BuchalterNemer
A Professional Law Corporation

Protecting Confidential Information and Trade Secrets in a Tech Accelerator or Incubator

Dylan Wiseman

Tech accelerators or incubators enable start-ups to collaborate and share ideas, strategies, resources, and know-how. Uber, Spotify, and countless others have emerged from accelerators, incubators, or technology campuses. Amidst the open corridors, lounge spaces, and scattered pizza boxes, start-up businesses need to be mindful of the risks to their intellectual property. Tech incubators present unique risks because most members are extremely sophisticated regarding computers and electronic storage media. Likewise, in many tech incubators, start-up entrepreneurs may not appreciate California's laws around the ownership of intellectual property.

For many start-ups, the concepts for products or services are the life-blood of their operations and future. There are various junctures where a start-up's IP could potentially be disclosed—raising capital, recruiting employees, beta testing or testing a prototype, and in the day-to-day meetings which often occur in close proximity to other members of the incubator.

To put these risks into context, it is important the understand California's laws regarding competition. California workers are free to work anywhere, even for a direct competitor, provided the competition is fair and lawful. In California, most covenants not to compete are void and unenforceable. (Business & Professions Code section 16600.) As a result, start-ups should take both legal and technical measures to protect their IP.

While California will not enforce covenants not to compete, California's courts often enforce confidentiality agreements and intellectual property assignment provisions. The more specific the confidentiality terms, the more likely a court is to enforce the provision. Start-ups should make certain that they describe with specificity categories of information they seek to protect. We recommend prioritizing and identifying what information is highly valuable, or would cause the greatest injury if it were improperly used or disclosed, and build the confidentiality agreement around those categories. Confidentiality agreements should exist with employees, contractors, vendors and suppliers.

Confidentiality agreement should also encompass "trade secret" information. California follows the Uniform Trade Secrets Act (Civil Code sections 3426.1-11.). Trade secret information may include source code, CAD designs, research and development tests, business plans, customer, vendor, and supplier information, and other commercially sensitive information which gives the business a competitive advantage.

California's version of the UTSA has some unique features. First, it protects against the theft, use, or disclosure of information which can be in electronic, paper or memorized by an employee. Second, under California's definition of a "trade secret" it is immaterial that some aspects of the trade secret could be found in publicly available sources. Under California's UTSA, our Legislature likely anticipated that companies would compile information in their research and development efforts from public sources and modify or incorporate some elements into their products or services. Start-ups should make certain that their confidentiality agreements reference California's UTSA because of these unique features.

Likewise, California has specific Labor Code provisions which should be followed to ensure clear title to the start-up's IP. (Labor Code sections 2870-2872.) If the specific terms of the intellectual property assignment statute are not followed, a start-up can easily find itself in expensive litigation over the ownership of its technology. That type of battle will undoubtedly infuriate angel investors or venture capital firms.

Technical measures should also be used to protect confidential information and trade secrets. Particularly given the open, collaborative environment, start-ups should use firewalls, passwords, redundancies, two-step authentication, and should avoid having workers use BYOD devices for work projects. While popular, Bring Your Own Device work environments make it extremely difficult to retrieve data when employees leave.

Most data theft results from employees uploading files to the cloud, or to various storage devices. To help protect against employees taking information, start-ups should monitor computer usage, and also make certain to conduct thorough exit interviews and screenings of new hires.

Implementing legal and technical protections can certainly help start-ups thrive while protecting the company's IP.

Dylan Wiseman is a Shareholder in the Firm's Intellectual Property and Litigation Practice Groups in the San Francisco office. He can be reached at 415.227.3506 or at dwiseman@buchalter.com.