Yours, Mine, or Ours: Discussing Ownership of Collaborative Works in the Cloud

Marilyn Phelps  
San Diego State University  
lynphelps@gmail.com

Murray E. Jennex  
San Diego State University  
mjennex@mail.sdsu.edu

Abstract

Increased usage of cloud storage and other networking technologies in knowledge management (KM) systems leave companies vulnerable to loss of proprietary rights as intellectual property law struggles to keep up with these advances. This paper reviews the current legal environment surrounding cloud and collaborative KM, discusses the implications for KM, and makes recommendations for how gaps between legal protection for intellectual property and KM can be overcome/corrected.

1. Introduction

Knowledge Management (KM) is about capturing knowledge created in an organization and making it available to those who need it to make decisions. KM achieves this by helping organizations leverage what they know and by improving connectivity between knowledge sources and/or knowledge users. Much of the emphasis in KM research is focused on knowledge impacts on organizational performance and competitive enhancement [4] [14] [26] [27] and explores how to mitigate knowledge sharing barriers and organizational issues. Additionally, technology research focuses on how to improve technologies to make knowledge discovery, creation, storing, transfer, sharing, and use easier. One such technology being adopted for facilitating knowledge storage and sharing is cloud computing.

Cloud technologies are service based products such as Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) that are hosted on the web by providers who offer the services internally or externally to other organizations. Cloud services provide cost savings to organizations by allowing organizations to utilize only the services they need while at the same time being easily scalable to meet future needs. Organizations use the cloud to support KM by providing storage and tools for knowledge manipulation, capture, and/or use in a central location that can be accessed by users who can be located anywhere in the world [28]. Since the cloud is available to anyone on the Internet it is supporting the need for collaboration resulting in knowledge creation and innovation and is encouraging organizations, particularly smaller organizations, to create and use virtual teams and knowledge networks, small intra-organizational groups tasked with knowledge sharing, creation, and innovation.

While improving knowledge flow, sharing, and use is very beneficial to increasing innovation in organizations, and there is much research focused on these aspects; there is little research looking at the potential risks. Cloud technologies are easy to use and are widely adopted for helping teams and organization innovate and do KM. However, there are many risks associated with the security of knowledge on the cloud [43]. Jennex and Durcikova [25] summarized the literature associated with KM security and found it to be focused on the technical issues associated with cyber security technologies and technology risk assessment (including cloud technologies). Little to no literature was found on the legal risks to intellectual property associated with using cloud technologies and approaches for KM and innovation.

This paper explores the legal risks of applying cloud based KM to managing knowledge and intellectual property in networked environments. Specifically, there is a gap between the current state of intellectual property law and the current state of technology and KM practice. This gap leaves companies vulnerable when using KM systems that utilize modern networking technology such as cloud storage. Additionally, the current state of intellectual property law leaves companies vulnerable to loss of proprietary interest over knowledge shared on knowledge networks and cloud based KM systems, suggesting the need to provide default statutory rules over network transactions.

Finally, collaboration between companies presents a large risk to the intellectual assets of the participants; intellectual property law needs to provide guidelines for these interactions. Companies need to be aware of the risks provided by both cloud usage and collaborative efforts so that they may protect themselves and push for change in the industry.

The scope of this paper is limited to the intellectual property landscape in the United States. It is recognized that much collaboration and innovation is
occurring across national boundaries and as such the issues discussed are impacted by the intellectual property laws of these other countries also. However, it is considered a good first step to first understand the legal environment of the United States due to the importance the United States in the world economy.

2. Methodology

This paper utilizes legal research methodology. Legal research methodology is not conducted the same as social research in the information systems (IS) tradition. IS research tends to be quantitative (using surveys) or qualitative (case study, action research, design), or a mixed method. Legal research uses a methodical approach to finding relevant legal opinions [33]. This is called doctrinal research and is the normal research method used by legal scholars, students, and attorneys [24]. This paper used patents as knowledge artifacts and conducted searches on intellectual property, patents, collaboration, and cloud computing. Articles were used that addressed the legal questions; who owns collaborative knowledge, who can use collaboratively generated knowledge, and what are the limitations on the use of collaborative knowledge. Contexts were looked at that included employees, licensees, third party use, inter-organizational, and intra-organizational.

