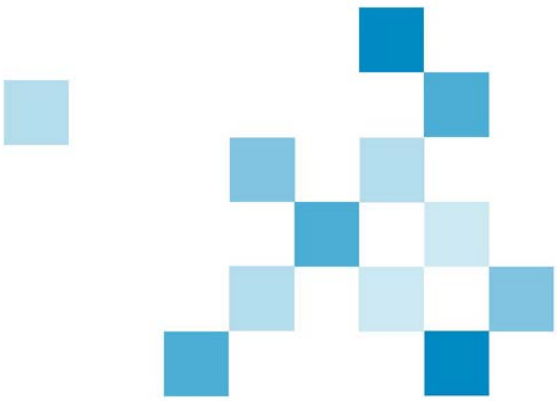
INGENIO WORKING PAPER SERIES

Ingenio
CSIC-UPV
INSTITUTO DE GESTIÓN DE LA INNOVACIÓN Y DEL CONOCIMIENTO

Collaborate but protect: the challenges of protecting your data

Autores: Puay Tang, Jordi Molas-Gallart, Robert Shields

Working Paper Nº 2008/6



INGENIO [CSIC-UPV] Universidad Politécnica de Valencia | Camino de Vera s/n | 46022 Valencia
tel. +34 963 877 048 | fax +34 963 877 991 | innco@ingenio.upv.es

Collaborate But Protect: The Challenges Of Protecting Your Data

Puay Tang[a], Jordi Molas-Gallart[b], Robert Shields[c]

[a] SPRU, Science and Technology Policy Research, University of Sussex
The Freeman Center
Brighton, BN1 9QE
East Sussex, United Kingdom

[b] INGENIO (CSIC-UPV)
Camino de Vera, s/n
Universitat Politècnica de València
46022 València
Spain

[c] Brigadier (Retired)
Director Xmoor Ltd
Moorlands, Hoe Road
Bishop's Waltham, SO32 1DU
United Kingdom

Acknowledgements

The research for this paper was partly funded by a joint grant of the UK Economic Social Research Council "E-Society Programme", and the UK Ministry of Defence under the Joint Grants Scheme (ESRC Award Reference RES-335-25-0017). It has also drawn upon the developing outputs of the Transatlantic Secure Collaboration Program, which is funded by major US and European Defence contractors.

Abstract

Data and its transfer is increasingly important to corporations as more companies use Information and Communication Technologies (ICT) based tools to conduct their businesses. This article addresses an insufficiently studied issue: data management in collaborative projects involving several firms and other organizations, including public sector ones. We focus on the use of advanced ICT tools to support collaboration in the design, development, manufacture and maintenance of complex product systems. In these instances, organizations need to exchange and share large amounts of proprietary technical data through data networks. How can collaborating organizations exploit the capabilities offered by ICT tools without increasing the vulnerability of their data to misappropriation or leakage? Do formal regulations and codes of practice provide a helpful tool to guide data management strategies? We find that the technologies, processes and contractual tools to enable data management and control exist but are not being deployed to the full extent of their capabilities, and discuss a range of strategies, approaches and tools that are starting to be developed in some industrial environments.

1 The Roots of the problem: More Collaboration requires more security of shared information

The importance of data and its management to the modern corporation is widely recognized. Data is central to the development, production and delivery of goods and services, and its management and use within corporations has been the object of detailed study.[1] As a form of Intellectual Property (IP) data is also valuable in itself.[2] It can, convey commercially sensitive information resulting, for instance, from substantial investments in research and technological development. In today's "knowledge economy" data is becoming more valuable and, consequently, protecting it is an increasingly important managerial challenge.

Yet, while protecting data is becoming more important, another trend is likely to make protection more difficult. To tackle growing technological complexity firms are increasing collaboration and the exchange of technical data and information. This creates a paradox: while interaction and co-operation between partners becomes necessary, this interaction exposes the firms´ to losing their distinctive knowledge assets and skills.[3] In this context the rise of Information and Communication Technologies (ICT) intensifies the paradox. On the one hand, they facilitate collaboration among firms and their clients. With their ability to capture, store, replicate and transmit data, they enable research and design work to be carried out simultaneously in different locations, and facilitate the outsourcing of technical tasks to the supply chain. These are factors that are encouraging firms to share data through electronic means. It has been shown, for instance, that the use of the internet to support business operations is changing the scope of firms, leading "internetworking associates" to narrow their organizational focus as they are able to outsource activities that were previously carried

[1] There is a wide literature, often of a technical character, about data management and analysis using IT tools (see, for instance, V. Dhar and R. Stein, *Seven Methods for Transforming Corporate Data Into Business Intelligence* (Upper Saddle River: Prentice Hall, 1997). More broadly, research on the managing of Intellectual Property to realize its full value has also focused on management *within* the corporation (see for instance M. Reitzig, "Strategic Management of Intellectual Property," *Sloan Management Review*, volume 45, 3 2004, pp. 35-39.)

[2] For the purposes of this paper, we will use IP and technical data interchangeably.

[3] J. Jordan and J. Lowe, "Protecting Strategic Knowledge: Insights from Collaborative Agreements in the Aerospace Sector," *Technology Analysis & Strategic Management*, volume 16, 2 2004, pp. 241-259.

out in house.[4] On the other hand, however, the same technologies that facilitate collaboration can make it easier for unauthorized third parties to get hold of it. [5]

The use of new ICT applications as tools to promote collaboration has been intensely analyzed; for instance, new web technologies can turn corporate intranets into active collaborative platforms.[6] Yet the focus of analysts has been firmly placed on the implementation of tools *within* the corporation. Similarly, the management of proprietary data and information has been analyzed at the level of the individual firm strategy,[7] but much less attention has been paid to the specific management problems that emerge when organizations need to share data in the context of collaborative projects. Jordan and Lowe´s[8] have analyzed knowledge sharing across firms involved in collaborative ventures in the aerospace sector. Aerospace firms need to enter alliances with other companies in the sector to be able to undertake the complex projects in which they are involved; to make the alliances successful they need to engage in high levels of interaction and cooperation with their alliance partners, and to exchange information and knowledge. On the other hand, this makes them vulnerable as their partners (who are also often their competitors) can obtain sensitive information of commercial value through such exchanges. Firms must exchange information while at the same time protecting themselves against knowledge appropriation.

