

**Securing Intellectual
Property in Collaborative
Environments:
a guide**

**Dr Puay Tang &
Dr Jordi Molas-Gallart**




**SPRU
University
of Sussex**

**December
2004**



Contents

- 4** Trends in collision?
- 5** What is IP and why is it important?
- 6** Do Shared Data Environments pose new risks?
- 9** The challenge for firms
- 13** Safeguarding Intellectual Property in Shared Digital Environments
- 16** References



The authors wish to express their gratitude to the UK Economic and Social Research Council (ESRC) and the Ministry of Defence for their financial support for this project, the findings of which form the basis of this publication. The authors would also like to thank the ready cooperation of industry representatives, the UK Council for Electronic Business and the Defence Procurement Agency.

The project 'Managing IPR in Shared Digital Environments' was funded under the ESRC e-Society Programme, Project Number RES-335-25-0017.

At a glance

The growing complexity of products such as warships and telecoms networks has meant that firms are often unable to deliver such products on their own. This has led to an increasing level of collaboration between firms and also clients, all of whom need to be involved throughout the design and production stages.

Such projects involve huge amounts of information, ideas, technologies, techniques, and designs, and the need to share these between firms. Information and communication technologies offer fast and efficient means for sharing such material through a variety of 'shared digital environments' involving the web, intranets and e-mail groups.

While the use of such shared digital environments can be highly efficient, it can also bring risks caused by the potential for loss or leakage of intellectual property.

The research reported in this document was the first attempt to systematically investigate the implications for the protection of intellectual property (IP) that are brought about by the use of shared digital environments. The research found:

- Surveys have shown that many firms have suffered serious financial consequences from losses of IP from within the firm, and have started to manage IP more actively. However, collaborative projects pose even more difficult challenges than those of managing IP within individual firms.
- Managing Intellectual Property can be difficult as a result of its intangible nature. Senior management often focuses on more readily identifiable tangible assets and tends to pay relatively less attention to IP management.
- Where they do attempt to manage IP, firms often rely on formal practices such as patenting. However, this focus on formal protection does not amount to a comprehensive IP policy, since much of the firm's most valuable IP may never be suitable for protection through such mechanisms.
- It is the engineers, designers and IT managers who will often have most direct responsibility for protecting a firm's IP, since it is they who will be interacting most closely with groups outside the firm. Yet these groups are rarely consulted by IP professionals in the protection of IP.
- A good place to start for effective IP management policy is with an IP audit, which should aim to identify the firm's most essential IP, how it is or can be protected, and how it is being shared.
- For IP being shared through digital environments, there are various techniques for tagging and tracking IP in collaborative projects. Available technologies to reduce the risks of IP loss, leakage or misuse in shared digital environments are currently not widely exploited.
- In summary, most companies and public-sector organisations do not have thorough policies or cultures aimed at managing IP. Protecting IP should be a central part of corporate strategy, and IP management strategies should be directed from the top to ensure effective implementation and cross-departmental cooperation.

1

Trends in collision?

Demand for complex products means that firms are needing to collaborate more

The same tools that make it easier to collaborate may also jeopardise the protection of the firm's intellectual property

As products such as aircraft, ships and telecoms networks become more complex, firms need to collaborate more with each other and also with their clients to be able to deliver new more capable systems. Firms are rarely able to deliver such products on their own.

The need for collaboration centrally involves the sharing of information, ideas, and designs. Information and Communication Technologies (ICT) have become powerful tools to facilitate collaboration among firms, and between firms and their customers. They can enable increased productivity, allow for streamlined management of joint projects, and help research, design, manufacturing and maintenance teams, working at dispersed locations, to communicate and share information.

At the same time, knowledge assets are becoming increasingly important in determining firms' competitiveness. With firms investing large amounts on Research and Development and depending on innovation (new products and processes) for their survival, the knowledge-based assets – Intellectual Property – thus generated are increasingly valuable.

These two trends can collide. The same tools that make it easier to collaborate may also endanger the firm's control over the designs and technology that it has generated after much effort. In other words, collaboration may jeopardise the protection of intellectual property.

This document addresses the challenges to the management of knowledge assets that collaboration between organisations can generate, particularly when such collaboration is facilitated by the use of ICT via 'Shared Digital Environments' (see box below).

What are 'Shared Digital Environments'?

