



Protecting Intellectual Property During the

What are the problems relating to IP protection? Here's an approach to solve some of these challenges, using a comprehensive program process alongside technology.

BY JEFF C. PARMET, ALEX ROSENBAUM, AND JAMES N. RYAN

As markets become increasingly knowledge-driven, the generation and protection of intellectual property has moved from its role as a secondary commercial activity to the “business critical” status. Many of the world’s largest and most successful companies consider intellectual property (IP) to be their foundation for market dominance and a key success factor in continuing their profitability.

Because enterprises understand the value of IP, they have embraced

the idea of its generation. According to the U.S. Patent and Trademark Office, there were 183,975 patents granted in 2001, as compared to 99,077 in 1990.

Enterprises are also realizing that the task of protecting IP is not trivial. They are moving away from dealing with matters on an isolated case-by-case basis, embracing instead the idea of a comprehensive, enterprisewide IP protection management program.

This article introduces the reader to the problems related to IP protection, offers an approach toward developing an effective IP protection methodology, and describes how and where technology fits into the overall solution. The task of developing a comprehensive IP protection management program consists of four main components:

- Identification of IP;



Internet Age

The authors are represented by the Carrera Agency, a talent management agency serving the information technology marketplace.

About the Authors

JEFF C. PARMET is a partner at Pricewaterhouse Coopers, in Washington, D.C. He has more than 30 years of IT experience, with an emphasis on computer system development and integration (including the utilization of computer forensics to analyze evidence in complex disputes and investigations). He has served as a consultant and testified as an expert on cases involving disputes over rights related to computer software and Internet domain names.

ALEX ROSENBAUM is currently designing a citywide enterprise information security architecture, which ensures standard security posture across a major municipality's government agencies. Previously, he served as chief solutions architect for the system design to secure communications between all government offices and the Department of Homeland Security. He has more than 15 years experience in the IT field.

JAMES N. RYAN began his solutions architect career with a mission-critical system for the Nation's Reconnaissance Office (NRO) that enabled IP-based communications among networks—certified at three separate levels of security. Most recently, his ten-year career in IT solution design-and-implementation includes architecting solutions for homeland security (to enable information-sharing among agencies) and for e-government. Send comments on this article to cm@ncmahq.org.

Legal Concept	IP Description	Specific Examples
Trademark	Logo designs, slogans, characteristics that identify products and services, packaging and advertising materials, and building designs.	General Electric company logo, the slogan "We bring good things to life," the Michelin Tire Man character, or the design of a McDonald's restaurant.
Trade Secret	Any confidential company information that gives the company a competitive advantage.	Patentable technology for which a patent has not yet been filed—a customer list, network usage, and traffic patterns for an Internet service provider.
Patent	Technological inventions, processes, methods, and substances. Should involve something beyond the everyday skill of an ordinary person, contain an inventive step, and not be an obvious solution to a problem.	Intermittent windshield wipers or digital video disks (DVDs).
Copyright	Printed and electronic media, such as books, music, art, photography, film, or choreography. Computer programs or architectural designs.	<i>Star Wars</i> books and movies, Microsoft Office programs, or Ansel Adams' "Moonrise over Hernandez" photograph.

Table 1

- Protection of IP from a legal perspective;
- Implementation of specific anti-theft controls; and
- Development and implementation of a response strategy.

Identification of IP

The process of evaluating an organization's intangible assets with the purpose of identifying IP is referred to as an IP audit. Companies undertake IP audits for different reasons. Often, these audits are used as valuation tools in order to assign a dollar value to intangible assets—for example, as part of pre-acquisition due diligence. Similarly, a venture capital firm may request an IP audit from a company in which the firm is considering investment. Another reason for a company to conduct an IP audit is to find material that the company is using without an express license. This may include unlicensed or under-licensed software, mailing lists, and employee and client data.

With respect to IP protection, however, the primary purpose for an IP audit is to identify those information assets created or owned by the company itself. These are assets that

the company would like either to keep out of the competitors' hands completely or to ensure that the company is properly compensated for usage. The examples of such assets may include proprietary software code and algorithms, technological designs, manufacturing processes, electronic books, recorded music, and company brands and logos.

Legal Protection

Once the intellectual property has been identified, the next step is to ensure that it is protected by law, if possible. **Table 1** presents a summary of different legal concepts in the IP realm.

Intellectual property law is complex—there are many exceptions to established rules and regulations. This is especially true in the case of international intellectual property law. When developing their IP protection program, companies are advised to engage a reputable law firm specializing in intellectual property.

Anti-theft Controls

Although there are many different types of IP, when discussing theft prevention it is helpful to group IP into two categories, as described in **Table 2**.

Internal IP

With internal IP, the main concern is to keep it from "exiting" the company. When it comes to external IP, the focus is different. In the external case, the main objective is to detect and shut down unauthorized distribution channels, as well as to detect and prevent the unauthorized usage of the assets.