The application of advanced ICT tools exacerbates the problem. ICTs can facilitate the sharing of technical information that is required to manage a process in which literally

---

[4] P. J. Brews and C. L. Tucci, "The Structural and Performance Effects of Internetworking," *Long Range Planing*, volume 40 2007, pp. 223-243.

[5] As the value of data to a company grows, the risks posed by illegal appropriation also increase. US surveys conducted in 2004 reported that 138 US companies suffered a loss of US$35-39 billion from incidents in which proprietary data was disclosed. More than two thirds of the surveyed firms saw computers, networks and the Internet as posing significant threats to commercially sensitive information. ASIS International, PricewaterhouseCoopers and American Chamber of Commerce, "Trends in Proprietary Information Loss. Survey Report," (Alexandria, VA: ASIS International, 2002). In the UK, a 2004 survey of 203 companies conducted by the UK National High Tech Crime Unit concluded that 12% of British firms had suffered data theft through the Internet, causing losses estimated in excess of £7 billion. J. Lyons, "Internet Investigations - International Standards and Co-operation," (Warsaw: UN/ECE Advisory Group for the Protection and Implementation of Intellectual Property Rights for Investment, 1-2 April 2004).

[6] A. P. McAfee, "Enterprise 2.0: The Dawn of Emergent Collaboration," *Sloan Management Review*, volume 47, 3 2006, pp. 21-28.

[7] M. Reitzig, "Strategic Management of Intellectual Property," Ibid., volume 45 2004, pp. 35-39, P. C. Grindley and D. J. Teece, "Managing Intellectual Capital: Licensing and Cross-licensing semiconductors and electronics," *California Management Review*, volume 39, 2 1997, pp. 8-41, P. Tang, "How electronic publishers are protecting against piracy: Doubts about technical systems of protection," *The Information Society*, volume 14, 1 1998, pp. 19-31.

[8] J. Jordan and J. Lowe, "Protecting Strategic Knowledge: Insights from Collaborative Agreements in the Aerospace Sector," *Technology Analysis & Strategic Management*, volume 16, 2 2004, pp. 241-259.

thousands of engineers and designers, from many firms and organizations are working together from dispersed locations. The ease with which the information can flow across corporate boundaries could make it, in principle, also easier for competitors to access commercially sensitive technical information. The main problem is *how can organizations securely guard their technical data while sharing it with their collaborative partners through means that allow the easy transfer and use of information.* This poses challenges that are different in nature and scope to those of IP management within the firm. For instance, within the firm, organizations can develop perimeter IP protection mechanisms, based on tightly controlled IT systems. Yet, as companies face opening up their data to partners and suppliers, the demarcation between internal and external IT networks becomes less clear. Securing and controlling access to data at the boundary from a plethora of users becomes correspondingly more difficult.

This article analyzes the solutions being developed to address these problems in the UK defense and aerospace industries. UK defense procurement policies emphasize the use of inter-organizational IT networks to improve project performance, and groups of firms, often competitors, and sometimes their customer organizations are increasingly sharing in the design, development, manufacture and operation of complex products. Industry and the UK Ministry of Defence (MOD) are developing precise codes of practice and procedures, guidelines and contractual conditions affecting all aspects of the contractual process and project management including IP management. This situation provides a unique test bed for analyzing the issues encountered when trying to use advanced ICT to support data sharing and collaboration among organizations, and the potential solutions that can be offered.

---

the degree to which collaboration technologies have been applied falls short of implementing the capabilities required by current collaboration

---

One might think that the same tools that are applied within the firm could be easily transferred to inter-organizational environments. In principle, the technology exists to share across organizations large amounts of technical data (including designs, product specifications, manufacturing processes, etc.) using electronic networks, software platforms, and electronic data management systems. But our research in the UK in 2004-5 showed that the degree to which collaboration technologies have been applied

falls short of implementing the capabilities required by current collaboration platforms. The situation has not changed much from that in the mid 1990s, when an expert in a major aerospace firm stated that the industry displayed "a file transfer rather than an open database mindset"[9].

We carried out a series of case studies of major defense projects involving all the main UK defense suppliers to identify the ways in which ICT tools were used to support collaborative projects and the problems they faced. We then analyzed a current transatlantic initiative to set up processes and regulatory environments to address these problems (see Appendix).

Our examples are derived mainly from the UK defense industries. Despite the peculiarities of this sector, there is nothing inherently distinctive in the IP contractual procedures and guidelines developed within defense. For instance, the guidelines on how to set up a contractual structure for a "shared data environment" as discussed below are equally applicable to any other industry wishing to pursue such a mechanism for collaborative projects. Further, the UK defense sector is becoming more open and akin to other competitive commercial environments,[10] where trust between suppliers, and between them and the client becomes a key component of the business relationship. The experience that the UK defense sector is developing is significant for other sectors.

Through our case studies we identified a set of common problems but found very few cases in which technical data was shared across organizations through databases accessible from outside the organization hosting them. In this paper we first present the main problems that IP management presents when using IT to share technical data across organizations. We then discuss two different instances of projects that had organized technical data sharing for product design and development across firms: both approaches revolve around the setting up of centralized technical databases but organize access to them by project partners very differently. A different approach is being developed to underpin a "federated" structure, in which data is stored in different sites and access is organized through multilateral arrangements. Whatever the approach selected the application of advanced IT for technical data sharing across organizations

[9] J. Molas-Gallart, "Telematics in Life-Cycle Management," (International Conference on Management and New Technologies. Madrid, 1996).
[10] J. Molas-Gallart and P. Tang, "Ownership matters: intellectual property, privatization and innovation," *Research Policy*, volume 35, 2 2006, pp. 200-212.

emerges as a complex undertaking, requiring the development of new governance systems and the collaboration between IT, legal, commercial and engineering functions.

