

5 Simple Steps Startups Can Take to Protect Intellectual Property

All emerging companies can and should take basic steps to protect their uniquely valuable intellectual property.

For many companies, especially startups, intellectual property often represents an important component of a company's value, perhaps the single most significant component. Investors and acquirors are often interested in such companies primarily for the potential embodied in their IP. Defects and deficiencies in a company's IP portfolio can raise significant concerns for investors and acquirors, and in extreme cases may drive them away entirely. Yet, despite the apparent centrality of IP to a company's value and potential, many companies fail to take basic steps to preserve such important assets. This article will describe a few basic steps in five key areas that any company can take to protect, preserve and enhance its IP.

1. IP Assignment and Nondisclosure Agreements

One of the simplest steps any company can take to secure its IP is to require all founders, employees, and other third-party service providers to enter into IP assignment and nondisclosure agreements. These agreements are short, straightforward and usually contain standard terms. Accordingly, most parties readily understand such agreements, so they should not result in substantial delays or increases in transaction cost. Despite their ease of use and general accessibility, many companies fail to obtain these agreements, often simply through lack of vigilance. Failure to obtain these agreements can result in the company not owning, not owning exclusively, or otherwise lacking rights to key portions of the IP required to drive its business. In certain cases, such omissions can derail financing or commercial transactions and even threaten the company's ongoing viability.

IP assignment obligations should provide that all IP that a person has created or may create in connection with the services provided to the company and/or derived from the company's proprietary information shall be the property of the company. However, certain states (including California) restrict the scope of what works can be assigned to the company by an employee. Companies should work with counsel to ensure that their assignment agreements comply with applicable state laws regarding the ownership of IP created by employees.

The agreement should also include affirmative current assignment language (e.g., "so and so hereby assigns to the company..."), as opposed to simply stating that the company shall own any IP created during the course of the services, to ensure that all intellectual property rights are effectively assigned under the agreement and that the company will not have to obtain another assignment to secure ownership of IP created after the agreement is signed. Founder IP assignments should be executed at

the time the company is formed and should also cover any IP the founder has previously created that relates to the company's business (if the intent is to use such IP in the company's business).

Companies should also obtain standard nondisclosure agreements from all parties who may have access to any of the company's confidential or proprietary information, including all founders and employees. These nondisclosure agreements should contain both restrictions on disclosure of the company's confidential information and also prohibitions on the third party's use of the company's confidential information for any purpose other than as contemplated in the nondisclosure agreement.

Companies should enter into IP assignment and nondisclosure obligations at, or prior to, the time a given third party commences providing services to, begins employment with, and/or first receives confidential information from the company. Although such agreements can sometimes be effective retroactively, in other cases they may not. In certain states, the promise of future employment may be insufficient consideration to support the assignment by an employee of an invention that was created prior to the signing of the IP assignment agreement, and additional consideration would have to be paid to the employee to effect the IP assignment. Even where retroactive assignments are enforceable, the third party may simply not be willing to sign the agreement, or may attempt to extract a price from the company in exchange for executing the agreement. Such actions are especially likely if relations with an employee or other third party have become strained or if an investor or acquiror has required such an agreement as a condition to closing a transaction. To help avoid these issues, companies should establish simple, quick, and clear protocols that provide employees who deal with commercial counterparties access to company officers who understand and have authority to negotiate and sign such agreements.

2. IP Prosecution and Registration

At inception, each company should develop a plan for evaluating at various stages if and when the company should submit applications for patents, copyrights and trademarks, as applicable. In particular, federal registration in the United States (and foreign equivalents) of these types of IP confers a number of important benefits. However, deadlines for submitting applications in many instances may require early analysis of the types of IP a company may create, what portion of the IP can potentially be registered, and whether it would be advantageous to pursue such registration in each case. As the registration process can be expensive, companies can sometimes delay registration until the company's budget permits such activities. However, analyzing the company's initial and potential IP portfolio and adopting a comprehensive IP registration strategy early on will help management develop the company's IP portfolio and remain aware of and work toward various application deadlines in a more focused, efficient and effective manner.

Companies should also register internet domain names, social media account names (including Facebook, Twitter and LinkedIn, among others) and corporate assumed names (*i.e.*, DBAs). These additional registrations support and strengthen a company's brand, allow the company to control and monitor its brand more effectively, and facilitate the company's use of the brand to reach a wider audience. Companies should confirm that desired web URLs and social media account names are available before selecting a corporate name and/or launching commercially. If a desired domain name or corporate name is registered by another person but is available for purchase from that person, it is often advisable to seek to purchase that name as soon as possible so that a company can more easily move to another name if the purchase becomes overly complicated or too expensive.

