simplicity of the setup and the way in which the sections are presented. It may not look elegant but it works. Eventually the project comes to an end. I will archive the project documents but never delete them as clients have the pleasing habit of coming back after three or four years. Of course, once archived the client cannot access the project site but there is nothing in my standard terms of business about the level of access they have to documents.

The entire purpose of collaboration applications is to be a resting place for documents that are of joint value to everyone in the team, be they within the organisation or just retained for the project. However, I suspect that few organisations have really worked through the Intellectual Property Rights of collaboratively posted documents (and I'm using "document" in a generic sense) especially when the organisation is not hosting the collection of files itself.

This is not an academic consideration. I am very grateful to Dion Lindsay (Real Knowledge Management) for alerting me to a court case that has (at least in my view as a non-lawyer) significant implications for hosted jointly shared data. This blog post is based on an opinion from Gowling WLG on the case of Trant Engineering Ltd v Mott Macdonald Ltd before the Technology and Construction Court (TCC.) The full judgement should be published shortly.

According to the summary published by Gowling WLG, Trant Engineering (Trant) was engaged by the Ministry of Defence (MOD) as contractor for the Mid Atlantic Power Project, a £55 million initiative in respect of the construction of a power station in the Falkland Islands. Mott MacDonald was appointed to provide design services and was also the Building Information Modelling (BIM) coordinator, controlling access to the common data environment (CDE).

When a fee dispute arose, Mott MacDonald suspended its services and blocked Trant's access codes to the CDE leaving Trant unable to access the design materials. This case focuses on the situation with the use of BIM files by the construction industry. These are of such a size that some form of external hosting may be the optimum solution, that is until a contractual issue arises that might prejudice access!

According to the Gowlings WLG opinion: "The TCC concluded that it had a high degree of assurance that Trant was entitled to have access to the design data which had, in fact, already been placed in shared folders. It was particularly relevant that Trant had previously had access to the CDE before Mott MacDonald had suspended performance of its services. The TCC therefore ordered Mott MacDonald to restore access to the relevant design materials, subject to Trant making a payment into court."

Although this case looks to be specific to BIM in English law, precedent is of the greatest importance in a court case. This case could set a potential precedent for future litigation to shared information depending on the view of the judge if it is indeed a valid precedent. Any organisation in a similar position would do well to bring this to the attention of its legal team. The issues are similar to those with cloud services where the implications for the integrity, sharing and deletion of files may not always be in line with the assumptions of the business. The cloud deal may make sense on a cost-management basis but care needs to be taken that the legal implications are fully appreciated across the organisation.

By coincidence the issues of joint and several IPR on project files is the subject of a paper entitled "The dynamics of intellectual property rights for trust, knowledge sharing and innovation in project teams" by Professors Johan Olaisen and Oivind Revang. (They only seem to publish as a duo!) It was published in the International Journal of Information Management in December 2017. Professor Olaisen's research interests are very much in the area of shared information in project situations. The abstract to the paper states:

"How can intellectual property rights (IPRs) influence trust, attitudes, commitment, knowledge sharing, and innovation in inter-organisational project teams? The four strategically selected team cases include eight global knowledge-intensive industrial oil service companies in Norway. The methodology included 24 in-depth interviews done in 2016. The study finds that formal intellectual property rights are key to building up and keeping trust in the team and also for building up the right attitudes within the team. The IPRs increased the innovativeness in the team and incremental innovations. The IPRs fostered a unique knowledge sharing in these four teams enabling them to work towards innovative solutions and delivering on time. Formal IPRs foster informal trust and expertise sharing and by that also the inter- organisational cooperation. The confidence and knowledge sharing strengthen the possibility for future collaboration and innovations both on an individual level and on a corporate level. The theoretical implication of our findings is that IPRs increase the trust, commitment, and attitudes within the team providing knowledge sharing and innovativeness for improved solutions and results. IPRs are positive for collaboration, and they are complementary governance mechanisms. The practical implication is that IPRs must be defined and accepted before the corporations start up the interorganisational teamwork. The contract typology should in the start up be sensitizing giving directions and security and in the end definitive."

As a one line summary, the clearer the IPRs the more valuable the information becomes. This might seem counter to common sense but in general in organisations very little attention is paid to information rights. Another aspect of this is the policy towards what is referred to as protective marking. Every content item should have a marking that unambiguously defines who has access rights to the material.

I enjoyed reading The Black Door on a recent vacation. Written by Richard Aldrich and Rory Cormac it is the story of spies, secret intelligence and British Prime Ministers from 1908 to 2017. Many of the themes in the book mirror those in any organisation, such as defining who is an "expert" in a particular area, and how to bring together and assess sources of information and knowledge from a wide range of organisations, each with their own reasons for taking a particular line on a topic because of corporate interests. As I write this article it's the first anniversary of the publication of the Chilcott Inquiry into the involvement of the UK Government in the Iraq war and in particular the dossier on the existence (or non-existence as it turned out) of Weapons of Mass Destruction. This of course highlights the issue of information quality, as a substantial element of the dossier was plagiarised from publicly available material. Another theme of the book is the extent to which supposedly secret documents end up being made public, and not just by Edward Snowden.

Recent ransom-ware attacks have highlighted the need for IT teams to ensure that corporate systems are safe from any form of external threats and also to ensure that information held by the organisation is not transmitted digitally to unauthorised people outside of the organisation. There is also a need to ensure that internally employees cannot gain digital access to information that they do not have permission to see. An important feature of a search application is ensuring that employees cannot gain access to limited circulation information.

I have added the word "digitally" in the above paragraph for the reason that information can easily be circulated in a paper format once it has been downloaded. This is where protective marking becomes so important as it should ensure that every document or data item is visibility tagged in a way that there can be no dispute about the permitted readership of the document. Protective marking schemes should be set out in a corporate information security policy (ideally compliant with ISO 27001) but the question then is who decides on the circulation of a document. (NB I'm using "document" in a generic way). The critical issue is whether the labelling on the document defines unambiguously who has access to the information. Role-based labelling ("Heads of HR") is of no value. Someone may be the local manager for HR and so regard themselves as Head of HR in the office, but that is almost certainly not the readership that the author envisaged.

A good starting point for understanding the scope of a protective marking scheme is the UK Government policy document, especially as many public sector organisations in the UK base their own policies on the UK Government document. This document also sets out how 'paper' versions of documents should be managed from a protective marking perspective. The current policy dates from April 2014. In addition there is a very good overview document on government information security management published in 2016 by National Audit Office.

The point I want to make is that just seeing information security as a digital asset management topic owned by IT is to totally miss the point. The damage that printed, or printed-out, information can do in the wrong hands can not only be embarrassing but it's very difficult to pin down the route by which the information broke out of its cage, a cage often no stronger that an attachment to an email that says "Keep this to yourself." As

with so many aspects of the digital workplace policies have to be developed, implemented and reviewed as a combined effort of IT and the business. How quickly can you find the current version of your organisation's protective marking policy?

All that I have written above should be covered by the corporate information management policy but in my experience this is rarely the case. I have come across instances where different parts of the same organisation have different approaches to protective marking, and then of course life gets really interesting when organisations merge or split. There are usually clauses in merge and demerge agreements about what are often referred to as controlled documents, but about the last description you can give to a collaboration space is that it is controlled. Indeed, the argument is probably that the less controlled it is the better. Well, the two Professors would suggest that this is not the case and the Trant v Mott case suggests that your legal team need to be involved sooner rather than later. Consider this a warning!

See also: Building Information Modelling