2 The sticky IP issues in collaborative environments

2.1 The protection of information

The first key problem with sharing technical data to develop new systems is the protection of "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 developed for a project, and therefore other firms may need to have access to other parties' "background information." By sharing background information companies run the risk of inadvertent leakage of commercially sensitive information; not only technical data about specific components, but also designs, design techniques or other processes that are generally kept as trade secrets.

The second potential problem relates to the *early* release of "foreground information," and technical data developed during the course of the project. Although the customer will have rights of use over such foreground information where it has funded its development, the concern for contractors relates to the possibility of access to data that is still being worked upon. This poses two concerns. First, work-in-progress foreground information may include commercially sensitive information on company techniques and processes that would *not* be reported in the final data packs delivered to the customer. Second, firms are concerned about liability issues that may be derived from the customer accessing and using data that are still in draft form and not ready for delivery to the customer.

The use of advanced ICTs generates additional concerns in relation to these problems. Because digital data is easy to replicate, systems to monitor and track the information shared and strict procedures on data sharing must be established. Such systems and procedures are more than a technical problem. Although approaches exist or have been suggested for strict data access control (see below), there is a palpable fear among the IP and commercial managers in all the companies interviewed that engineers do not adequately appreciate the importance that misappropriation of information may have for

their firm. Anecdotes abound of engineers that were only too happy to share proprietary and commercially sensitive technical details with their peers in other companies. Interviewees attributed such behavior to "cultural" traits within the engineering community that drive individuals to share their work with their partners across organizational divides, much in the same way that academics are widely assumed to do. These concerns are exacerbated by the use of digital exchange networks, as they could allow a loquacious engineer to send reams of technical information across to project partners at the click of a mouse.

All the companies interviewed made a compelling case for the need to "educate" their engineering staff about the importance of protecting their IP appropriately, particularly as advanced ICT tools are increasingly supporting inter-organizational collaboration. There is ample evidence to show the importance of changing behavior when new tools or processes are introduced in companies. So here too, it is not surprising to observe that cultural patterns lag behind new methods of working.[11]

2.2 Convergence of product and process data

Another problem lies in the confluence of product and process data within the same data sets for systems design. This is the case, for instance, in the manufacture of specialized components for aero-engines or for aero-structures, which is driven by unique software-based processes. Naturally companies do not wish to reveal these processes to third parties, but sharing product data in electronic format could imply sharing also software-based processes when product and processes data are inextricably linked. Companies that base their competitive advantage on the uniqueness of their manufacturing processes fear that shared technical databases could make them vulnerable to disclosure of their trade secrets.

2.3 Divergent approaches to IP management and data control among collaborators

To complicate matters even further, defense projects will often involve foreign partners operating within different legal and regulatory environments. For instance, sharing of technical data will often come under export control regulations. This means that any

[11] S. Thomke, "Capturing the Real Value of Innovation Tools," *Sloan Management Revew*, volume 47, 2 2006, pp. 24-32. at pp. 31-32.

data sharing system will require control access systems and procedures able to cope with the export and technology control regulations in each of the participating countries, otherwise collaborating companies may violate their partner's national export control regime. IP management methods will have to be coupled with the technical and regulatory structure emanating from this need to adhere to different export control regulations.

---

any data sharing system with foreign partners will require control access systems and procedures able to cope with the export and technology control regulations in each of the participating countries

---

A related problem is the lack of consistency in the meaning of the terms used by firms and governments to class the different levels of information protection and access. For instance, terms like "restricted" are interpreted differently among firms and governments. Although we found no cases in which these differences led to identifiable financial losses or leakage of vital IP, our interviewees were adamant about the need for consistency and common use of terms, particularly when structuring platforms to share technical data in international collaborative projects.

Further, beyond differences in legal terminology and regulations, coping with different approaches to IP management across countries is also problematic. Firms may not be able to trust the practices of their foreign partners and may decide to withhold information. We were offered examples of firms involved in international collaborative *research* programs that were deliberately withholding information, thus resulting in the joint research project performing at a sub-optimal level.

2.4 Diversity of solutions and lack of an IP strategy

All of the firms involved in our case studies, and their customers in the UK Government are simultaneously using different network technologies and inter-organizational systems to support their work in large complex projects. These projects typically involve many suppliers coordinated through a prime contractor to provide a system or a service for use by the UK armed forces. In practice, we found that every project established its own set of network technologies and inter-organizational systems. Each adopted different contractual clauses, different IT systems and different approaches to the management of IP. This meant high set up costs for every project (there is an

element of reinventing the wheel and limited cross-project learning), and a variety of network environments. In one case, a large corporation was running over 300 separate projects supported by different IT networking arrangements and contractual conditions to manage and share data with, often the same, customers and suppliers. Such a situation engenders not only additional costs but also a situation in which it is difficult to maintain data integrity and control the information flows through the variety of inter-organizational systems in place.

In one case, a large corporation was running over 300 separate projects supported by different IT networking arrangements and contractual conditions to manage and share data with, often the same, customers and suppliers

Partly these variances are due to the lack of detailed corporate IP policies, a finding also reported by a study commissioned by DLA, a London-based law firm.[12] Although large companies are familiar with the process of protecting their IP, and employ patent attorneys, copyright specialists, etc. within an IP department; their strategies are narrowly focused on the legal protection of *rights* rather than the management of *intellectual property*. For instance, the firms interviewed for this project either focused their IP management approaches on patenting strategies or relied on trade secrets. Yet a concentration on IP protection does not amount to a comprehensive corporate IP management policy. We observed that the IP management "ethos" was biased, in the main, toward formal protection processes, essentially deciding whether or not to patent. The often-informal practices that determine, for instance, when and how to share proprietary information with clients and partners are not instituted as part of a corporate IP policy. Only one firm interviewed had a clearly articulated IP management policy supported by an IT system to track the patents used in each of the firm's products.