Shared Digital Environments (SDEs) involve the use of electronic networks, software platforms and data management systems to allow different organisations involved in a project to share technical data in real time. Existing technologies allow large amounts of technical data, including designs, product specifications, and manufacturing processes, to be shared in real time. SDEs can therefore facilitate collaboration in the design, development, manufacture and operation of complex products. Such environments quickly and easily allow geographically dispersed organisations to exchange technical data about the systems they are developing, often lowering the cost of inter-organisational collaboration.

However, the firms that are collaborating in one context may be competitors in other contexts, so their interests can be convergent in some respects but conflicting in others. Thus there is a need for firms to consider how they protect their intellectual assets while they participate in collaborative projects.

2

What is IP and why is it important?

Intellectual Property (IP) can be defined as any legally protected product of the intellect that does not exist in a tangible physical form and yet has commercial value. IP refers to commercially valuable *intangibles*; these include ideas or inventions that may have been expressed in written form but do not have a physical presence. Information is IP, if you think of it in terms of 'data that makes a difference' to corporate performance (Davenport and Prusak 1998).

IP can be expressed in many different forms: books, blueprints and technical manuals, for instance. Because it can be expressed, IP can be made available to other parties, although of course, some may be difficult to replicate. IP and its expressions are owned. Different types of Intellectual Property Rights (IPR) consist of, for instance, trademarks, copyrights, designs and patents.

How important is IP?

Today, management experts agree that Intellectual Property is a key asset influencing corporate performance. One informed estimate from the late 1990s reports that about three-quarters of the Fortune 100's total market capitalisation is represented by knowledge assets (Davenport and Prusak 1998). As the recognition of the commercial value of IP increases, its protection and management becomes an increasingly important challenge. Intellectual Property is not just important in new industries, such as software, biotechnology and microelectronics; it is also vital in more mature industries such as steel, petroleum and textiles.

Intellectual Property is not just important in new industries, but also in many mature sectors

The effective management of IP can yield significant benefits. For instance, protecting IP can help a company gain competitive advantage through a temporary technological lead, or it can raise entry barriers for market followers. Intellectual Property can provide sustainable business advantages, because unlike material assets, which decrease in value as they are used, IP assets often increase their value with use.

Protecting IP should not therefore be seen as a specialised function better left to IP specialists such as patent attorneys and copyright experts. Instead, it should be seen as an important element of corporate strategy.

3

Do Shared Data Environments pose new risks?

Business users often see ICT as bringing significant new threats to the protection of sensitive proprietary information

When different organisations collaborate in the development, manufacture, and support of complex products, the use of advanced Information and Communication Technologies (ICT) can greatly facilitate this process, through the creation of Shared Digital Environments (SDEs – see box page 4).

However, managing IP in SDEs poses problems that are different in nature and scope to those of managing IP within individual firms. The whole idea of SDEs is to make it easy to use, replicate and access information. Data is stored and accessed through a system over which the original owner of the information may have little control. This can increase the risk of data that conveys valuable IP leaking to competitors. However, as we shall see in chapter 5, ICT can also offer tools for tracking and managing the use of IP, providing a key tool for helping to protect it..

The risks of IP losses through ICT are not a new concern. Several surveys have stressed that business users see computers, computer networks and their associated technologies as having created significant new threats to sensitive proprietary information. A survey of 203 UK companies, conducted by the UK National High Tech Crime Unit in 2004, reported that 12 per cent of the firms had experienced instances of data theft through the Internet, causing losses amounting to approximately £7 billion (Lyons 2004). Another survey on information security reported that in a third of companies, internal users' lack of security awareness had led to theft of IP, loss of confidential data and third party access to a company's information system (Ernst & Young 2004).

The risks posed by the growing use of electronic data networks, and the rise of SDEs in collaborative projects, both suggest the need for IP management strategies that address data control and access.

The risks posed by the growing use of electronic data networks, and the rise of Shared Digital Environments in collaborative projects, both suggest the need for IP management strategies that address data control and access

Protecting IP within SDEs: key challenges

Three key challenges for protecting IP within SDEs emerged in this research:

1. The handling of 'background information';
2. The delivery and use of draft results, and;
3. Divergent legal and regulatory contexts.