Often, when organizations first try to tackle the problem of leakage of internal IP, their thoughts turn immediately to technology. Unfortunately, a comprehensive technological solution to this problem does not exist. Within a typical commercial organization, there are simply too many routes by which internal IP can exit.

Point solutions, however, do exist. They include tools that can scan electronic mail for IP-related content or analyze data that passes through the company network or the Internet connection, looking for patterns that may reveal IP leakage. Electronic mail, corporate networks, and the Internet are the most obvious exit points. The number one exit route, however, is not theft through the network, but simply copying IP onto a diskette and walking out the door with it. Sales associates, for example,

IP Category	Description
Internal IP	This type is what a company uses internally, to gain competitive advantage. As far as the company is concerned, its competition should never have access to this type of IP. This type generally falls into the trade secret category. It includes customer lists, internally developed market data, proprietary manufacturing processes, and unique business development techniques.
External IP	This type is either used for advertising, marketing, or promotional purposes, or it is inherent in company's products or services. It may include assets that are trademarked, patented, or copyrighted. As mentioned above, examples include company logos, slogans, and jingles. Digitally recorded music, movies, and electronic books also can be included in this category. Commercially available software—such as Microsoft Windows or Adobe Photoshop—is another example.

Table 2

will most likely have access to customer databases. These databases usually include customer contact data, lists of products and services sold to these customers, notes about subjects that a particular customer is interested in, or notes about business initiatives taking place at customer or client companies. Since the sales associates are often on the road, they may have copies of the entire database installed on their laptop computers or on CD-ROM. Often, the turnover rate among the sales team is fairly high. When sales associates leave the company, they can take customer data. They may also share this data with friends, some of whom may work for or have contacts with competitors.

Another example of an IP exit point is software developers, who often work from home or telecommute. They could potentially have access to source code of a company software application. These developers may have a copy of this source on a personal computer at home. This computer is outside of the company's administrative control, and the environment at the developer's home is most likely less secure than the office one. This situation can lead to the source code in question falling into the "wrong hands" or appearing on the Internet.

What about an engineer, who is the lead designer for a company's flagship product? This person may accept an offer from another company, possibly a competitor. It may not be the

engineer's intention to disclose any trade secrets; however, it is very likely that this person will use experience gained at his or her previous job for new tasks. Thus, the competitor's product or service will wind up being developed using IP of another company, although indirectly.

The Government Approach

Government organizations are very familiar with the problem of information leakage. In order to prevent state secrets from leaking to foreign governments, federal government agencies implement complex, multi-level security controls. In addition, there are export control laws carrying severe criminal penalties for those taking information deemed critical to national security to a foreign country.

Government agencies limit access to sensitive information only to those individuals that absolutely require such access. They also classify information by level of sensitivity, and allow access only to those individuals with the proper level of clearance.

When considering an individual for a high level of clearance, government agencies conduct an investigation into the individual's background. They look at the individual's work and personal habits, interview friends, relatives, neighbors and past employers, and check for existing criminal records; often, the individual will take a lie detector examination.

Sometimes, these investigations take 8 to 12 months to complete and

are very expensive. Government organizations, however, have huge security budgets, and they spend hundreds of millions of dollars, attempting to keep sensitive information secret. Yet, even with these elaborate controls in place, leaks still occur.

The Commercial Approach

Most commercial organizations, especially small- and medium-sized ones, simply cannot afford to expend this much effort on curbing leakage of internal IP. They often find that the leakage risks simply do not justify the investment. Also, they find that taking a government-like approach to such protection would impose too rigid a structure on their normal everyday business activities. The flexibility they require in order to stay competitive would disappear.

Rather than relying on technology for controlling internal IP leakage, commercial organizations are better off taking an administrative approach. This approach consists of three major parts: regulation, employee awareness, and enforcement.

- (1) **Regulation**—Companies must ensure that the corporate policy clearly identifies what the company considers to be IP, and that the policy clearly explains what the penalties for disclosure to unauthorized parties are. The policy should be quite specific and provide examples of IP, as well as example scenarios that describe

how unauthorized or accidental disclosure can happen. This policy should be reviewed on a periodic basis to ensure that it covers any new internal IP.

(2) **Employee Awareness**—Companies must ensure that the policy is communicated to all employees. Every employee should sign a document acknowledging his or her understanding of the policy and the consequences of violations. New employees should sign this document as part of the hiring process, and existing employees' personnel records should be evaluated to ensure that they have signed the document. It is also appropriate to conduct training sessions that focus on internal IP as part of orientation for new employees and periodic refresher sessions for existing employees.

Companies should also conduct exit interviews for employees, who leave the business. During this interview, these employees should be reminded of their internal IP obligations. The employees should sign a document reaffirming the confidentiality. The company should retain a copy of the signed document for future reference, since it can serve as evidence, if required.