3 Developing Solutions: two approaches

These issues are being tackled. Defense agencies and their industrial suppliers continue to seek solutions to address the aforementioned problems but many remain in their planning stages. We present here the two main approaches to the development of shared

[12] N. Tait, "'Alarming' findings on intellectual property," (London, 2004).

technical databases to support the work of large networks of suppliers and customer organizations:

1. The use of a centralized technical database managed by a project partner; access to the database by other project partners is administered through bilateral arrangements with the managing organization. Existing systems use relatively simple implementations of this approach.
2. The mutual granting of access to databases held by the different project partners to other project partners. This distributed approach does not require the setting up of a centralized database but allows the transfer of technical information to facilitate collaboration among partners in project development, design and manufacture. This approach requires access management systems built upon "federated identity assurance systems" managed by trusted third parties. These systems are being developed and are currently at the "proof of concept" stage.

3.1 Centralized databases backed by bilateral arrangements

Centralized databases require the existence of a database manager responsible for administering access to the data and insuring that illegal access and usage of data is prevented. The database manager typically engages in bilateral agreements with all project partners requiring access to the centralized database. Yet in our research we identified two very different ways in which this relationship can be organized:

1. A "regulated approach" based on the use of commonly agreed contractual clauses and forms that establish the characteristics and rules guiding the operation of the centralized database.
2. A "prime-dominated" approach, where the prime contractor controls the definition of the inter-organizational system and imposes it, together with its associated IP conditions, to its international supply chain.

We discuss both examples in turn.

3.1.1 Regulated Approach

This approach involves the use of a set of contractual conditions agreed jointly between industry and procurement agencies, in our case study, those of the MOD. These contractual conditions are embodied in, so-called, "defence conditions" (DEFCONS).

Accompanying forms and templates for annexes that can be appended to contracts are known as DEFFORMS. There is large set of these documents, which provide detailed contractual clauses and provisions applicable to different situations, available for contract officers to include in contracts. [13] Although they are not mandatory, they provide, in practice, an established contractual framework that defines the MOD negotiation policy for key aspects of defense procurement, including IPR and data protection issues. DEFCONs and DEFFORMS are a common tool in UK defense contracting.

Industry and representatives of the procurement agencies jointly developed, between 2000 and 2001, a set of DEFCONs and DEFFORMs (known as the "687 family") to establish how a "Shared Data Environment" (SDE) should operate in collaborative projects. They provide guidance on how to set up the obligations and responsibilities of the manager of the centralized database in the SDE as well as user rights and obligations.

In our case studies, the Type 45 warship provides an example of a collaborative program that adopts the regulated approach. Exhibit 1 below describes the first program to make use of the "687 family" of DEFCONs and DEFFORMs developed by industry and procurement agencies to establish the norms under which a centralized product data system will be made available to a variety of program stakeholders: the development and construction of a the "Type 45" frigate for the UK Navy. BAE Naval Ships, the prime contractor, five main supplier firms and the program client, the Defence Procurement Agency were involved in defining the SDE, its applications and management, and the user practices. This process was conducted through an "Enterprise Integration User Group," which comprised representatives of all the main stakeholders responsible for overseeing the system implementation and reviewing and updating the enterprise integration strategy. The resulting "Enterprise Integration Implementation Plan" affirmed that IPR previously owned by a stakeholder would not "normally" be published in the SDE, and that, if it was, such "background IPR" would be protected by access controls and made accessible only to the required and authorized-to-access stakeholders.

[13] Ministry of Defence, "Guidelines for Industry. 10 The Intellectual Property Rights (IPR) DEFCONs. Part B," Defence Procurement Agency, 2004).

Access to the database is organized through a "folder" system, which controls different access levels, according to the role of the project participant. The system is based on Internet architecture, can be accessed through a Wide Area Network or dial-up connections, and uses a suite of off-the-shelf software applications. In some cases the applications have had to be modified in-house to adapt them to the specific needs of the program.

Exhibit 1: Regulated approach: the Type 45 warship

The Type 45 Anti-Warfare Destroyer is a large 7350-ton ship designed to provide fleet defense for the UK Navy. Six platforms have already been contracted out of a total planned requirement of eight.

It is interesting to note that five years after its initial development, "Type 45" remains the only full-fledged program to implement some of the contractual tools in the "687 family." In this program, the prime contractor (BAE Systems Naval Ships) is charged with creating and managing a database of project information. Access by users is underpinned by a "database information agreement" that sets out mutual obligations for all parties. These include IP conditions on the data uploaded to the database by project partners, and an obligation on the contractor to grant a user license to the final customer (for example, the Navy) in the Ministry of Defence to operate and maintain the database once it is transferred to the operator.

The Type 45 SDE is limited in the extent of the applications and data exchanges it supports, falling rather short of the wider aspirations at which 687 was aimed, namely sharing of all relevant information and data required for the project. Instead, the Type 45 system carries extensive information on *project management* tasks, and provides a tool for sharing limited project information across several participating firms and the client representatives. For instance, the system is limited to information that does not have a classification of "Confidential" or higher national security restriction, a classification of which is not unusual in defense projects. Further, all the participants in this program are domestic firms, thus avoiding the legal complexities that would emerge in a project with international partners.

Technical data published in the SDE includes graphical representations of the "product geometry" and results in a "product model" that can be used to guide the evolving design within the collaborating firms. However, detailed design data, for instance the CAD files for the design of the different elements are not shared through the SDE.

Despite these limitations the Type 45 SDE presents a new stage in the extent to which collaborative ICT-base tools have been implemented to facilitate the collaboration across organizations involved in the development, production and operation of a complex product and the management of stakeholders' IP. The system has been operational for almost five years.

Data sharing in a shared digital environment is less complex when there are only domestic partners.