Additionally, the rest of this paper uses the term knowledge to refer to knowledge, information, and/or data; and a patent. This is done to simplify the discussion. This is not to imply that patents, data, information, and knowledge are the same but it does recognize that most all knowledge has accompanying information and data that provide context. Interestingly enough current legal definitions do not recognize that knowledge, information, and data often exist together as a single entity although KM researchers and practitioners do recognize the multidimensional nature of these terms.


Intellectual property law features a limited number of devices to support innovation by protecting innovators.

The most common types of intellectual property are trademarks, copyrights, and patents. Trademarks protect only a name or logo of a brand [44]. Copyrights protect creative expressions. This does not include the content, only the specific method in which is was conveyed [44]. The most relevant intellectual property tool to companies is the patent.

Patents protect ideas, and are classified as plant, utility, or design [38]. Plant patents concern innovation in the field of botany [38] where KM technology has little effect. Utility patents cover inventions, whether they are designs, processes, items, compositions, or an improvement of such [38]. The ornamental design of the item is protected by design patents [38].

Patent law is not complementary to collaboration. Current patent law requires all patent owners to join as plaintiffs in order to enforce a collaboratively owned patent [16]. This holds also in the event that once owner is only a licensee [16]. This means that if one owner doesn’t wish to litigate, the patent can’t be enforced.

More troubling is the fact that only one of two co-owners is required to execute a license of patent to another individual [39]. If you have a collaborative patent with another individual, that person has a right to sell that idea to a third party for profit, barring you from any recovery from that third party [39].

If the collaboration is international, the issue must be considered in even more depth before making the decision to collaborate. Despite their flaws, the above U.S. patent laws are more favorable to collaboration than in many countries. While business owners considering an international business relationship should consider problems that could arise from application of international law, international patent issues are beyond the scope of this article.

There are international as well as domestic risks that come with using the cloud for KM systems; many of the aggravating factors stem from weaknesses in the law and regulation of the cloud computing industry.

The largest issue with cloud computing is the ownership of the knowledge stored on the cloud. Many clouds require ownership or a license to the content stored, which gives the operator full access to the knowledge [36]. Gartner has created a Global IT Council that outlines rules for cloud computing [18]. These rights and responsibilities aim for clarification of operator rights over cloud content, existence of service-level agreements, and notification of all relevant jurisdictions [18]. These rights are not enforceable standards, but one company’s guidelines for operating fairly.

Often, the cloud operator is determined to own content created onto the cloud, or be a licensee of the knowledge ([30] or look at Google agreements). If what is on the cloud is a mix of user-owned, and content created on the cloud, the cloud operator is a joint owner [12].

Cloud computing reduces the enforceability of patents [19]. Because the enforceability of a patent relies on the physical location of the infringing party [16, p. 271], use of the patented knowledge or system must be entirely located within the US or it is unenforceable against the infringer [35]. The
borderlessness of the cloud and its knowledge makes international distribution of a method highly likely, thus invalidating many potential claims against misuse of patented knowledge.

When collaborating over a cloud, the evidence of patent or copyright infringement or breach of confidentiality is likely to be done through the cloud, by copying into another cloud or downloading from a cloud [13]. In this case, detection of infringement can also be difficult [22]. Knowledge and processes that infringe or are evidence of an infringement can be located across multiple data/knowledge centers in different jurisdictions [22].

A related issue is determining the applicable law to cloud servers that are located outside the country. This article will not delve into the details of jurisdictional standing, but it is another factor complicating cloud-related intellectual property enforcement.

