INTRALINKS®

Enterprise. Strength. Collaboration.

Sharing Sensitive Corporate Documents without Compromising Security and Governance

For many companies, such as those in the pharmaceutical, software development or entertainment industries, IP is much more valuable than any physical asset.

As confidence slowly returns to the global economy, mergers and acquisitions, new product launches and initial public offerings (IPOs) are just beginning to rebound. This is no return to business practices as they were a decade ago; it is clear that companies are operating in a continuously changing landscape that requires new levels of agility and adaption in order to remain competitive.

Many companies are responding to the need for increased business agility by communicating and collaborating more closely with networks of external business partners to accelerate and innovate across the full spectrum of enterprise business processes, from product design to legal, financial and operational activities. While this approach enables companies to shorten product life cycles and enhance innovation, it also creates longer and more complex supply chains — which introduce many more points of additional risk where sensitive information may be compromised.

For example, collaboration in this real-time economy means companies are sharing their intellectual property (IP) across borders and under demanding time constraints in order to innovate and bring to market the stream of new products and services their markets and customers demand. This creates unique organizational challenges in terms of protecting precious corporate IP and managing corporate risk, and doing so in many different jurisdictions simultaneously.

The role of the GC in protecting corporate IP in the new global economy

It is often the role of the General Counsel to take the lead in setting policies and guidelines to assure that company IP is adequately protected — a role that is central to company success. For many companies, such as those in the pharmaceutical, software development or entertainment industries, IP is much more valuable than any physical asset.

Yet the growing levels of inter-enterprise collaboration described above increasingly threaten control over IP — a challenge that is exacerbated by the growing mix of multi-jurisdictional regulatory requirements. But losing control over IP can be a very expensive mistake and can even threaten a company's existence.

Many companies, however, have loosely defined or overly broad IP protection policies in place. Employees are not versed in these policies, and at the same time, they are under pressure to do what it takes to get work done quickly. The result is a range of practices and ad hoc systems to support collaboration with outside partners. Few if any of these systems are robust enough to meet the full range of needs.

Typically, ad hoc systems that companies have evolved use components such as e-mail, FedEx and other courier delivery methods, and software such as Google Docs and other freely available or low cost document-sharing systems that people can access on the fly and put to use for their immediate needs. These practices inevitably lead to loss of control over company IP. When conflicts arise, they do not provide the clear audit trails and documentation needed to stand up in legal proceedings.

As a result, GCs are faced with the need to establish a "highest common denominator" — i.e., setting standards that are equal to or higher than the most demanding standards their company is likely to encounter — to guide their companies and manage the risk appropriately. This paper explores some of those risks and best practices in managing them.

GCs are faced with the need to establish a "highest common denominator"— i.e., setting standards that are equal to or higher than the most demanding standards their company is likely to encounter — to guide their companies and manage the risk appropriately.

Balancing the need to collaborate with the imperative to maintain control

Richard Foster, author of *Innovation: The Attacker's Advantage*, states that, "To survive and thrive business leaders must create, operate and trade without losing control."[1] His research indicates one of the biggest challenges companies face is balancing the need to collaborate with a wider network of external partners while still maintaining control over their valuable business assets.[2] In particular, maintaining control of intangible assets and IP is key to success over the longer term.

According to the World Intellectual Property Organization, IP is defined as "creations of the mind," and includes, inventions, literary and artistic works, symbols, names, trademarks, images and designs used in commerce.[3] Given the frequency and intensity of collaborative projects that companies are engaged in and given the global nature of those collaborations, there are different bodies of regulations governing IP, privacy, and related issues that need to be addressed.

Among the most stringent bodies of regulations are the Sarbanes-Oxley Act, the Dodd-Frank Wall Street Reform and Consumer Protection Act and NAFTA IP laws in North America, and European Union regulations and IP laws for Europe. The European Commission states on their website under Trade Topics that "IP rights are becoming increasingly important for European inventors, creators and businesses."[4] The European Commission makes it clear they intend to see that other countries respect EU standards for IP. And compliance with Dodd-Frank is virtually impossible without strong information governance practices that document all appropriate communications.