3.1.2 Prime dominated approach

The complexity inherent in shared technical data through advanced ICTs is magnified when it involves international partners, primarily because of compliance with different export control regimes and national regulations on IPR and privacy.

Participants in the Type 45 SDE pointed out that a reason for the relative simplicity and success of the SDE is that it serves a domestic project, which does not allow access to foreign suppliers. The Joint Strike Fighter (JSF), US-led, international development and production program provides an example of the challenges faced when international collaboration is organized around a centralized product database.

The prime contractor for the JSF is "Lockheed Martin Aeronautics" (LMA), who is both the final assembler and systems integrator. The company is also a sub-systems and parts manufacturer for the aircraft. LMA has implemented a central repository for all the technical data for the aircraft, which rests on Internet standards and a combination of off-the-shelf software tools. LMA mandates that all suppliers use this system as a condition for participating in the project, and manages, controls, defines and establishes its architecture and data management procedures.

The system for sharing data in the JSF program revolves around a Joint Data Library (JDL) that serves as the node for the sharing of technical data across project participants. Ownership of data in the JDL is indicated by restrictive agreed legends, which are included in the footer of all data and drawings.

Access to the JDL is established through formal agreements, so-called Technical Assistance Agreements (TAAs) between LMA and its suppliers. TAAs provide the formal approval mechanism enabling stakeholders to post and access data in the SDE, and specify the kind of data that can be accessed and used by the supplier. TAAs have become very complex tools to operate, particularly when they involve foreign (non-US) suppliers. Often several TAAs are signed with each supplier covering different sets of data for which the supplier acquires rights to upload and download. In particular, when the suppliers are foreign nationals the TAAs have to take into account US export control regulations and establish data access controls accordingly.

Exhibit 2: Prime dominated - the JSF Program

The participation of foreign companies clearly makes the management of shared data across electronic networks more complex because of different national legislations, particularly with regard to technology export controls (of which information is obviously an integral component). While the JSF system for sharing information is effective, it is arguable that it is inefficient.

The positive effect of requiring a TAA to access the JDL is that a mechanism is established to takes into account export control regulations so data accessible by a partner through the JDL is, in practice, approved for transfer abroad in accordance with existing US export control regulations. There are, however, many negative effects.

First, the system has become cumbersome to operate. For instance, a British firm participating in the program has signed more than 160 TAAs covering, among other things, different requirements relating to the export and re-export of the technical data in different components and sub-systems.

Second, any data communication between two suppliers has to be approved by the prime contractor, regardless of the TAAs signed between the two suppliers and the prime. Accordingly the JDL is partitioned: suppliers cannot access the project data of other suppliers, only LMA as prime contractor has access to all data and information in the JDL. Further, when a supplier is involved in different subsystems it will access different and separated folders under different TAAs. This means that different parts of a corporation working on other sections or aircraft sub-systems will not have access to each other's data sets within the JDL. A positive effect of this data segmentation is that each supplier has its "own" set of folders containing its information, thus providing a means of data protection, and avoids potential confusion as to what information belongs to whom.

Third, the system slows down collaboration across suppliers. If a company needs data from another supplier, it will have to request it from LMA, who will then "post" the information in a common folder available to both companies, after checking that the requested information is available and indicated on the TAAs signed by both companies. Furthermore, such a tedious procedure results in data replication across folders, which introduces configuration challenges and a high risk of data fracture. This happens because the data in one folder could be updated without the same data being changed in another folder, thereby ending in two versions of the same document.

The fourth pitfall is the cumbersome nature of access management. Any supplier employee wishing to access JDL data will have to request permission from the prime contractor, who then manually checks whether the individual is covered by a TAA and the rights that this TAA establishes. Once this information is ascertained, LMA provides access to the relevant project folder or folders. Yet the onus is on the individual to ensure that the information or access rights it needs are listed on the relevant TAA. Participating companies have had to train the employees working on this system on the complex operating procedures by which it is managed.

The participation of international partners increases the complexity, unwieldiness and difficulty of data management in a shared digital environment.

3.2 Federated Trust Environment Approach

Clearly, there are limitations to both of the approaches to setting up centralized technical databases for data sharing across partners reviewed above. Both the "regulated" and the "prime-dominated" approaches are dependent upon a central logical data set for a specific project under control of either a third party or the prime contractor. The protection of the information is provided by the data base technology, and the access is controlled by mechanisms unique to the project. This can be wasteful

since project 'stove-pipes' will be created, common information shared among different projects can become mismanaged, and individuals working across multiple projects will require multiple identities for accessing different systems.

These difficulties can help explain the limited diffusion and modest applications that in practice have characterized the deployment of ICT-based collaborative tools. Currently, when deployed, these systems are unwieldy to operate or address a small part of the total work to be carried out, and in any case are expensive to implement. The wheel has to be re-invented for every project, and it is a very expensive wheel. If more projects with more collaborative partners across more nations are to be supported by ICT-based collaborative tools the type of bilateral arrangements discussed above will prove inadequate.

The challenge is to allow the re-use of systems for technical data sharing across different projects, while meeting the demands of the regulatory authorities and customers. Thus, there appears to be a need to develop common approaches endorsed by a group of powerful customers and suppliers with the capacity to push the implementation of common technical solutions and standards of practice throughout the industry. This is already being undertaken by the Transatlantic Secure Collaboration Program (TSCP), an initiative of a group of European and US firms, involving all major aerospace and defense suppliers, with the support of governments, to develop a framework for secure transatlantic collaboration.