1. Dealing with 'background information'

'Background information' refers to the wide range of pre-existing proprietary information that a company brings to a collaborative project, from technical data and components and subsystems, to manufacturing processes and design techniques. These will need to be integrated with technology brought by other firms or specifically developed for the project, so other firms may need to have access to such background information.

By sharing background information through SDEs, firms run the risk of inadvertently leaking commercially sensitive information. Such information not only includes technical data about specific components, but also designs, design techniques or other processes that are not usually protected through a patent, but rather through being kept secret.

Firms need to guard against losing IP when sharing background information

Particularly in the defence sector, laws and regulations may impose strict rules on the sharing of information

2. Access to draft results

Another potential problem relates to the early release of 'foreground information': information developed during the course of the project. This is a concern that applies particularly to the use that the client may make of information to which it can have access by virtue of its participation in the SDE. The client is likely to have rights of use over such foreground information whenever it has funded its development.

The concern from the point of view of the contractor who has generated the information relates to the possibility that, through an SDE, the customer may access data that is still being worked upon. This raises two potential problems:

- First, work-in-progress foreground information may include commercially-sensitive information on company techniques and processes that will not be present in the final data packs delivered to the customer.
- Second, there may be liability issues derived from the customer accessing and using data that is still in draft form but that may not be ready to be delivered to, and used by, the customer.

3. Divergent legal and regulatory contexts

In projects involving partners in different countries, systems for controlling access to data via an SDE may have to cope with different legal and regulatory requirements. In the defence sector, export control and technology transfer regulations will be particularly important: sharing of IP will invariably come under export control considerations. Collaborating companies have to ensure that access by other partners to data on an SDE does not violate national export control regimes. Furthermore, the IP regimes of collaborating partners may be different from each other, thus making the situation even more complex.

4

The challenge for firms

Most organisations do not have a strategic approach to protecting their IP

Before firms become involved in the use of Shared Digital Environments in collaborative projects, they need to be clear about their approach to protecting their Intellectual Property. Any approach to protecting the firm's IP within a collaborative environment is unlikely to succeed in the absence of a clear corporate IP management strategy.

Despite the widely acknowledged importance of IP, most organisations do not have a strategic approach to protecting their IP, and senior management often lacks commitment to this vital challenge. Firms still mostly deal with IP issues on a one-by-one basis, usually when problems occur. In practice, this is like trying to lock the stable door after the horse has bolted.

When companies do have corporate IP management policies, they are often rudimentary and focus on the supervision of specific, formal and highly visible ways of protecting IP, mainly through patents. But although much IP does not lend itself to protection through formal mechanisms, it can still be enormously valuable. Most organisations therefore need to broaden their approach to protecting IP.

This chapter outlines what firms need to do to achieve clarity in managing their IP: this could be regarded as a pre-condition for successfully protecting IP in collaborative projects involving SDEs.

Know what you know

Surprisingly, most businesses tend to treat all of their IP alike and do not differentiate between which of the IP is essential to their business (crown jewels) and which they can risk losing without causing too much harm. A useful way of establishing a 'baseline' is to conduct a company-wide IP audit.

What can firms do to achieve clarity in managing their IP?

An IP audit should seek to identify which part of the company's IP is valuable, why, and how it is being used, shared and protected. It should also note any cases where IP has been lost, or where the firm's IPR has been infringed. Only when an organisation has such knowledge about its IP can it start to formulate a thorough strategy for protecting it. It is plausible, for instance, that the firm might be spending too much protecting IP of little value. Conversely, leaving unprotected any IP that is central to the company's business can be hugely damaging.

Only when an organisation has a clear picture of its IP can it develop an effective strategy for protecting it

Protecting some IP formally does not amount to a comprehensive IP management policy

The need for an IP audit is not confined to companies: government organisations should consider adopting the same practice. Some government organisations may argue that there is less of a rationale for them to conduct an IP audit because they do not intend to commercialise their IP. Yet even when these organisations do not pursue commercial goals, there is still merit in having structured procedures for managing publicly funded IP. With the increasing trend towards collaboration between customers and their suppliers, there is a need for government customer organisations to keep track of the complex set of IPRs affecting the data they use and embodied in the systems they acquire or operate.

The importance of IP audits will grow when the UK Freedom of Information Act comes into effect in early 2005. There will then be an urgent need for government organisations to know what information is proprietary to firms and what may be released to the public under this Act. Intellectual Property management, including regular IP ownership audits, is thus becoming a requirement for public organisations.

