January/February 2015

Intellectual Property: Guidance to the Upstart Tech Company for Protecting IP Rights

By: Gregory Perleberg

Historically, entrepreneurial businesses have been the catalyst for our economy's growth. Too many times, however, the dreams of upstart business owners are crushed due to a lack of attention to intellectual property and related issues. This article will address avoidable legal problems to help ensure that your business has the best chances of becoming the next industry leader.

A company's overall valuation is directly related to its intellectual property portfolio. In fact, for technology and e-commerce businesses, IP can represent in excess of 80% of a company's value. Types of IP include **copyrights** (e.g., original works of authorship such as advertising materials, software code and music); **trademarks** (e.g., brand names, logos and internet domain names, and in some cases shapes); **patents** (e.g., any new and useful process, machine, manufacture, or composition of matter, and in some cases, designs); and **trade secrets** (competitively valuable business information, such as confidential customer lists).

For any early-stage business, it is critical to protect intellectual property from theft and infringement—both in the United States and in other countries where the company does or expects to do business. Companies should inventory their IP to examine what might be eligible for patent, trademark, copyright or trade secret status. Once it is known what IP a company possesses, it can then review its options for protecting that property, and do a cost/benefit analysis to determine which IP protection measures make the most sense. A U.S. utility patent is generally granted for 20 years from the date the patent application is filed. U.S. trademarks can last forever, as long as the trademark is used in commerce and defended against infringement. For copyrightable works (created after January 1, 1978), protection extends for 70 years after the death of the owner. For "*works made for hire*" (covering the usual type of work owned by a business, such as website designs obtained through an independent contractor), the copyright lasts for a term of 95 years from the year of its first publication or a term of 120 years from the year of its creation, whichever expires first. Licensing agreements are also an important element of successfully commercializing IP rights.

Key considerations for business owners include:

- Document the creation of your intellectual property. The ideal documentation is federal registration through the U.S. Patent and Trademark Office (www.uspto.gov) or the U.S. Copyright Office (www.copyright.gov). In the event of infringement, registration can be an important part of your case and may be required if you plan to sue the infringer.

- Do not overlook the importance of trademark "*clearance*," which allows a qualified trademark attorney to review and analyze current uses of your particular mark as well as those that may create a likelihood of confusion and risk of infringement. Should a third party discover your use of an infringing mark, they may demand that you discontinue use of the mark (replacement signage, packaging, etc., can be costly), stop using a domain name, sue you in an effort to collect damages or enjoin your business from continued operation using that trademark. While a trademark clearance reveals potential problems, it may also reveal that you are indeed the first to use a particular trademark, and therefore, may be entitled to seek federal registration.

January/February 2015

- Take caution when including literary, music and artistic works in connection with your advertisements and website. Unless placed in the public domain, using a third party's materials (e.g., a photo or even a few notes of a song) may constitute copyright infringement and expose your company to substantial legal liability. As a rule of thumb, prior written authorization should be obtained.

- Always utilize written agreements with freelance web developers, graphic designers, writers, and the like, specifically providing that your business will own any developed materials as a "*work for hire*." **And, carefully review the provisions of *any* contract involving limitations of liability, warranties and indemnification/hold harmless obligations.**

- Employees should be restricted from divulging to their new employers their former employer's trade secrets or using them to the former employer's disadvantage. Most states have adopted the Uniform Trade Secrets Act ("UTSA"), which defines a trade secret as "*information that derives independent economic value, actual or potential, from not being generally well known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use and which is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.*"

  Examples of "*information*" under the UTSA are formulas, drawings, patterns, compilations, programs, devices, methods, techniques, or processes. Generally, to be considered a trade secret, the information must be kept in a locked or secured location. Think of the "*secret recipe*" for Coke locked away in a vault. Trade secrets may include not only designs and formulas, but also customer lists and pricing information. Safeguards should also be put in place to prevent departing employees from removing or emailing to themselves any customer lists, technical documents, training manuals or computer programs/software belonging to your company.

- If you suspect infringement, contact an attorney specializing in intellectual property law. This area of the law can be complex and an attorney's help can be crucial.