The solution this group is developing is the establishment of a Federated Trust Environment of identity and access management, underpinned by audit. Unlike a centralized database supported by bilateral arrangements, a Federated Trust Environment is characterized by a system of distributed databases accessible to project partners and sustained by a multilateral regime for identity assurance and access management. Participants in the environment must be assured that individuals accessing the data are who they say they are. This requires a robust identity management system that establishes commonly agreed methods for proofing and vetting, before a credential is issued. The credential will then be presented at system log-on or for access to any application for any project or for access to any database wherever it is located.[14]

[14] There are examples of systems of this type already being implemented. For instance, the US Department of Defense has issued over 4 million cards to its employees that double as identity cards for access to sites and tokens with private key encryption credentials needed for access to DoD IT systems. A

Further, different individuals will be entitled to access different types of data and do different things with them (read, download, change,…). This must be organized through an access management system. Information in accessible databases is to be organized into standard categories according to their sensitivity and marked electronically.

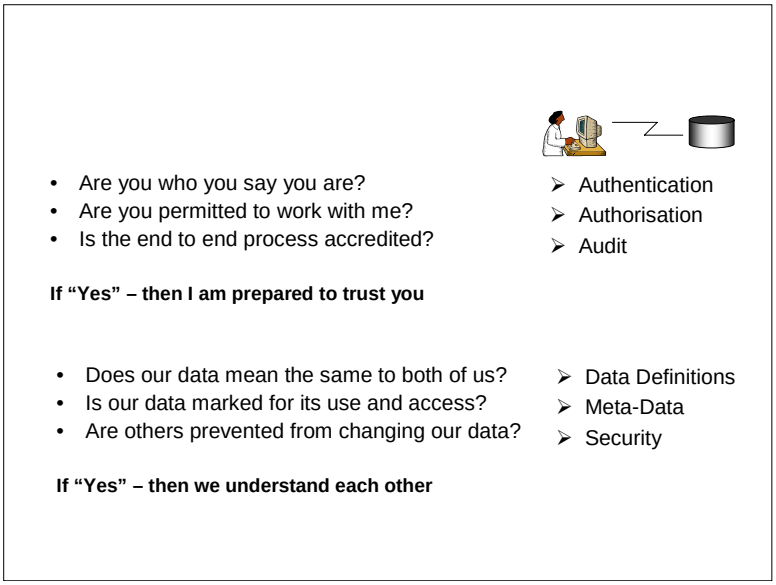


Figure 1. Secure collaboration – trust and understanding

The TSCP is developing the norms and procedures to establish identity and access management systems and testing them. The objective is to establish an e-collaboration architecture allowing potential collaborating partners to establish their trustworthiness to others by having a proven capability to manage others' information by giving it the appropriate protection, and demonstrating compliance with the regulators in charge of export and national security policies. Once these abilities are certified, organizations would be able to engage in collaborative work accessing each other's data. For this environment to work companies will require assurance that their collaborating partners are working to the agreed policies and therefore certification and audit by a trusted third party. This differs from the centralized database approach where responsibility to administer and control data access falls on the system manager, typically the prime contractor. In contrast, a distributed system requires third party involvement to ensure that adequate access control to protected data exist within each collaborating partner's

---

first test, allowing a DoD individual, using her own credential, to access protected data in an application held in an industry system, has been successfully carried.

own ICT system. Such a system will be applicable across projects, doing away with the present practice of setting a different system for every large project launched.

The process to develop this environment is long and difficult. More than 50 specialized personnel have worked on this project at any one time and the results are publicly available (www.tscp.org). TSCP originally commissioned Booz Allen Hamilton to produce a Framework and a Design for building secure IT collaborative environments, including the required processes, mechanisms and technologies for collaborating partners.[15] TSCP with the collaboration of participating firms is now testing the concepts of Federated Identity and Access Management and drafting the framework policies so that corporate capabilities can be used across multiple programs and multiple jurisdictions. The participant companies have built testing labs to prove that identity credentials from one organization can be accepted by another, having been cross-certified through third parties. A certification organization, CertiPath, has been selected to develop and test certification an audit licensing scheme.

Repeatable solutions for data sharing provide optimal protection but they require commitment from collaborating partners and significant upfront investment.

---

4 Practical steps

Whichever approach is to be taken for the development of shared databases, some early actions will help in establishing a suitable framework for secure collaboration. The practical steps are:

- Establish an ICT infrastructure to share information rather than exchange it (Use accessible databases not email)
- Set up an Information Manager in each organization to bring together the engineering, program management, commercial, legal, compliance, security personnel and ICT functions

[15] Booz Allen Hamilton, "Transatlantic Secure Collaboration Program (TSCP). How-To-Guide," UK Council for Electronic Business, 2004), Booz Allen Hamilton, "A Framework for Secure Collaboration across US/UK Defense," UK Council for Electronic Business, 2003).

- Set up a cross-organizational Information Managers' forum to develop an agreed collaborative approach to data sharing
- Agree the generic classes of data to be shared and that not to be shared
- Agree the level of protection required for shared data and who can access it

The next steps depend upon the commercial framework of the program. We can distinguish 3 main approaches.

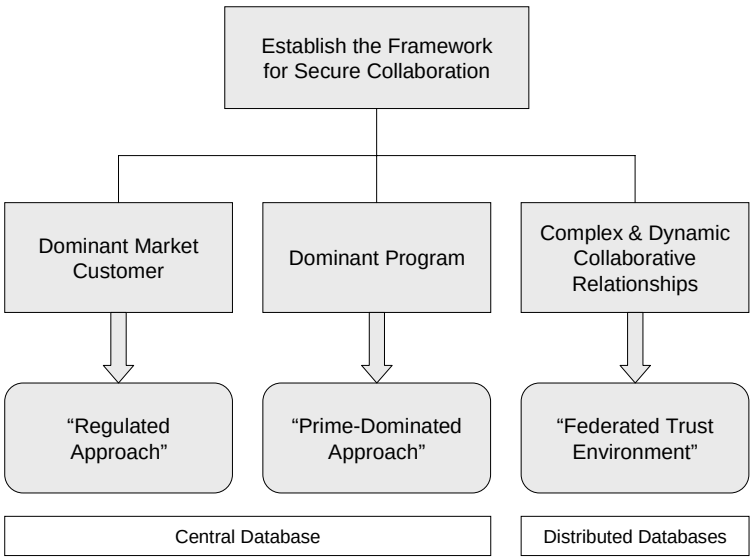


Figure 2. Deciding the database approach

1. *Dominant Market Customer*. If there is a strong customer that dominates the market or sector, which is likely to have multiple contracts amongst many common suppliers, then there is an incentive for suppliers to have longer term standards for collaborative information sharing. The practical steps are:
    a. Motivate the dominant customer in the sector (defence, petro-chemical, retail) to be the catalyst in developing standard methodologies for sharing data
    b. Work with other suppliers to develop and test the standards
    c. Build internal systems and procedures compliant with the standard that could be re-used in other programs and with similar customers in the same market