Current practices in corporate IP protection

At present the most comprehensive global standards regarding the protection of IP are those maintained by the World Trade Organization (WTO) and known as the Trade-Related Aspects of Intellectual Property Rights or TRIPS regulations.[5] All member countries of the WTO are signatories to these regulations but many of those countries lack corresponding national laws to fully implement TRIPS. But the parties to individual projects that involve sharing of IP must still enforce these regulations.

[1] Richard Foster, *Innovation: The Attacker's Advantage* (Manila: Summit Books, 1988)

[2] *Creative Destruction Whips through Corporate America*, Innosight, Winter 2012 **http://www.innosight.com/innovation-resources/strategy-innovation/upload/creative-destruction-whips-through-corporate-america_final2012.pdf**

[3] World Intellectual Property Organization, **http://www.wipo.int/portal/index.html.en**

[4] European Commission, Trade Topics — Intellectual Property website - **http://ec.europa.eu/trade/creating-opportunities/trade-topics/intellectual-property/**

[5] World Trade Organization TRIPS website - **http://www.wto.org/english/tratop_e/trips_e/intel2_e.htm**

Clearly, an inter-enterprise content and collaboration platform that provides security, compliance, and precise information governance could supply complete and auditable documentation – and thereby play a decisive role in these high-stakes legal battles.

A current case in point is the case now being litigated between Apple and Proview Electronics, a Chinese company that claims ownership of the iPad trademark in China. Trademark lawyer and patent attorney Michael Cohen explains, "the chain of events is not clear, but the core dispute is whether Apple ever obtained proper license or acquired use of the iPad trademark in China from the correct owner."[6] When this dispute began Apple was barred from using the iPad trademark in only a few provinces, but recently the ban has spread more widely in China and in some cities iPads are even being confiscated by local authorities.

Moreover, this is just one of dozens of IP lawsuits surrounding smartphones and tablet computers and involving companies such as Apple, Google, HTC, Microsoft, Motorola Mobility, Nokia, Research in Motion and Samsung Electronics.[7] The stakes are high enough that several of these companies have been motivated to make multi-billion-dollar acquisitions to obtain necessary patent rights.

As the Apple-Proview litigation winds its way through the Chinese legal system it will become critical for the contending parties to produce dated documents and detailed and verifiable audit reports showing exactly when certain actions were taken, who made what offers and when different parties purchased what rights. There will doubtless be conflicting claims, and the viability of those claims will depend in large part on the completeness and veracity of the relevant documentation that each side can produce.

Clearly, an inter-enterprise content and collaboration platform that provides security, compliance, and precise information governance could supply just such complete and auditable documentation — and thereby play a decisive role in these high-stakes legal battles.

Systems and technology for protecting intellectual property

Over the last decade, a host of new technologies for inter-enterprise collaboration have emerged. Most do not possess the enterprise-grade information security, compliance and governance characteristics that are requisite for large corporations. A few, however, predate the current "bring your own device" (BYOD) fad, and are mature and available to meet company needs to respond to fast-paced business collaboration needs while maintaining proper controls over company IP. Given this dichotomy, as General Counsels search for the right secure document-sharing solution to protect their enterprise IP, there are several requirements and differentiating system characteristics that require careful consideration and analysis.

The first characteristic to consider is that the system must enable external collaboration partners to easily access permitted documents from any location with an Internet connection. And they should be able to use anything from a desktop PC or laptop to a consumer IT device like an iPhone or iPad. Because the number of users in collaboration projects will grow or shrink unpredictably, such a system should be deployed on a software-as-a-service (SaaS) basis to reduce up-front cost and enable a pay-as-you-go model proportional to the number of partners using it in any given month. This gives them the best control over operating expenses.