Establishing corporate-wide IP management policies

Some companies, particularly large ones, are familiar with some of the processes available for protecting their IP, especially the more formal processes: large firms often employ patent attorneys, copyright specialists, etc. within an IP department. Yet a concentration on formally protecting IP does not amount to a comprehensive IP management policy. An IP management policy should establish company-wide procedures for identifying and using corporate IP, whether it is formally protected or not.

Need for cooperation across the firm

A significant insight to emerge from this research is that any corporate IP management policy needs to sit at the interface of IT strategy, commercial and contractual policies, and engineering and design practices. While it will usually be necessary for commercial and legal personnel to 'steer' the policy, it is the engineers and technical personnel who will mostly be responsible for implementation.

*IT, commercial
and IP functions
need to
be drawn
together.
A corporate-
level
commitment
is imperative.*

In practice, however, many firms treat the management of IP and its associated IPRs as a specialised function within a company. Lawyers and patent attorneys deal with patents and other forms of protection as needed. IT managers deal with corporate systems for data access control, and rarely consult with the legal or commercial departments on IP issues, such as the potential for data leakage inherent in the treatment and transfer of electronic data.

For their part, those involved in corporate strategy mainly concern themselves with managing tangible and financial assets, and IP management seems to be treated as a specialised task that does not readily find its way into the boardroom. But IP management policy needs to involve all of these communities, and therefore needs to be instigated from the top of the corporation.

Nurturing the right attitudes

Awareness of the importance of IP management has to permeate the whole organisation. Four key features are needed to nurture a culture of IP protection:

- leadership from the top;
- the continuing development of a coherent strategy;
- communication of the strategy and its procedures, and;
- company-wide accountability for protecting IP

Training in the use of the various technical applications and procedures for IP management is one way of communicating management's commitment to IP management. Anecdotes abound of engineers that are only too happy to share proprietary and commercially sensitive technical details with peers in other companies. Such behaviour may be attributed to 'cultural' traits within the engineering community that drive individuals to share their work with their partners across organisational divides.

*Nurturing a culture that protects IP
needs managerial leadership, coherence,
communication and accountability*

IP should be viewed across the organisation as an asset that needs to be protected actively

Although some of these anecdotes involve instances in which such exchanges were not facilitated by electronic networks (sometimes in conversations and data exchanges in paper form), concerns remain about what would happen when the digital systems for collaboration are in place that could allow a loquacious engineer to send reams of technical information across to project partners with the click of a button.

Training in, and induction to, the firm's procedures for protecting IP is likely to be most effective when accompanied by the development of an 'accountability culture' – making the protection of IP a responsibility for all concerned. Importantly, training has to be conducted systematically as part of a company-wide policy: training sessions conducted on a project-by-project basis cannot substitute for a comprehensive program.

Senior management needs to realise that IP should be viewed as an asset that needs to be protected by a thorough strategy. It needs to develop a firm familiarity with the IP issues raised by the growth in collaborative work, and make IP management a strategic management priority. These actions will be instrumental to effective and successful IP management throughout the organisation. The importance of top-level commitment to corporate-wide IP management policies cannot be emphasised enough. This is the bedrock of IP protection upon which any involvement in SDEs must sit: the main responsibilities for establishing effective ways of protecting IP in SDEs lie with senior management.

Top-level commitment within the firm to protecting IP is the bedrock upon which any involvement in SDEs must sit

5

Safeguarding Intellectual Property in Shared Digital Environments

Firms need to pursue deliberate policies in order to protect their Intellectual Property in collaborative projects

Firms need to pursue deliberate policies in order to protect their Intellectual Property when becoming involved in collaborative projects, especially when projects involve the use of Shared Digital Environments. This final chapter outlines the various things that firms can do in order to protect their IP in such situations.

Using available contractual tools

Contractual conditions may help in IP management by clarifying the rights of all partners to a contract, including those in charge of establishing the ICT infrastructure on which an SDE will rely. Contractual requirements can be quite specific, defining, for instance, procedures and rules regarding the management of the SDE, and the marking and segregation of the data the SDE contains.