2. *Dominant Program.* If the program is a significant size and has one partner that is a systems integrator and prime contractor, who owns most of the IP and provides many of the sub-systems, then the practical steps for suppliers are:
    a. Establish the ICT network based upon the prime's system
    b. Set up access controls acceptable to all collaborating participants
    c. Use applications that have as much common consensus as possible (suppliers who have to change will incur costs to the program)
    d. Ensure the infrastructure and information management costs are charged to the program – very little will be re-usable
3. *Complex and Dynamic Collaborative Relationship.* If the collaborating partners have (or will have in the future) differing information sharing requirements and operate to different rules on protection (such as in an international program subject to multi-jurisdictional regulations), the practical steps are more expensive, but the solution should be more resilient over time:
    a. Establish the business case for a federated trust environment based upon the otherwise consequential costs of:
        1. Non-compliance of national regulations
        2. Non-compliance with contracted requirements on data protection
        3. Loss of IP
        4. Configuration of replicated data
        5. Unauthorised access to program, company or government data
    b. Work with partners on common policies for identity and access management that will comply with governments' regulations
    c. Confirm with the regulators (commercial or government) that they will support the policies
    d. Invest in Identity and Access Management technologies and engage auditors to assist in promoting 'trustworthiness' of the organization in holding data owned by other parties.

The choice of approach depends on the characteristics of the collaborative project, whether it (a) has dominant market player; (b)is a dominant program in which the prime contractor owns the majority of the IP or (c) is international with differing information sharing requirements

5 Drawing the lessons

This article has analyzed the data access issues that arise when different organizations involved in the development and delivery of a large product system consider using ICTs to support technical collaboration in design and manufacture. We have found that establishing ICT systems to collaborate across organizations in the development and production of complex products is an intricate task: e-collaboration is not easy and many of the problems it generates have not received much attention in the management literature. For instance, current literature on corporate IP management focuses mainly on the management strategies to be developed by an individual firm, and yet we have found that the data problems posed by collaborative activities have worried aerospace and defense manufacturers in their use of ICT. Many of the problems faced are derived from the complex problems faced in project implementation. Often, the devil in the application of ICT to support interorganizational collaboration is in the implementation details.

Despite the difficulties we have identified, defense industries are particularly well-placed to address the data issues raised by collaborative projects from which lessons and practices may be learned or adopted. First, defence firms have a long experience in engaging in large development and manufacturing projects requiring collaboration among many different firms, and with a powerful customer playing important roles in project design. Second, the existence of a small number of leading suppliers and of a single customer (at least at national level) should simplify the institutional complexities of dealing with IP and data management questions. In the defense industries a small group of organizations can coordinate policy solutions that can then be transferred to the whole industry.

This paper has shown several instances in which potential solutions are being developed by a small group of suppliers working with the defense procurement agencies (like those being developed by the TCSP, or the conditions available for UK defense

contracts). Importantly, many of the solutions that have been developed are freely available: DEFCONs, DEFFORMs, and TCSP reports are all available on the Internet, and can provide guidance to firms in other sectors about how to tackle the issues surrounding technical data sharing among different organizations.

In the end, the main challenges for collaborative project using and sharing data across ICT networks in any sector are of a managerial and regulatory nature.[16] Technologies to manage technical databases, to transfer this data securely through ICT networks, to enable identity management, and to control data transfers are available. What has proved, so far, extremely difficult is to harness existing technical capabilities by developing and deploying data management processes, and tailoring and implementing ICT systems to follow these processes. This requires, among other things, a commitment to allocate the necessary resources for managing information as a protected and valuable asset throughout any collaborative partnership. Any of the systems we have discussed is expensive to implement. But they are not nearly as expensive as the costs arising from non-compliance, configuration of replicated data, recovery from lost IP or the management of multiple bilateral relationships with suppliers.

In the projects we studied we found that sophisticated systems to enable real-time collaboration across partners were viewed by project directors as additional costs rather than investment for the future, as it is often difficult to attribute specific monetary benefits to the introduction of these technologies. Yet, this cost is largely due to the fact that each project is addressed in isolation, so that each new SDE has to be developed almost from scratch. Developing a re-usable solution would tackle this problem, but the up front investment necessary to set up a whole company to be able to operate the federated systems being designed under TCSP auspices are again substantial. For instance, a corporation of 20,000 employees would have to invest over $9 million to certify the whole firm at the highest level of security.[17]

The initiatives presented in this paper are building blocks towards the development of e-collaboration solutions. These, however, are being developed through collaboration among suppliers (who are at times competitors in the market) and their customers. No

---

[16] A. Dutta and K. McCrohan, "Management's Role in Information Security in a Cyber Economy," *California Management Review*, volume 45, 1 2002, pp. 67-87, Ernst & Young, "Global Information Security Survey 2004," Ernst & Young, 2004).

[17] See http://www.tscp.org/Documents/TSCP%20Public%20Release/TSCP-Generic-Migration-Plan-Cost-Model-v1.0.xls.

firm on its own can develop the tools and approaches that will need to be adopted by a whole community.

Further, whatever the solution implemented, the use of advanced ICT to share and protect technical data in collaborative projects requires the existence of a coordinated IT and IP strategy at the corporate level. Commercial and legal personnel must be involved in developing the policies but so should the engineers and IT personnel who will be responsible for implementing and running the system.