(3) **Enforcement**—When someone is caught intentionally or accidentally leaking information, companies should take immediate disciplinary action, as specified by the policy, with no exceptions. Companies should also ensure that the news of the incident and action taken is communicated to all the employees. This will let everyone know that the company is serious, when it comes to protecting its IP.

External IP

As mentioned earlier, external intellectual property most often includes assets that revolve around a company's products and services. Companies

rely on these assets for direct revenue generation. Everyone, including the competition, can readily gain access to these assets simply by buying the product or service. Thus, in this case, the problem is not preventing the IP from leaving the company, but rather preventing unauthorized (free-of-charge) use and redistribution of the assets. The approach to tackling this problem consists of two parts: (1) detection of unauthorized usage and distribution of external IP assets, and (2) the elimination of this activity.

Detection of Unauthorized Sources

Prior to the existence of the Internet, this problem was more manageable. Currently, however, millions of computers are connected to the Internet. Services, such as file transfer protocol (FTP) the World Wide Web, and different search engines—make it easy to find and download electronic media. We have peer-to-peer services, such as KaZaA, which allow millions of individuals to share files anonymously and in a completely unregulated way. The Internet makes the task of searching out unauthorized external IP distribution sources extremely labor-intensive.

Many organizations find it expensive to handle this problem

themselves, and thus turn to third parties for help. These third parties are companies that provide services for monitoring on-line content. One such company is Cyveillance, Inc., based in Arlington, Virginia. Cyveillance has developed proprietary extraction agents to comprehensively monitor on-line content.

Working 24-7, these automated agents gather intelligence from a diverse set of on-line sources and protocols, including

- The World Wide Web (HTTP);
- Usenet (NNTP);
- FTP sites;
- Message boards;
- Internet Relay Chat (IRC);
- E-mail distribution groups and spam;
- Auction sites; and
- Peer-to-peer networks, such as KaZaA, Netscape's FastTrack Server, Gnutella, and other popular networks.

These automated agents locate products sold by unauthorized parties



ASSOCIATES®

**Your Proven Partner
In Contracts &
Procurement Staffing**

301-770-0090 1-800-844-0090
www.xlanow.com

Serving Our Clients & Community Since 1989

11140 Rockville Pike, Suite 350, Rockville, MD 20852

(or in non-standard forms), by constantly monitoring on-line auctions and e-commerce site catalogs. Through quick identification, companies can rapidly address these Internet sales and protect their revenue and reputation.

Elimination of Unauthorized Usage and Distribution

“Cease-and-desist letters” are usually effective ways to stop infringers from posting, selling, or giving away copyrighted, trademarked, or patented materials on the Internet. Most often, an infringer wants to avoid legal action and the potentially significant damages. In those cases where infringers ignore legitimate demands to cease such activities, litigation usually follows.

In May 2003, reports that ran in the *Wall Street Journal* indicate that four college students agreed to pay between \$12,000 and \$17,500 to the music industry to settle lawsuits for running file-sharing services that the industry claimed were allowing users to swap songs in violation of copyright laws.¹ The recording industry is losing millions of dollars to free-file swapping services and has recently become much more aggressive in enforcing its intellectual property rights. The industry isn't stopping at targeting the purveyors of file-swapping services. The industry now has its sights set on students, who merely share their music libraries with other individuals.

Recently, a court in the District of Columbia ordered Verizon Internet Services, Inc., to provide the names and addresses of customers the music industry has identified as “possible song swappers.” One of the biggest challenges is that most people do not believe they are doing anything wrong by sharing their electronic music libraries with others who share theirs.

The Recording Industry Association of America (RIAA), however, believes differently. Matthew J. Oppenheim, the RIAA's senior vice president for business and legal affairs, said in a prepared statement, “The message is clearly getting through that distributing copyrighted works without permis-

sion is illegal, can have consequences, and that we will move quickly and aggressively to enforce our rights.”² Time will tell if the RIAA's aggressive tactics prove to be effective.

A Case Study: AP and Cyveillance

The Associated Press (AP) operates as a not-for-profit cooperative and is dedicated to creating value for its subscribing member organizations. AP's mission is to provide accurate, balanced, and informed news for media use around the world. The cooperative distributes news, photos, graphics, audio, and video through 5,000 radio and television stations and 1,700 newspapers in the United States alone—reaching more than 1 billion people every day. The firm's services also extend to 121 countries, supplying factual coverage to approximately 8,500 international newspaper, radio, and television subscribers.

The Challenge

Tempted by the unregulated nature of the Internet, many Web site developers have realized that they can improve the profitability of their sites by poaching the content that AP generates for its members. These copyright violators plead ignorance of the law, but even the case of true ignorance is certainly no defense. Clearly, the use of content without an appropriate license is tantamount to stealing and thus carries serious penalties.