In the UK, a wide choice of DEFCONs ('Defence Conditions') is available for defence contract officers to include in contracts. These provide detailed contractual clauses and provisions applicable to a wide set of situations, and are often accompanied by explanatory notes and other supporting material. For instance, in collaboration with industry, the UK Ministry of Defence has developed extensive guidelines and sets of contractual conditions on the management of IP in what it calls shared *data* environments. These tools and information are freely available in the Internet and can be applied and adapted to a variety of contractual situations in the defence industries and elsewhere.

Achieving clarity from the start

With appropriate investment, ICT networks not only facilitate collaboration within and across organisations, but also provide tools for improved IP management. They can achieve this through the capacities they can provide to audit and trace large amounts of technical documents. Existing tools are already quite robust, but several problems remain with their use.

Collaborating firms and clients need to agree on ways to protect IP from the start of a project

There are three main challenges to managing IP effectively in SDEs

The biggest challenges to collaborative IP management in an SDE are:

1. agreeing on the ICT tools that are to be used to monitor and track the information shared through the SDE;
2. agreeing on how to use these tools – establishing strict user procedures on data sharing, access to, and control of, the use of data, and;
3. managing the SDE system throughout the collaborative partnership – establishing procedures to ensure continual robustness of the system, its security and functionality, and adherence to user procedures.

These challenges are likely to be addressed differently across projects. There is no single software-based tool or implementation model that solves everyone's collaborative IP management problems. Existing experience on the use of ICT in defence projects shows that a variety of networks and systems have been used for different projects. It is normal for projects to be governed by varying contractual clauses, supported by specific ICT systems and implementing different IP rules and practices. This means that each project incurs high set-up costs (the wheel is being constantly reinvented), and creates confusion as the same IP may be treated differently across projects. There is scope for gaining consistency if the present project-by-project approach is substituted by corporate-wide policies. Two main models to manage data sharing in SDEs exist.

Managing data sharing in SDEs: two models

There are two main models that can be followed to set up an SDE. One approach is to segment the data in the central database into different folders. Each participating organisation will have access only to its own set of folders. This can slow down collaboration among suppliers, however. If a company needs data from another supplier, it will have to request it from the SDE manager, who after following an established set of procedures will 'post' the information in a folder accessible to both suppliers. These approaches are operationally cumbersome and could cause data replication across folders. The danger with data replication is data fracture; that is, the data in one folder could be changed or updated without the same data being changed in another folder, thereby ending in two versions of the same data.

Different models can be adopted to set up an SDE

Technical solutions are not a panacea: commitment needs to come from the top of the firm

The alternative is to administer the system by tagging each data element with information including its origin, commercial confidentiality markings, and security and other access restrictions, and then linking the access rights of individuals to the tags. This requires a parallel identity and access management system, in which all individuals must have proof of identity to log on to the system. Access will depend on the individual's organisation, role within the organisation and any other factors, like nationality, with a bearing on the definition of his or her access privileges. Such a 'data level' management system would allocate access rights automatically thus eliminating the need for a manual management of access privileges. The building blocks (technologies and procedures) to set up such a system exist.

Technical solutions are not a panacea. To implement effective IP management, both public and private organisations must be clear about what IP they seek to protect, how to protect it and the corresponding risks in the absence of effectual IP management. Indeed, we have already learnt that while there are systems to monitor and track the information shared through an SDE, strict procedures on data sharing must be established. Such procedures cannot be effectively established in the absence of commitment from senior management.

Organisations must be clear what IP to protect and how to protect it

References

Davenport, Thomas H, and Laurence Prusak. 1998. *Working Knowledge: How Organizations Manage What They Know*. Boston: Harvard Business School Press.

Ernst & Young. 2004. *Global Information Security Survey 2004*: Ernst & Young.

Lyons, John. 2004. *Internet Investigations - International Standards and Co-operation*. Paper read at UN/ECE Advisory Group for the Protection and Implementation of Intellectual Property Rights for Investment, 1-2 April, at Warsaw.



Securing Intellectual Property in Collaborative Environments
Puay Tang and Jordi Molas-Gallart

SPRU, University of Sussex
The Freeman Centre, Brighton BN1 9QE, UK
e-mail: p.tang@sussex.ac.uk
j.molas-gallart@sussex.ac.uk

Consultant Editor: Dr Alister Scott of TheKnowledgeBridge
alister@theknowledgebridge.com

Design by Jenny Hughes: design@theknowledgebridge.com



SPRU
University
of Sussex

December
2004