Contractual obligations, IP practices and IT architecture must be linked and coherent to ensure that IP is properly protected and used, and data access effectively controlled. This requires close collaboration between the commercial/legal and IT departments, and therefore needs to be led from the corporate executive level. An executive drive is needed to bring together the commercial, IP and IT functions within the company and across the different partners in a collaborative project, and to support the establishment of strategies for secure data usage in collaborative projects. This need for executive commitment is consistent with the recommendations derived from previous research on ICT implementation. McAfee has highlighted that managerial support and leadership is crucial for successful adoption of new ICT technologies for collaborative environments within the firm.[18] Similarly, P. Weill and J. Ross remind company policy makers that that only when senior managers are committed to the establishment and implementation of secure and advanced IT applications, can their companies get more value from IT.[19]

Effective management of IP in collaborative programs requires (1) executive leadership to ensure close coordination between the commercial/legal and IT departments and (2) careful consideration of the characteristics of the project.

What we have shown here is that executive commitment is not only necessary for effective and successful implementation of IT systems within the firm, but must also drive the setting up of IT systems to underpin interorganizational collaboration. The costs of implementation and the complex regulatory environment (different IP legislation, technology export control regulations,…) in which technical data exchange

[18] A. P. McAfee, "Enterprise 2.0: The Dawn of Emergent Collaboration," *Sloan Management Review*, volume 47, 3 2006, pp. 21-28.
[19] P. Weill and J. Ross, "A Matrixed approach to designing IT Governance," Ibid., volume 46, 2 2005, pp. 26-34.

systems must operate place their implementation beyond the reach of the specialized IT department. We have also attempted to provide a menu of choices to secure data sharing among partners in collaborative programs/projects.

Methodological appendix

Our analysis conflates two different streams of research. First, a study was carried out of the extent to which "Shared Data Environments" were implemented in the UK defense market, and the IP issues that emerged when firms and their customer organization tried to use ICTs to share technical data in digital format across organizations. The two cases discussed in the article (Type 45 Frigate and the JSF) were taken from this research. This study followed a case study methodology. We first undertook a documentary study of the IP practices and regulations for defense contracting as laid out in the "contractual conditions" used by the MOD procurement agency (the Defence Procurement Agency – DPA). We followed with a program of semi-structured interviews using two different interview protocols, one addressing corporate policies and activities, and another oriented to the analysis of IP management practices within specific projects. The main objective of the interview program was to determine the ways in which firms addressed IP management in a digital environment both within the corporation and in collaborative programs. To guide the interviews we designed a protocol structured according to a list of IP management topics with potential effects on firm and corporate performance. We based the list on IP management issues identified by the extant literature on IP management within specific sectors and firms.[20] A panel of academic, industrial and government IPR experts validated the interview protocol, which we then piloted through a 6-hour long interview with two IPR and commercial managers of a major UK defense corporation. Following the pilot we adapted the protocol and used the two different formats, as noted above.

[20] O. Granstrand, "The economics and management of technology trade: towards a pro-licensing era?," *International Journal of Technology Management*, volume 27, 2-3 2004, pp. 209-240, B. Guilhon, R. Attia and R. Rizoulieres, "Markets for technology and firms' strategies: the case of the semiconductor industry," *International Journal of Technology Management*, volume 27, 2-3 2004, pp. 123-142, B. H. Hall and R. H. Ziedonis, "The Patent Paradox Revisited: An Empirical Study of Patenting in the U.S. Semiconductor Industry, 1979-1995," *Rand Journal of Economics*, volume 20, 1 2001, pp. 101-128, P. Tang and D. Paré, "Gathering the Foam: Are Business Method Patents a Deterrent to Software Innovation and Commercialization?," *International Review of Law Computers & Technology*, volume 17, 2 2003, pp. 127-162, P. Tang, "How electronic publishers are protecting against piracy: Doubts about technical systems of protection," *The Information Society*, volume 14, 1 1998, pp. 19-31, P. C. Grindley and D. J. Teece, "Managing Intellectual Capital: Licensing and Cross-licensing semiconductors and electronics," *California Management Review*, volume 39, 2 1997, pp. 8-41, C. S. Shapiro, "Navigating the Patent Thicket: CrossLicenses, Patent Pools and Standard Setting," 2001).

We then carried out interviews with all major UK defense systems producers. Between November 2003 and July 2004 we conducted detailed interviews with 20 relevant executives; involving IP Directors, Commercial executives, IT systems directors, program directors and lead engineers. In addition we held several meetings with other officials from industry, the DPA and a defense industrial association. In total we carried out 66 hours of meetings and interviews with 33 senior officials and executives. Except for six telephone interviews, the rest were all face-to-face interviews and meetings. Within each participating company most of the interviewees were self-selected by their organizations based on their work on IP management and IPR issues both within the company, and in collaborative projects and defense contracts. Because of the commercial sensitivity of the issues explored we do not attribute the information collected and used in this article to any name and affiliation of the individuals interviewed.

The second stream of work that the article draws on is the development of an approach to federated data and identity management by the main UK and US defense contractors with the support of the US and the UK defense ministries. This effort, which was initially managed through UKCeB, has evolved into the Transatlantic Secure Collaboration Program, for which the Director is still provided by UKCeB, and is one of the authors of this article.[21] The Program was undertaken in parallel with our research and continues till today. The participant companies have built testing labs to prove that identity credentials from one organization can be accepted by another, having been cross-certified through third parties. Federated identity management is being applied to secure email, collaborative document management and to PDM applications for product design. Access management policies are being scoped and an auditor licensing scheme developed. The Program is itself managed collaboratively, through multiple working groups of participants reporting to a Governance Board. The US DoD and UK MOD are members. TSCP has contracted a Design Authority to coordinate and document the technical work, as well as leading on the development of the labs.

[21] Robert Shields was the Director of the TSCP Program until 2006.