3. IT Systems Security

In addition to securing ownership of IP through assignments and registration, companies should prevent unauthorized access by securing their IT systems. Companies should

- Use secure and encrypted cloud storage, email and file transfer applications (many free services do not provide much security)
- Require and use appropriate passwords on computers and mobile devices
- Encrypt flash drives and other portable media used by company personnel
- Adopt and abide by a simple document retention and destruction policy

Companies should also conduct basic diligence regarding the IT systems security of potential business partners, such as vendors and other strategic partners who may handle the company's proprietary information. In certain cases, companies may seek contractual provisions requiring such counterparties to implement minimum IT systems safeguards of their own with respect to any of the company's proprietary information shared with such counterparties.

Many startup companies in particular fail to take appropriate steps to secure their IT systems, mistakenly believing that such efforts would be cost prohibitive. Several of the steps described above, however, cost very little. And those items that may require some degree of expense can usually be addressed at reasonable and worthwhile price points.

4. Employee Retention and Post-Termination Obligations

One of the best ways for a company to protect its IP is to ensure that the people who understand the IP best continue to work for the company. A former employee is probably more likely to misuse or misappropriate a company's proprietary information than a hacker or vendor. Although forcing employees to stay with a company is of course impossible, a fair and reasonable approach to employee compensation and otherwise generally creating a positive working environment will go a long way toward decreasing a company's IP risk. Providing employees with reasonable equity compensation subject to vesting may also be helpful.

Employees do, of course, leave even the best of companies. Accordingly, companies should obtain from employees non-competition, non-solicitation and non-disparagement covenants that extend for a reasonable period following termination of employment, to the extent permitted in the applicable jurisdiction. Like employee inventions assignment and nondisclosure agreements, companies should condition employment on new employees signing employee non-competition (to the extent enforceable under applicable state law), non-solicitation, and non-disparagement obligations before commencing work, as obtaining such documents can become difficult and/or expensive later on, especially if an employee is unhappy or is being terminated.

5. Create a Culture of IP Awareness

The suggestions described above will be less effective if a company's management and employees are not working attentively to implement them. Adopting simple but relevant corporate policies, publicizing them internally, enforcing them consistently, and especially training personnel on them will help increase focus on the matters described above. Increased focus will bring increased efforts and vigilance. For example, companies will benefit from training human resources managers and heads of business units regarding the importance of not allowing new employees to begin employment without signing appropriate employee agreements, training new employees regarding document retention and IT security policies, and training sales teams and other personnel who interface with vendors and commercial partners on the necessity of routine nondisclosure agreements and what information is, and is not, subject to such nondisclosure agreements. Conducting such training repeatedly and regularly will help ensure that new personnel are trained quickly and will continually help remind existing personnel of the importance of such matters.

Conclusion

A company's IP is often a distinctively valuable and critical asset to its business and is therefore worth taking affirmative and thoughtful measures to protect. There are many basic, and often inexpensive, actions that companies can and should take to preserve, protect and enhance their IP. While the suggestions above are by no means exhaustive, taking the steps described in this article will help emerging companies strengthen and secure their IP and position them to leverage their IP portfolios for growth and success.

If you have questions about this *Client Alert*, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

[John H. Chory](#)

john.chory@lw.com
+1.617.948.6032
Boston

[Sarah K. Gagan](#)

sarah.gagan@lw.com
+1.617.948.6049
Boston

[Alexander D. Lazar](#)

alexander.lazar@lw.com
+1.617.948.6039
Boston

You Might Also Be Interested In

[Virtual Currencies: New York State Department of Financial Services Discusses Proposed Regulations](#)

[A Look at the Surge in Life Sciences IPOs](#)

[Avoiding Trouble in Emerging Markets](#)

Client Alert is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the lawyer with whom you normally consult. The invitation to contact is not a solicitation for legal work under the laws of any jurisdiction in which Latham lawyers are not authorized to practice. A complete list of Latham's *Client Alerts* can be found at www.lw.com. If you wish to update your contact details or customize the information you receive from Latham & Watkins, visit <http://events.lw.com/reaction/subscriptionpage.html> to subscribe to the firm's global client mailings program.