In addition, the system should leverage investments in internal document sharing systems your company may already have made. Microsoft SharePoint, for example, is widely used within companies for this purpose and can be extended by third parties to provide the needed information governance practices. Such a system must connect with the enterprise's internal document sharing system and enable external partners to retrieve and view documents that they have permission to see.

[6] Los Angeles Trademark Lawyer and Patent Attorney Michael Cohen, *Trademark Blog of the Trademark Lawyer's Mind*, **http://patentlawip.blogspot.com/2012/02/proview-trademark-litigation-with-apple.html**

[7] *Justice Department Poised to Clear Google-Motorola Deal* - WSJ.com, February 9, 2012 Available at **http://online.wsj.com/article/SB10001424052970203315804577211603523857404.html**

To ensure that your inter-enterprise collaboration tool is secure, you should select a provider that has intensive security measures in place. Ideally, the provider should allow on-site inspection, SOC 2 compliance, and ISO 9000 certification.

The system should enable a granular level of control over all the material your company shares, including moment-to-moment management of who can access what, and what they can do with it — whether they can just view a document online or if they can also download the document. If you do let someone download a document, the system should automatically watermark the document with the name of the person doing the download. So if that person leaks or loses the document, their name is literally all over it.

The system should encrypt documents as they leave your company and they should remain encrypted when they are in transit over the Internet and when they are at rest in databases that reside outside your company's data center.

To ensure that your inter-enterprise collaboration tool is secure, you should select a provider that has intensive security measures in place.

Auditable document-sharing helps support risk readiness

Don't be dependent on a single person to manage the document sharing process — use a system that records data and automatically enforces rules. A good IP protection system enables you to set up a solution that collaboration partners can access from anywhere with any kind of device from a PC to a smartphone. The platform enables you to control and monitor who sees and downloads what documents. Share documents in a secure and auditable environment right from the start because that is the best way to respond to the unpredictable business environments that are now the norm.

Good solutions will also provide a high degree of transparency into who looks at what documents and for how long. And the system will automatically record this information for all the documents and all the people using the system. This transparency provides a complete and detailed audit trail, should the need arise.

A common issue that companies must be prepared for when they share their IP with outside entities such as contract manufacturers is the counterfeiting of goods and services. Suppose a large global company found that a small local manufacturer was making use of its IP without a proper license, and this local manufacturer was producing low quality products that hurt the market reputation of legitimate products the global company produced and sold. The global company has two options. The global company would need to either negotiate a licensing and OEM agreement with the local manufacturer that provided royalties and addressed the product quality problems, or it would need to initiate litigation, which could become a long and expensive process.

Avoiding litigation and reaching a successful negotiated resolution to a case like this one depends on the global company having secure control of its IP and the ability to produce detailed audit reports showing what IP was shared with whom, at what times, and for what purposes. With verifiable information like this, negotiated settlements are likely in most cases. In the absence of such information, litigation may be the only course.

Modern IP security and compliance policies

It's estimated that intellectual property theft costs U.S. companies about $300 billion every year.[8] To prevent that theft, companies need more than highest-common-denominator inter-enterprise content and collaboration platform. They also need new policies and procedures and they need to educate their employees in the use of all three — the collaboration platform, the policies and the procedures.

[8] Derek Slater, *Intellectual Property Protection: The Basics*, CSO Magazine, February 14, 2011, **http://www.csoonline.com/article/204600/intellectual-property-protection-the-basics**

Companies should determine what categories of information would hurt them the most if it were lost, and consider which categories of IP are most at risk of being stolen. This analysis should help companies see where they need to focus most of their efforts and money.

Review existing IP policies and update them frequently. Define the guidelines clearly and give examples for how to identify and respond to specific types of situations and business collaboration requirements. Begin by categorizing IP and making sure the company has an up-to-date accounting of its IP in each category. Detail the different protection needs for each IP category.

