ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Vanishing IP: 6 Tips to Secure Your Company’s Most Valuable Assets from Departing Employees

Technology, Privacy, and eCommerce

Employees come and go — it's a part of corporate life. One thing that should absolutely not leave with a departing employee is your company's intellectual property (IP). Otherwise, it could appear in the public domain, a competitor's war chest, or the dark web marketplace where it could possibly be sold to the highest bitcoin bidder.

This past year, a slew of high-profile trade secret and intellectual property disputes have been filed in the United States, and under the recently enacted Defend Trade Secrets Acts (DTSA), which provides a federal, private, civil cause of action for trade secret misappropriation. Some of these disputes might have been prevented if sensible measures were taken to safeguard IP from departing employees. In addition, many corporations are dismayed to learn that their IP is not eligible for protection because basic precautions were not followed to maintain its protectable status under state or federal law.

For example, both the DTSA and most state laws based on the Uniform Trade Secrets Act (UTSA) generally require that a company take "reasonable" measures[1] to maintain the secrecy of its trade secrets. Otherwise, protection can be lost forever. Courts, however, have come to drastically divergent conclusions as to what constitutes reasonable measures under the particular circumstances of a given case. Below are some commonsense approaches that may protect your company from vanishing intellectual assets, especially at the hands of departing employees.

1. Draft clear employment agreements and corporate policies

Employment agreements are probably the simplest (and most effective) safeguard that can be taken well before an employee considers fleeing for greener pastures — ideally on each new hire's first day. However, not all employment agreements are equitable.

In addition to the standard IP ownership provisions, which should be drafted to effectuate transfer of all IP from employer to employee as an operation of law immediately upon the creation of any protectable asset, these agreements should also include confidentiality and non-disclosure provisions.

Furthermore, employment agreements should clearly identify any IP that is believed to be already owned by the employee. This includes IP developed prior to commencing employment or IP developed without company resources and outside the scope of their employment. Starting the employer-employee relationship off with a clear, written understanding of any pre-existing IP can help prevent costly disputes long after the employer and employee have parted ways.

Employee handbooks and written corporate policies can sometimes be seen as part of the contractual promises between an employer and employee, particularly when they are incorporated or referenced in the employment agreement itself. These policies should clearly delineate what rights, if any, remain with the employee upon termination and what rights stay with the corporation. Confirm that your handbook and IP policies comply with all applicable state laws, which sometimes require carve-outs for IP created by the employee entirely on their own time, without the use of any company assets or information, or that does not relate to the company's or employee's line of work or business.

In addition to the standard IP ownership clauses, some employment agreements and corporate policies can also include "cooperation" clauses that require former employees to cooperate with any continued development or enforcement of IP. This cooperation may come in the form of executing a patent declaration, providing technical consulting, or sitting for a deposition in an enforcement action involving IP developed by the former employee. These cooperation clauses help clarify the expectations between the parties, particularly if the company pursues the enforcement of IP developed by a former employee.

2. Conduct exit interviews

Although sometimes difficult to schedule, especially for wayward employees, exit interviews can serve as a useful reminder of an employee's confidentiality obligations after departure, particularly for employees who may have accessed sensitive company information or IP. These interviews can also be used to:

- Remind a departing employee to return all company-issued computers, storage devices, and security devices;
- Require the employee to affirm that all sensitive or confidential company documents have been returned or destroyed; and,
- Document the ongoing rights and obligations between the parties.

When searching for company documents, departing employees should review all personal email accounts, personal computers, storage locations (e.g., USB drives) and backup locations (e.g., cloud storage).

3. Provide and log employee IP training (and retraining)

Mandatory employee training can come in many forms and cover a variety of topics. One topic might include the marking and handling of confidential corporate information.

Marking documents “confidential” can be effective, especially if documents are consistently and uniformly marked — and unmarked upon the information becoming public. Many companies also require regular re-training and reaffirmation of confidentiality training, which can help a company show that it took reasonable measures to maintain the secrecy of its trade secrets.

4. Maintain a corporate trade secret registry

Disputes often arise during litigation surrounding what constitutes a corporate trade secret. One way to eliminate this uncertainty is to maintain a corporate trade secret registry. The registry can identify or log all information (e.g., source code, hardware designs, prototypes, or even in some cases customer lists) that the company believes are worthy of trade secret protection.

While a competent court or jury may ultimately decide whether the information identified in the registry qualifies for protection, a registry serves as a useful tool to remind employees about the existence of potentially sensitive information, as well as the confidentiality and marking obligations associated therewith. The registry can also be expanded to serve as an access log to detail who have accessed or currently possess a sensitive corporate asset.

5. Tighten electronic and physical access security policies

In general, many companies choose to limit access to putative trade secrets on a strict “need to know” basis. Limiting access helps prevent inadvertent disclosure and prying eyes from learning the contents of the secret. Limiting access can include the use of physical or electronic security/audit policies.

Highly sensitive information such as source code can be stored on a physically separate server or standalone computer without network or external drive access. This information uses tighter access policies, such as mandatory encryption and multi-factor authentication. Less sensitive information, on the other hand, might be stored on the company’s main data server and subject only to user password security.

6. Enforce, enforce, enforce!

A company’s IP is only as strong as the enforcement of the corporate policies designed to protect it. Lax enforcement may lead to public disclosure and the loss of trade secret status. Companies should task their legal departments to strictly enforce all IP agreements and policies, including marking policies, confidentiality and non-disclosure agreements, and employment and exit agreements.