Several years ago, AP determined that it could not rely on the government to identify content poachers, monitor them, or demand cessation of their illegal activities. AP found that site developers had begun to thief content aggressively, entirely unfazed by the threat of legal sanctions. To make matters worse, it was clear that the effort required to manually monitor these rogue sites would be Herculean—a Google search for the term “AP” can yield more than 10 million results, and a significant portion of the poached data is not even attributed to AP.

The Solution

In March 2000, AP recognized that the risks of inaction were too catastrophic to ignore. AP hired Cyveillance, and its strategists worked with AP representatives to identify the leading Internet-oriented risks to their franchise. These strategists targeted the largest risk—sites that pirated AP's intellectual property.

Since that point of identification, Cyveillance's brand protection service has regularly provided AP with detailed information on poaching instances, through an interactive system that also allows AP to track improvement against its performance metrics. AP has then sent “cease-and-desist letters” to approximately 95 percent of the unauthorized sites that either display AP articles or graphics for commercial purposes, or associate the AP name or logo with inappropriate content, such as pornographic or racist material.

Over the years, Cyveillance and AP have worked together in this search, aiming to ensure that the system is calibrated to identify the most critical transgressions. Cyveillance has taken responsibility for the analysis of all the results, measured the impact of content theft in top-line dollars, and recommended process refinements, as appropriate.

The Results

Over a three-year period, AP used Cyveillance data to track down 963 sites that misused its content. By converting a portion of these sites into customers, it took only an estimated six quarters to achieve payback on their investment. This hard-dollar payback was only the tip of the iceberg, however. To AP, the lion's share of value was generated by using Cyveillance data to protect the ongoing value of its exclusive content. The results outlined below demonstrate the magnitude of the benefits that AP has realized by working with Cyveillance.

On the new revenue side, specific data regarding client conversion rates and contract values is difficult to obtain.³ Cyveillance worked with AP to

develop some very rough but conservative estimates. Assuming a 10 percent conversion rate and contract value at 25 percent below the average deal size, the estimated payback of AP's initial investment exceeds 100 percent within six quarters. Factoring in only the value of this incremental revenue, the three-year return on investment (ROI) of the project was 49 percent, and the 5-year ROI was 77 percent.⁴

AP views this new revenue stream, however, as incidental, when compared to the value of protecting its pre-existing revenue stream. AP found that cease-and-desist efforts were highly effective, succeeding approximately 92 percent of the time. Of course, it's difficult to quantify the benefits associated with efforts to prevent poachers from accessing content that was developed for AP members. Still, we can get a sense for the value by considering that the project's ROI would increase beyond 1,600 percent, even if monitoring efforts were merely to prevent 1 percent deterioration in global revenues.

Conclusion

The task of developing a comprehensive, enterprisewide intellectual property protection program is a complex one. At first, it may seem overwhelming and intimidating. The key is to divide the effort into manageable components, as described above, and then to focus on the process rather than the technology.

A single technological solution to the entire problem does not exist. Companies that turn to technology before establishing a process run the risk of falling victim to one of two outcomes.


First, they may successfully implement a point solution to protect one particular type of IP, or to block one particular exit point. This may give them a false sense of security. Based on the technology vendor's claim, companies may think the IP is protected, while, in fact, leaks and unauthorized usage still occur. The second outcome is even worse: a company invests in the technology, but, in the absence of an overall IP

protection plan or process, the technology "sits on a shelf" indefinitely.

Both of these outcomes result in little or no ROI and little or no progress toward IP protection. The solution is to first formulate a plan, and then to develop a process. It then makes sense to consider technological solutions for labor-intensive or repetitive portions of the process. *CM*

Endnotes

1. *Wall Street Journal*, May 2003.
2. Associated Press.
3. AP's unique, highly decentralized, global accounting system makes it extraordinarily challenging to extract precise data in these areas.
4. The ROI for each of the time periods is calculated in the following formula: (Present value of benefits – Present value of costs) / (Present value of costs).




Certificate in

Procurement & Contracts Management

Fall 2003 Online Courses

- [Introduction to Contract Law](#)
- [Introduction to Contract Management](#)
- [Introduction to Procurement](#)
- [Introduction to Contract Administration](#)
- [Introduction to Contract Dispute Resolution](#)
- [Introduction to Contract Risk Management](#)
- [Introduction to Contract Law](#)
- [Introduction to Contract Management](#)
- [Introduction to Procurement](#)
- [Introduction to Contract Administration](#)
- [Introduction to Contract Dispute Resolution](#)
- [Introduction to Contract Risk Management](#)


UNIVERSITY OF VIRGINIA
 School of Business and Economics
 Charlottesville, VA 22904-4138
 Phone: 800.924.6463