Gregory Perleberg is an attorney in the firm's Intellectual Property and Corporate Practice Groups in the Los Angeles office. He can be reached at 213.891.5106 or gperleberg@buchalter.com.

January/February 2015

Mergers & Acquisitions: Five Legal Issues Entrepreneurs Should Consider Before Agreeing To an Earn-Out in M&A Transactions

By: Julia Nguyen

In technology company mergers and acquisitions, there is an inherent asymmetry of information between the skeptical buyer and the optimistic seller on the valuation of the target company and its future profitability. This is especially true when the target company has little operating history but significant growth potential, or has a new product or technology that may increase its profitability in the future. To bridge this valuation gap, buyers and sellers may compromise on an earn-out, which is a deal structure where part of the purchase price is deferred until after closing and is calculated based on the performance of the target company over a set time period. The following are five legal issues to consider before agreeing to an earn-out.

1. Initial Structure of an Earn-Out

In general, earn-outs have the potential to create contentions between the buyers and sellers over the interpretation of the earn-out terms and the operation of the target company during the earn-out period. Earn-outs can vary widely and generally are tailored to suit the target company and the parties' expectations, so clear terms and expectations should be set forth in a written agreement. These terms should include the source of the earn-out, the benchmarks to measure performance, a formula for calculating the payment amount, and the period of time over which the earn-out will be measured.

2. Performance Metrics

Many disputes over earn-outs arise when the seller disagrees with the buyer's calculations of the target company and whether the seller has met the performance metric. The most common performance metrics used in an earn-out formula are: revenue, net income, EBITDA and earnings per share. Sellers may want to choose revenue because it can be easier to achieve and is less easily manipulated by the buyers. Buyers may want to choose net income because it takes into account costs. The parties often compromise on EBITDA, which accounts for operation costs and expenses, but excludes non-operational items such as interest, tax, depreciation and amortization expenses. With technology companies, it may be difficult to set financial targets if there is no historical information to use as a basis. Non-financial performance metrics like number of users, product development, number of products sold or launch of a new product may be more appropriate. Choosing a non-financial performance target will oftentimes lead to fewer disputes because the focus is on the operational effectiveness of the target company and it is harder to manipulate by altering accounting practices.

3. Post-Closing Covenants

Once the buyer absorbs the target company, the seller may not have sufficient control to manage the target company to achieve the performance metric. The seller should consider covenants that will set some limitations on the buyer's ability to operate the target company. Such restrictive covenants may require the buyer to operate the business consistently with how it was operated prior to closing and prevent the buyers from making significant changes that reduce the earn-out purchase price—like discontinuing products, reducing the sales force or shifting sales and costs of the target company. The seller should require the buyer to act in good faith and use reasonable efforts to take every action necessary to maximize the earn-out purchase price. The seller may also want acceleration rights that would result in immediate payment of the earn-out purchase price if events occur that negatively impact the earn-out performance metric—such as a subsequent sale of the target company or a change-in-control of the buyer.

January/February 2015

4. Integration of the Target Company with the Buyer's Business

Because buyers may have the opportunity to manipulate the financial performance of the target company, issues may arise if the target company is merged into the buyer's other businesses. Sellers should consider requiring the buyer to maintain separate books and records for the target company to be reviewed by the sellers and their accountants to avoid the potential for such manipulations and future disputes.

5. Earn-Outs Tied To Future Employment

Buyers may want to tie the earn-out purchase price to future employment of the founders and certain key employees of the target company, because this may be important to the future success of the target company. Before sellers agree to this earn-out arrangement, they should consider the tax implications. Earn-out payments may be taxed as compensation income when tied to the seller's continued employment as opposed to the more tax advantageous capital gains rate. Furthermore, this earn-out arrangement could prevent the seller from getting a clean break from the target company and moving on to the next great idea.

As the M&A market continues to heat up in 2015, many tech companies will be faced with deciding whether the flexibility offered by earn-outs is outweighed by the complications they often present.

Julia Nguyen is an attorney in the firm's Corporate Practice Group in the Orange County office. She can be reached at 949.224.6238 or jnguyen@buchalter.com.