In the current state of the law, the majority of cloud operators cannot be held accountable for losses resulting from accidental breaches of confidentiality with regard to the content stored on clouds. These breaches do happen [11]. Cloud operators are in a position where they can release themselves from all liability through their user agreement [30]. There is simultaneously a lack of standards requiring a level of protection [49].

4. Alternate Methods of Protection

Despite the weak protection provided for collaborative efforts on the cloud, using cloud KM systems to jointly create knowledge between individuals and organizations is still popular. Some organizations have found alternate means of protecting their intellectual assets in the cloud, but they are less than perfect.

Many companies protect themselves from potential intellectual property concerns through contract [41]. This can quickly become complicated and costly because the contracts made with the cloud services provider and the collaborator require different permissions and restrictions. In addition to the difficulties already inherent constructing a fair contract is the fact that some states, such as California, refuse to enforce non-compete agreements [8]. This allows prior partners and employees that had access to or contributed to the KM to establish competitive businesses, providing contrary incentives to that of KM, which promotes sharing large amounts of knowledge over great distances with many people efficient.

Another method of reducing the risk of intellectual property loss is to limit what kinds of knowledge can be shared over the collaborative cloud KM system. This requires thorough employee training and controls over who can read vs. write certain types of knowledge. This is a very safe way to protect sensitive knowledge from getting abused by a cloud operator or collaborating partner. The major drawback to limiting input onto the KM system is that by limiting what can be shared, the organization is limiting the growth and innovation that make KM and cloud sharing the superior method knowledge development.

Separating the knowledge input into the system by the user is one of the conventional methods to protecting intellectual assets, but is not easily applicable to collaborative cloud KM systems [3]. It essentially involves giving each user only a fraction of the stored protected knowledge, which alone can’t be used in a way that harms the company [3]. This prevents large-scale collaborations, which is an acceptable restriction for companies who have limited goals for external collaboration, or only allow internal collaboration. On the cloud or any computer network, collecting the knowledge and constructing the protected asset from the individual pieces of knowledge is much less difficult, which counteracts any benefits of separation [29].

A similar method that results in a different outcome is separating the knowledge output by user. Software that records each contribution as the product of an identified user solves many problems of ownership, but makes collaboration more difficult [21]. This method also takes planning to implement, because you have to consider who owns the final product [41]. Typically, the owner who wrote the final product has control of it [41]. This slows innovation because it deters sharing that could lead to another partner making the final breakthrough and thus owning the product [41].

Having all collaborative partners own the product, regardless of who finished it, leads to the same problems as discussed earlier with patents, because all parties have equal rights to distribute, even to competitors of the company [2]. Contracting around this future distribution leads to the same difficulties as relying on contracts form the beginning.

Employee education can partially protect company interests by reducing accidental sharing of knowledge [40]. If the employees understand the consequences of giving out knowledge that isn’t in the benefit of the company to share for purposes of collaboration, and are held accountable for what they share, they will be less likely to give up knowledge the company didn’t intend to share [5]. The company must also make sure employees are educated on exactly what knowledge can be shared for collaborative purposes. Employee education does not protect from intentional releases of sensitive knowledge, nor does it keep the collaborative partner from using knowledge the company intended to share in a harmful manner. This method should not be relied on, but should instead be used in conjunction with a more effective method.
Licenses provided by the company to the collaborative partner that allow use of the knowledge for the purpose of the collaboration, and strictly limit other uses can be very effective [20]. This requires ownership of intellectual property such as a patent in order to have something to license [15], and therefore will not work for companies who are interested in collaborating on ideas that will result in a patent, or in ideas not in pursuit of a patent.

The most effective method of protection is to abstain from sharing any sensitive knowledge, and from cloud use and collaboration all together. This will greatly reduce the risk of loss of intellectual assets, at the price of also restricting knowledge growth. You decide the risk you are willing to take on weighed with the potential benefit to the company from collaborative KM on the cloud.