The legal department should also work closely with human resources to take swift action against offending employees. Repeatedly condoning clear violations of a company’s IP policies may be one consideration that courts evaluate when considering whether reasonable measures were taken to protect the confidentiality of corporate IP.

Of course, this list is neither exhaustive nor required to protect your IP. Reasonable measures to maintain the secrecy of information can depend on the industry, locale, and type of information. However, implementing some of these measures will ensure that your corporate IP remains safely in the corporate coffers.

NOTES

1 The UTSA’s definition of a trade secret requires “efforts that are reasonable under the circumstances to maintain its secrecy” (Unif. Trade Secrets Act § 1(4)) while the DTSA requires the owner to take “reasonable measures to keep such information secret” (18 U.S.C. § 1839(3)).

Olga V. Mack

Fellow

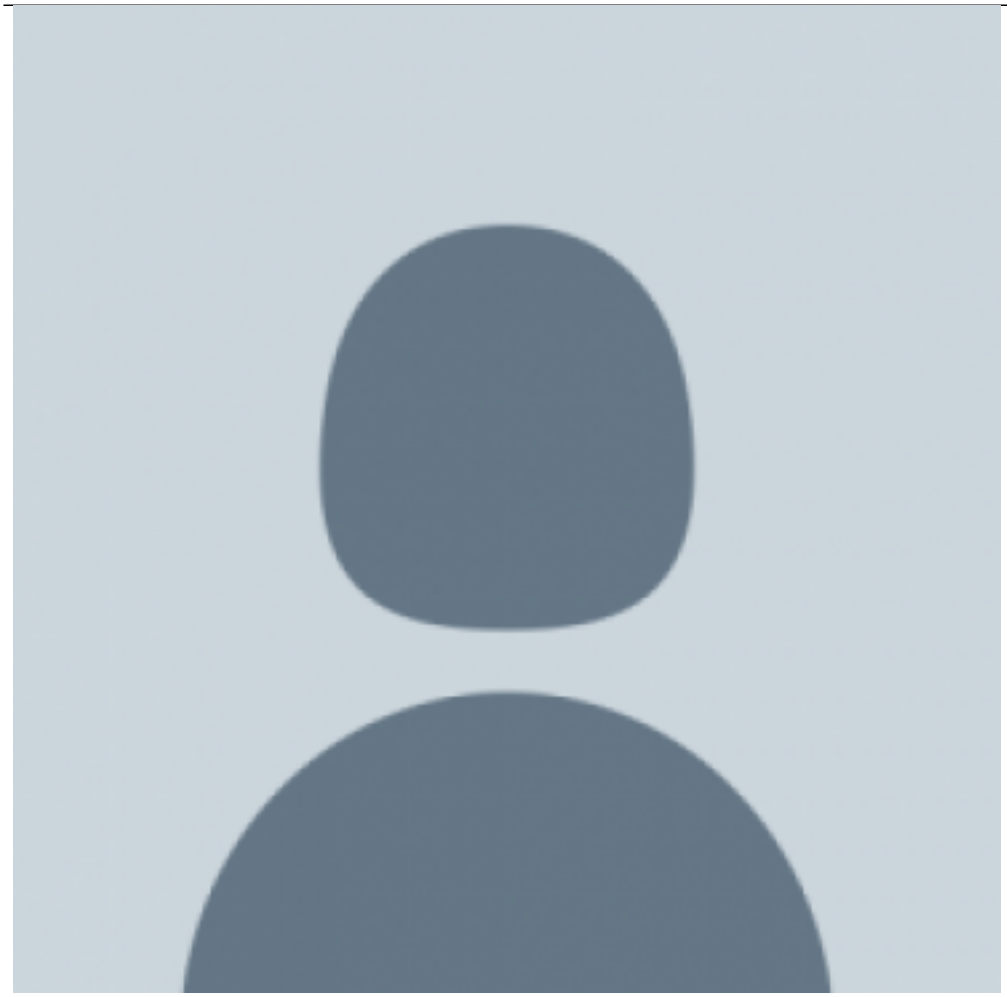
CodeX

Olga V. Mack is a fellow at CodeX, The Stanford Center for Legal Informatics, and a Generative AI Editor at law.MIT. Mack shares her views in her columns on ACC Docket, Newsweek, Bloomberg, VentureBeat, Above the Law, and many other publications.

Mack is also an award-winning (such as the prestigious ACC 2018 Top 10 30-Somethings and ABA 2022 Women of Legal Tech) general counsel, operations professional, startup advisor, public speaker, adjunct professor, and entrepreneur. She co-founded SunLaw, an organization dedicated to preparing women in-house attorneys to become general counsels and legal leaders, and WISE to help female law firm partners become rainmakers.

She has authored numerous books, including Get on Board: Earning Your Ticket to a Corporate Board Seat, Fundamentals of Smart Contract Security and Blockchain Value: Transforming Business Models, Society, and Communities. She is working on her next books: Visual IQ for Lawyers (ABA 2024), The Rise of Product Lawyers: An Analytical Framework to Systematically Advise Your Clients Throughout the Product Lifecycle (Globe Law and Business 2024), and Legal Operations in the Age of AI and Data (Globe Law and Business 2024).

Brian Mack



Brian Mack is a partner in Quinn Emanuel Urquhart & Sullivan’s San Francisco office. He joined the firm in 2011. His practice focuses on high-stakes complex commercial litigation and intellectual property disputes, including patent, copyright and trademark infringement, antitrust, unfair business practices, and intellectual property licensing. He received his JD from Fordham University School of Law in New York City.