



Strategies for IPR/DRM protection and secrecy Document collaboration or product systems ?

Summary

If your intention is to send information outside of your business because that is how you do business, or because this is what you are compelled to do, but you must take steps to protect the theft or misuse of that information you need a different solution to the 'collaboration' approach.

Collaboration Systems assume that you have control over the environment of all the recipients, usually because they are your staff. But outsiders are not your staff, they don't play by your rules and you can't enforce your rules on them using collaboration techniques.

The LockLizard Product System approach has been designed to manage information and content that is also going to outsiders. That does not mean that you cannot use it internally for protecting information and content, but unlike collaboration based products it also works outside of the organization, on multiple platforms and in multiple environments that you are not in control of.

Introduction

A lot is being written about Intellectual Property Rights (IPR) and Digital Rights Management (DRM) and how critical they are to the organization, but rather less is being written about what these topics mean, and which models and approaches are appropriate for which business scenarios.

Further, there is a general confusion about what IPR actually is, and how it might be protected, especially among the technology community.

So before you can sort out your DRM, you really need to understand what it is that you are trying to protect, and from whom, and why. Only then will it become clearer which tools are going to be the most appropriate for what you want to achieve.

In this white paper we describe differences between information, IPR and trade secrets, and where these might apply. We discuss what are the practicalities for DRM controls, and what these might realistically be. Finally we look at the different market models for current protection products and how they work, and then conclude on the suitability of approaches.

IPR or trade secret or what?

Anyone wishing to do a 'Google' search on the term IPR will stagger away with over 6 million entries to plunder. This is a technical term meaning that you can read the intellectual property of others and make some use of it. You will also find out that it's an acronym for a great deal more than just intellectual property.

But even if we strip out half the entries we still have an enormous list to chew over. And which of them are relevant?

Well, going to the other side of the question, what are you able to register Copyright (or obtain patent) in? Well, this might get easier – books, plays, films, music, broadcasts, semiconductor designs, databases, biological structures such as the human genome, chemicals and so on.



Now this at least gives us a clue as to what we could be talking about. Copyright concerns itself with some (fairly) specific things, and also, like patents, makes it plain when it does not provide protection. It does not protect the recipe for the exact herbs (and ratios of them) that are used in the manufacture of drinks such as Coca Cola or Benedictine. These are Trade Secrets.

It also does not cover 'know how' about how to do something, such as how to go about designing a semiconductor. That is something inside a person's head and it cannot be controlled. (Don't ask us, ask the lawyers. In the UK, at least, there is no copyright in the content of a legal contract, and in the European Union it has been held that there is no copyright in the content of a database unless work was done to gather, verify and add value to information captured and stored in a database. Mere collecting does not qualify.)

And of course that is only the start of the confusion.

If you have created something largely based on work done by someone who is not part of your business or who has not signed an agreement that says you own whatever intellectual property they provide (like using the content of this white paper, for instance) then you don't own any IPR and you could face legal action if you claim that you do. And if what you are protecting is Trade Secrets, and you fail to control who can see them (like leaving them on screen so that they can be read by someone walking past in a public location, say) then you likely have no rights at all. So if your business is pack full of consultants and outsiders your ideas about IPR (and, quite frankly, Trade Secrets) security may be closer to a pipe dream than reality!

So maybe the cynical business managers are actually correct, much of what you have is not intellectual property at all, but is a secret that you would rather keep. Some rather well defined areas are either IPR or patent, but in the main we are talking about trying to keep a secret – and that is much more of a challenge. After all, if it was Copyright then you would put a © symbol on it so that everyone was quite certain what it was. So a simple rule of thumb is that if you could not honestly put the copyright or © symbol on something then it MUST have been a Trade Secret if you thought it was worth protecting. (Curiously, information prior to patent could be argued to be copyright so that you get some protection, unless, of course, the patent fails under prior art.)

So we ought to conclude that internal information, unless we can see clearly it is a copyright work or material for a patent, is likely to be a Trade Secret, assuming that we want to try and protect it. Please bear this carefully in mind when reading the following sections of this white paper.

Digital Rights Management

DRM as a concept is rather like 'A man for all seasons.' Unlike magic, however, DRM controls are just additional access controls, and it is in that light that we look at them. A clever vendor's marketing department ought to be able to suggest to you that it is a combination of the silver bullet and the answer to a maiden's prayer. In other words, it does not matter what your information control problem is, then DRM can solve it.

Well, let us look carefully at what DRM can realistically offer.

First off the bat, so to speak, is the ability to see the information at all. This may be to read some text, see a film, hear some music (it is a form of seeing since it is exposing the work to one of the five senses, and thank goodness we don't yet have works that involve touch or taste). This is likely to be the most important of all, because once you have seen a work (whether copyright or secret) then you have it imprinted on your brain (assuming both that the work had any value and the recipient any brain).