5. The Gap

There is a disconnect between the needs of organizations participating in collaborative KM and the protection by the law. Patent law hasn’t fully evolved to handle multiple owners with different interests. The law governing cloud technology doesn’t account for collaboration, and doesn’t set standards to protect users from cloud operators [23]. Regulation of the internet has grown greatly, but in terms of cloud computing it’s still as it was in the wild west, with cloud operators playing the role of sheriffs who have free reign to set their own rules with little accountability for any repercussions of their actions [31]. These factors make participation in collaborative KM systems on the cloud very risky. The risk-averse nature of companies will prevent them from utilizing the full potential of collaboration over the cloud, thus levels of innovation in the United States will not be able to reach the growth potential [9].

The law allows individual owners of jointly owned intellectual property to act in their best interest, even though their actions may cause harm to other owners [2]. There is no protection of one owner from the other owners [2].

Companies wishing to participate in unrestricted collaboration must forego a level of protection of their intellectual assets [17]. All methods of protection either restrict growth, as is the case for limited sharing, separation of knowledge of users, and assigning ownership of product by contract, or have weaknesses in their construction that could be exploited by their collaborators or other individuals. The latter is a problem when using methods of protection including contract, employee education, and licensing.

Cloud computing, an industry that lacks standards protecting the users, is not yet safe for sensitive knowledge, even with due diligence. Even with proper research to identify or negotiate with a cloud operator with a user agreement that provides adequate protection for the company’s shared content, there is little recourse in the event they utilize a loophole in the contract [22]. Small companies who don’t have the resources to negotiate with big player cloud operators nor to form their own air-tight contracts are left with the bare minimum protection they can create for themselves [6].

The cloud technology benefits from its borderlessness, but intellectual property law is not built to handle issues without clear jurisdictions [34]. The cost benefit of using the services provided by cloud operators who have outsourced servers or processes is one of the main advantages that draw companies towards cloud usage [48]. When technology utilizes physical space in foreign jurisdictions, there is no protection by U.S. law [35]. This leaves many companies who invest in intellectual property protection without recourse even in the event of intentional infringement.

6. Potential Issues

The lack of legal protection of collaborative KM systems utilizing cloud technology can lead to a multitude of conflicts, resulting in costly legal battles that may or may not prove successful. KM systems that involve sharing of knowledge between different organizations are not the only ones at risk; issues can arise from companies using a local KM system as well. Loss of intellectual assets can result from intentional or accidental breaches.

6.1. Intra-Organization

Intentional distribution of knowledge among employees will not protect the company from loss if the employee is an owner of the knowledge [39]. An employee of yours who is an owner of the intellectual asset can sell it to a competing organization [39]. There is no recovery from the employee or the buyer. Also, if there are multiple owners of the knowledge and the organization wishes to bring suit against an infringer, each employee that is an owner must agree to the suit, or the suit will not be allowed to go forward, because all interested parties aren’t represented [16]. When working on projects that have multiple employees contributing, and therefore multiple owners, holdouts can be an issue that will either increase the cost of bringing the suit, or completely bar the suit.

Cloud operators taking ownership of cloud content is also an intentional act that could harm the company. If the operator decides to sell knowledge gathered from documents the organization has created on the cloud,
the company will not be able to recover for damages if it was allowed by the user agreement.

Because cloud operators will contract around liability for accidental loss, even if their contract protects confidentiality of the content, high instances of sub-par security over servers and the network is likely to result in an accidental breach [11]. Accidental breaches have the same consequences of intentional breaches, and should be afforded the same level of preventative measures on behalf of any company providing data/knowledge storage services.

6.2. Inter-Organization

When using a KM system for collaborating with other organizations, or individuals outside the organization, there are risks in addition to the intra-organizational threats. The same problem as when employees are listed as owners arises if multiple organizations are listed as owners, each has the right to sell knowledge created by both to competing organizations [39].