Companies should determine what categories of information would hurt them the most if it were lost, and consider which categories of IP are most at risk of being stolen. This analysis should help companies see where they need to focus most of their efforts and money.

The Michigan Bar Journal (MBJ) has published a "short list" of best practices for protecting IP,[9] highlighting the main features of a good IP security and compliance policy.

The list starts with the need to educate both management and employees. Everyone in the company should have a basic understanding of trademarks, copyrights, patents and trade secrets. MBJ says people are often the weak link in any security system and IP protection that counts only technology without including people is likely to fail. In addition to training, employee background checks should be done on the people who will be handling the most sensitive data, both at your company and at your business partners.

Once companies have identified and categorized their IP, they should label that IP on everything from paper documents to web screens for material online, according to MBJ. They should make sure that people gaining access to this material know it is confidential information. A set of procedures and practices regarding the handling of each category of IP should be created and distributed to all for whom it is appropriate. Included in this should be a set of standardized agreements signed by employees and business partners that specify what their obligations are with respect to company IP.

Companies should partner with experienced outside counsel if they do not have lawyers in-house who are experienced in IP law, MBJ recommends. Cost effective enforcement measures should be put in place with a focus on the most critical IP and the IP most likely to be stolen. Companies should also remember to tailor their policies and enforcement measures as needed to address the IP laws of all the different countries where they do business.

Conclusion — Business is about preparing for and responding to opportunities

The 2011 Corruption Perceptions Index, which ranks all the countries of the world by their perceived levels of corruption in government, is an interesting barometer to drive home the paradox of IP protection in the global economy. Popular destinations for outsourcing and contract manufacturing in Asia and South America are ranked as having high levels of corruption in government, which typically also merge into those countries' business practices.[10]

Yet these are often the same countries whose emerging economies offer significant business opportunity for global corporations — and the same countries, therefore, where many collaborative business partners will be located. It is the job of the general counsel to prepare the company to handle the security, compliance and information governance problems that may arise in pursuit of those business opportunities. A General Counsel's choices can both enhance the enterprise's ability to quickly respond to new opportunities and also strengthen its ability to protect and manage its intellectual property.

An appropriate IP security system, built on a strong inter-enterprise document-sharing foundation and backed up by highest-common-denominator policies and procedures, will enable an enterprise to be both agile and compliant — deal ready and risk ready. That is the best way to succeed in the real-time global economy.

[9] Barbara LaSusa, Lawrence LaSousa, *Intellectual Property 'Best Practice' Tips for Small Law Departments*, Michigan Bar Journal, January 2007, **http://www.michbar.org/journal/pdf/pdf4article1105.pdf**

[10] *Transparency International, Corruption Perceptions Index 2011*, **http://cpi.transparency.org/cpi2011/**

INTRALINKS®

Enterprise. Strength. Collaboration.

IntraLinks is a leading global provider of Software-as-a-Service solutions for securely managing content, exchanging critical business information and collaborating within and among organizations. More than 1 million professionals in industries including financial services, pharmaceutical, biotechnology, consumer, energy, industrial, legal, insurance, real estate and technology, as well as government agencies, have utilized IntraLinks' easy-to-use, cloud-based solutions. IntraLinks users can accelerate information-intensive business processes and workflows, meet regulatory and risk management requirements and collaborate with customers, partners and counterparties in a secure, auditable and compliant manner. Professionals at more than 800 of the Fortune 1000 companies have used IntraLinks' solutions. For more information, visit **www.intralinks.com** or **blog.intralinks.com**. You can also follow IntraLinks on Twitter at **www.twitter.com/intralinks** and Facebook at **www.facebook.com/IntraLinks**.

AMERICAS
1 866 INTRALINKS
info@intralinks.com

EUROPE, MIDDLE EAST & AFRICA
+ 44 (0) 20 7549 5200

ASIA PACIFIC
+ 65 6232 2040

LATIN AMERICA
+ 55 0800 892 2247

Terms of use

IL-WP-SHARING-120229