January/February 2015

Bank/Finance: Debt Financing for Tech Companies That Do Not Have a Long Credit History

By: Bukola Mabadeje

Small and medium size technology companies that do not have the benefit of a long credit history are often faced with a challenge when it comes time to obtain debt financing. Traditional lending institutions look to a company's credit history to make credit decisions. Credit history in turn is based on the historical cash flow of the company. Notwithstanding, there are alternative bases on which a lender could extend credit to a borrower that either lacks or has an inadequate credit background.

It is now fairly common for banks and other commercial lenders to make loans without a long credit history of the borrower, as long as there are assets of the borrower which the lender can look to as a source of repayment and also as collateral in the event of failure to repay the loans.

Such assets go beyond the obvious real estate assets, to include less obvious assets like accounts receivable, equipment and inventory of a company, which could form the borrowing base of a loan, as well as the assets to which the bank may take a lien. The more readily convertible assets for such loans are accounts receivable—i.e. the income due to a borrower from any number of third party contracts for the supply of goods or services. A lender would simply appraise the value of such accounts receivable, and advance credit based on the expected income.

To illustrate, suppose the borrower anticipates an approximate dollar amount of receipts from its contracts within a certain period of time. The lender would lend a percentage of that expected income with the expectation that the payment received would be used to pay off the loan. The lender also would perfect its security interest in the accounts receivable by filing a financing statement at the appropriate State UCC filing office.

With a steady and sizeable portfolio of assets along with the right lender, there may be an abundance of financing sources available to the atypical borrower.

Bukola Mabadeje is an attorney in the firm's Bank and Finance Practice Group in the San Francisco office. She can be reached at 415.227.3510 or bmabadeje@buchalter.com.

January/February 2015

Cyber Security/Data Breach: President Calls for New Anti-Hacking Legislation

By: Oren Bitan

With recent high profile cyber-attacks against Sony and other companies, data hacking has quickly risen to forefront of issues on the President's agenda. That's why, as widely anticipated, the President took the opportunity during his recent 2015 State of the Union address to urge Congress to enact additional cyber security protections, including legislation that would introduce data breach notification laws requiring companies to notify affected consumers within 30 days of an attack.

As the President cautioned during his State of the Union address, "[n]o foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism. And tonight, I urge this Congress to finally pass the legislation we need to better meet the evolving threat of cyber-attacks, combat identity theft, and protect our children's information."

Privacy advocates, like the Electronic Frontier Foundation, have cautioned that any new legislation threatens to undermine consumer privacy. In addition, watered down federal legislation could unwittingly weaken existing laws in some states like California if it preempts state laws that are more restrictive than any federal law eventually enacted. For now, companies and consumer advocates should continue to monitor what action, if any, may be taken at the federal level. At this point, it is not clear that this Congress will pass such legislation given the current political climate.

For more information, please join Oren Bitan for a Buchalter Teleseminar on May 20, 2015 entitled "A Brave New World: The State of Data Hacking Laws in 2015." Please click here to register for this complimentary teleseminar.

Oren Bitan is an attorney in the firm's Litigation Practice Group in the Los Angeles office. He can be reached at 213.891.5012 or obitan@buchalter.com.

January/February 2015

Aviation & Aerospace: The Launch of Commercial Drones

By: Paul Fraidenburgh

The only thing outpacing the Federal Aviation Administration's rapid development of guidelines and regulations governing unmanned aircraft systems (also known as drones) is the list of industries seeking to use those systems for commercial purposes. In recent months, the FAA has approved a small but growing number of petitions seeking authorization to operate small UAS (55 lbs. and less) for commercial purposes ranging from agriculture to filmmaking to flare stack inspection. The petitions were filed pursuant to Section 333 of the FAA Modernization and Reform Act of 2012, which provides a procedure for expedited authorization for commercial operations using small UAS. The companies that filed the successful petitions are currently conducting the only legal commercial UAS operations in U.S. airspace.

As drone technology continues to disrupt new industries, the importance of Section 333 petitions as the sole avenue for conducting commercial operations has become increasingly clear. Though the FAA has worked with NASA and Congress to develop a comprehensive set of regulations governing commercial UAS operations, internal agency audit reports have revealed that the regulations are not expected to be finalized until 2016 or later. Until then, Section 333 will remain the holy grail for UAS operators who plan to conduct commercial operations in the foreseeable future.