The risk of accidental distribution of sensitive knowledge is higher when collaborating with KM systems. Breaches are more likely to occur when sharing knowledge with additional parties you have no control over. If the collaborating partners have sub-par security, this may allow third parties access to the KM platform containing the shared knowledge. Contracts with other organizations can and should assign liability under these circumstances, or require a level of security of all involved parties.

7. Possible Solutions

How do we fix it? Can we fix it? There are many possible ways to respond to the gap in the law and technology, some more effective than others.

Reforming patent law could protect the collaborative aspect of modern KM systems, and protect the cloud knowledge in some cases as a byproduct. One method is to allow short-term utility model patents, as China does, to allow incremental steps towards the final product to be patented [37] [47]. These are often considered “junk patents” [47], but they could protect collaborators from the cloud providers and from each other during the time leading up to a breakthrough. A second method is to restructure the patent system under the organizational approach [7], which could lead to the same outcomes, theoretically [46].

Alternatively to complete reform, small additions can be made to current patent statutes to protect businesses. These could regulate licensing or sale of patent by one owner when there are other owners who oppose the sale. In the event that only some owners are willing to join as plaintiff, that party can submit written refusal to join and waiver of any potential recovery. Then the party pursuing enforcement can continue with the suit to protect their interests.

To protect companies from the cloud, one method would be to force adoption by cloud operators of the Gartner Rights and Responsibilities for Cloud Computing [18]. The following are the seven rights and responsibilities they suggest:

- “Right to retain ownership, use and control of knowledge
- Right to [service level agreements] that address liabilities, remediation and business outcomes
- Right to notification and choice about changes that affect the service consumer’s business processes
- Right to understand service technical limitations or requirements upfront
- Right to understand legal requirements of jurisdictions where provider operates
- Right to know the security processes the provider follows
- Responsibility to understand and adhere to software license requirements.” (Gartner site)

Using this as a legal standard would standardize many of the contract terms that put cloud users at a disadvantage. The language would need to be revised to reduce any vagueness, so that it is more easily enforceable. User agreements would be similar across the industry which would reduce consumer confusion as well as transaction costs. This would need to be combined with a method to protect from loss due to collaboration.

Similarly, the U.S. government can choose to write their own framework for cloud computing [30] [32]. This would be more costly to the state than applying a privately constructed guideline. To minimize costs, one of these previously proposed standards could be used as a basis, and then expanded on with their own research, as well as call for comments from cloud operators, individuals, and companies utilizing the cloud. This could be started by either Congress and then delegated to the Federal Trade Commission (FTC) and Federal Communications Commission (FCC) [26] [42]. The FTC could use their core privacy principals as a starting point, and then construct the legislation to specifically apply to cloud technology [42]. This method would also need to be used in conjunction with a solution for the risk of collaboration.

The solution providing the lowest cost to the state is to allow private parties to create norms and customs of cloud [10]. This would have the same effect as the
about solutions, which call for enforceable standards, but without the enforceability. Under this approach, uniformity of the user agreements would be minimal, and there would be a period of time before the standards were followed by a majority of providers. After years of use by a majority of providers, it could be used in court as the industry standard, providing evidence of unconscionability. Unconscionability, or unfairness of contract, can be used to void the user agreement with clauses deviating from the industry standard if the user can prove that it was unfair under the specific circumstances [45]. There would be more proof of unfairness needed, but non-adherence to the industry standard can weight the argument in favor of the user. This would not apply well to collaboration agreements because each agreement needs to reflect the needs of the companies, which will vary by case.

International law could be expanded to protect domestic companies from cloud operators, as well as international collaborative partners. There are two methods that best address cloud computing-specific issues: establishment of extraterrestrial jurisdiction and relationships with foreign countries that allow for U.S. patent protection abroad [34]. Extraterrestrial jurisdiction is controversial, but has been exercised by the international court in circumstances not dissimilar to those concerning cloud operators [34].