Be aware that the law establishes that there are absolute rights of the recipient to use published information for private study, to produce a parody of it, and to quote a proportion of it (customarily 5%) as a reference in another work or for the purposes of criticism. It doesn't matter what you think your rights should be, the law (at least in the US and the EU) establishes that these rights exist, are proper, and are good.

The second thing that DRM may be able to do is limit the recipient's right of reproduction of the information. That may be to allow them to obtain a copy, say, by sending it to a printing device.

But, of course, this could be difficult to police. After all, once a printed copy is available then it is a fairly trivial affair to photocopy it, or even to have it scanned and then reproduced as, say, a pdf file. Or perhaps it is printed out several times using controls on the printer, or through the operating system of the computer, or perhaps it is actually sent to a file in a form that allows it to be printed again. There is the same problem that once it is on a computer screen it is possible to take a digital photograph and import the picture into the computer. This works fine with text but is not so good with graphics because of loss of quality.

Similar problems occur when you are dealing with music or sound, because it is possible to record the signal that is being sent to the loudspeakers, and in film/video because you can have a camera record either the visual image on the screen or collect the signals being sent to the playback device. Again there are usually losses of quality, but it is very difficult to prevent this kind of copying.

Perhaps easier is the ability of DRM controls to prevent someone from being able to readily copy the original file (whatever its contents) and distribute it to anyone they choose. Here DRM can work to create files that cannot be readily processed unless the person trying to process it has a provable authority.

A final possible use of DRM controls is to be able to provide the controller with information about the use of the information, such as who has used it, when they have used it, if there is reason to think they may be trying to circumvent the DRM controls, if they have tried to pass the work to others, and so on.

This latter group of 'audit' related DRM information could be a double-edged sword (a sword with no handle). And that is because it possibly moves into the realm of personal data collection, something regulated in the EU, Canada, and increasingly in the rest of the world. Whilst you can collect personal use information with employees and contractors by providing for that in the contract of employment, it is proving more difficult to do so with outsiders, and especially consumers, because they are protected by law.

Who is going to be the recipient?

This is the most complicated question that you have to answer. Is it to be a system that focuses on internal use of information, or is it for providing information to outsiders such as third parties, customers, consumers? The answer to this will indicate which of the following solutions is going to perform best for you in which circumstances.

Collaboration or Product solution ?

There are many approaches to providing controls over internal users of systems. For the simplicity's sake we shall refer to them generically as Collaboration Systems. That is because information that is internal to the enterprise is usually shared among staff who have the power to review, add, amend or approve information as it becomes prepared and finalized. Thus, they collaborate in order to create a finished result or product.



Collaboration Systems fit fairly readily into existing file access control mechanisms and also into internal IT department thinking and practices. They can be implemented in a variety of ways because the internal IT department are in a position to call all the shots. They can determine what applications run on the desktop. They can monitor and log access to vital information. They can impose document management systems, logon controls, and even PKI (assuming you have deep pockets) in order to support the internal management requirements that you decide to impose. They can integrate with all the internal technical infrastructure that is usually unique to the enterprise environment.

Product Systems are much better when the editing has stopped and you have a finished 'product' to distribute. This is a model that works well both outside and inside the enterprise. This is because it follows a different strategy from the Collaboration System. A Product System cannot predict what the recipient administration system is, the platform, how it is implemented and the potential rules. So it implements its own instead, regardless of the environment it is in. And it does not rely upon external 'trust' structures such as PKI because it cannot rely upon their availability or meaning.

As a result, Product Systems are more robust and more effective for use in distributed markets and when dealing with other enterprises, especially if the arrangements are unique or temporary.

Conclusions

There are currently no 'one size fits all' solutions to provide a seamless integration between Collaboration Systems and Product Systems.

Collaboration Systems are useful for internal purposes where the environment is known and can be easily controlled. They are most useful for managing 'active' documents that are constantly changing and being edited and shared by groups of people in a company. However they have the drawbacks of being expensive, require consultancy services to implement, and not readily usable (if at all) outside the organization. They are also expensive to support. If passwords are used for protection then they can be simply shared and are totally unmanageable. If a PKI system is in place, the third party has to be identified, have a public/private key pair already set up, and have given you their public key before they can start using your service.

Product Systems are useful for internal purposes where documents are 'finalized' (in published form and cannot be edited by others) and for external purposes where you have no control over the environment. They are much simpler to implement (LockLizard DRM products for example are supplied ready-to-go, enabling you to be up and running in less than 5 minutes), and costing from as little as \$2495 ensure you get a quick return on your ROI. LockLizard products have the advantage of PKI systems (the security and manageability) without the complexity, key management and support overheads to worry about.