For more information about the latest legal developments on commercial use of drones, please click here to read the Q4 2014 edition of Buchalter Nemer's Aviation & Aerospace and Surface Transportation Quarterly Newsletter.

Paul Fraidenburgh focuses his practice on representing technology companies in regulatory affairs and litigation. As a member of the Aviation & Aerospace Practice Group, Mr. Fraidenburgh has gained a national reputation for his representation of clients in the unmanned aircraft systems industry. The Wall Street Journal, Los Angeles Times, and several other publications have quoted Mr. Fraidenburgh on the topic of unmanned aircraft systems, and his clients are among the most cutting-edge filmmakers and aviation companies in the world. He can be reached at 949.224.6247 or pfraidenburgh@buchalter.com.

January/February 2015

Labor/Employment: New Minimum Wage and Overtime Exemption Thresholds for 2015

By: Michael Westheimer

Wage and hour issues are a pervasive source of litigation in California and nationwide. To help mitigate this risk, tech industry companies in California need to be aware that certain minimum wage and overtime exemption thresholds are adjusted annually. The following are various state and local pay thresholds effective as of January 1, 2015.

California's overtime exemption for computer software professionals has a pay threshold that currently requires payment of either: an annual salary of at least $85,981.40, a monthly salary of at least $7,165.12, or an hourly rate of at least $41.27.

California's minimum wage currently is $9.00 per hour, and is scheduled to increase to $10.00 per hour effective January 1, 2016. As a related issue, changes to the state minimum wage also impact the pay thresholds for certain state overtime exemptions.

- California's overtime exemptions for executive, administrative and professional employees all have a pay threshold that requires payment of a salary of at least twice the state minimum wage for full time employment. The salary threshold currently is $37,440 per year, and effective January 1, 2016 it will increase to $41,600 per year.
- California's overtime exemption for commissioned (inside) salespersons has a pay threshold that requires payment of total compensation in excess of 1½ times the state minimum wage. Total compensation currently has to exceed $13.50 per hour worked, and effective January 1, 2016 it will have to exceed $15.00 per hour worked.

Finally, some cities in California have (or soon will have) a higher minimum wage for employees working within their geographic boundaries. Current city minimum wages are:

- San Francisco – $11.05 per hour
- San Jose – $10.30 per hour
- Oakland – $9.00 per hour, increasing to $12.25 per hour effective March 2, 2015
- Berkeley – $10.00 per hour, increasing to $11.00 per hour effective October 1, 2015
- Richmond – $9.60 per hour
- San Diego – $9.75 per hour

Michael Westheimer is an attorney in the firm's Labor and Employment Practice Group in the San Francisco office. He can be reached at 415.227.3530 or mwestheimer@buchalter.com.

January/February 2015

Commercial Litigation: Court Decision Addresses Court's Jurisdiction to Hear a Lawsuit Alleging Defamatory Internet Posts

By: Randall Manvitz

The rise of social media has seen a corresponding rise in lawsuits seeking redress for alleged defamatory statements posted on Internet sites. This raises many novel legal issues, including whether a person can be sued in a faraway state because he or she posted a statement on the Internet that allegedly harmed someone who resides in that faraway state.

The California Court of Appeal recently issued an interesting opinion in *Burdick v. Superior Court*, analyzing whether a California state court has personal jurisdiction over an out-of-state defendant who allegedly posted defamatory statements on Facebook about a California resident. The court held that posting defamatory comments on a website while knowing that a plaintiff resides and will be damaged in California is insufficient on its own for the minimal contacts necessary for personal jurisdiction. Personal jurisdiction must be based on the defendant's forum-related acts instead of the plaintiff's forum contacts, so to establish jurisdiction it is necessary that the defendant: "expressly aim or specifically direct his or her intentional conduct at the forum, rather than at the plaintiff who lives there."

While the facts in *Burdick* were insufficient to establish jurisdiction over an out-of-state defendant in California, the parameters of personal jurisdiction over a defendant who intentionally damages a resident of another state via the Internet is sure to be a hot topic for years to come.

Randall Manvitz is an attorney in the firm's Litigation Practice Group in the San Francisco office. He can be reached at 415.227.3644 or rmanvitz@buchalter.com.