A less controversial way to expand international protection is to create new relationships with other countries, or allow previous relationships with other countries, to be the foundation for standards regulating all cloud service operations in countries that have entered into this agreement [34]. Organizations like the World Trade Organization or United Nations could propose standards either proposed by a private company and expanded to an international scope, or drafted by an organizational committee. Members of the international organization could agree to be bound by these regulations, expanding the reach of protection from cloud operators but still allowing a level of borderlessness to keep the cost of cloud computing low.

A statute could be put into effect setting restrictions on where cloud operators and servers can be located [10]. The statute would list jurisdictions subject to U.S. patent protection and regulations on cloud operators as valid locations for operation. Ideally, there would be a simultaneous effort to create international relationships that allow U.S. patent law to be enforced in more jurisdictions, so the list of permitted locations would grow. Cloud operators could have the option to establish operations in locations not approved by the statute on the condition they waive their right to challenge exercise of U.S. patent protection on grounds of jurisdictional standing. This will reduce the advantage of the borderlessness, thus reducing flexibility to lower costs [8, p. 151].

8. Recommended Course of Action

The best way to solve such a complex problem is to simultaneously develop multiple methods, so that each weakness in the law is addressed. Supplementing current patent law to be more favorable to collaboration and cloud usage while at the same time fostering international relationships to allow international enforcement of standards regulating the cloud computing industry is the most thorough solution.

More research should be done to determine whether the utility model patents would have a positive effect in the U.S. economy. If the results of that research indicate otherwise, small additions nullifying the current case law on collaborations, and allowing more flexibility in the case of patent joint ownership should be made.

A complete reform of patent law would be controversial, and take a long time to implement. With technology developing at an increasing rate, this prolongs exposure to risk. Expanding on existing patent law reduces the cost of developing an entirely new system and doesn’t put any existing patent protection at risk.

Building off of existing frameworks proposed to regulate cloud providers would cut down on costs to the state for research and development. The other solutions, while plausible, have more drawbacks than this approach. Allowing public norms to establish themselves will take too long, and be a litigious process. Forcing compliance with one company’s proposed standards, like the Gartner Rights and Responsibilities, may not be fair to other providers whose interests may not have been considered in the construction of the guidelines.

These regulations can then be proposed to international organizations for further development, and eventually acceptance. A uniform guideline across borders fosters competition internationally, while protecting cloud users from being taken advantage of. Extraterrestrial jurisdiction is not the best option because it is still rarely applied and seen in a negative light. Courts will be hesitant to further impose on foreign countries, risking the degradation of international relationships, or foreign governments imposing their jurisdiction over domestic companies in return [34].

Until the law has evolved to deal with these issues, companies must take action to protect themselves. Although it is expensive, a company considering participation in a collaborative cloud KM system should hire an attorney to create as favorable a contract with potential collaborators as can be negotiated. The company can retain only cloud service providers that
allow the company to retain ownership and confidentiality of content, and have a high level of system security.

9. Conclusion

The law will eventually evolve to protect companies from the risks posed by use of this new technology, because the law favors innovation. To promote innovation policymakers will need to remove the barriers to participation in collaborative KM. Supplementing current patent law to protect members of a collaborative KM strategy could also protect organizations from cloud providers, but would need to be done in conjunction with jurisdictional limitations allowing enforcement of U.S. patent laws.

Policymakers and large companies need to take steps to facilitate these changes in order to keep up with technology. Large companies are in the position to effect this change, and also to gain the most benefit from regulation over cloud computing as well as collaboration in KM systems. Until these issues have been resolved, the only way to protect yourself is to do your due diligence and not to rely on other organizations or cloud providers to make decisions in your best interest. The law will not protect you if you enter into a legally binding contract and it results in harm. If your organization doesn’t have the time to properly institute these methods of protection, avoid using collaborative KM systems, especially on the cloud.

10. References


