Trade Secrets: What Game Developers Should Know

August 24, 2021

By Anthony D. Del Monaco, Forrest A. Jones, and Seth W. Bruneel

Intellectual property is critical to the gaming industry, as we have explored through this series. Patents, trademarks, and copyrights (white paper forthcoming) all rely on disclosure to the public. What if the property you want to protect doesn’t fit neatly into one of those three categories? What if disclosing this information to the public will destroy the value in it?

As we resume our series exploring the basics of intellectual property law and its application to the gaming industry, we discuss what you can do when disclosure of your intellectual property is not an option: protect it as a trade secret.

I. What Are Trade Secrets?

Trade secrets, at their most basic, are precisely that: secrets you keep that allow you to perform your trade. Trade secrets, however, can be more than simply a company’s confidential, internal information and policies. If you structure them correctly, they can also have some unique legal protections.

The legal definition of trade secrets is information that (1) has been the subject of reasonable measures to maintain its secrecy, and (2) derives independent economic value from not being generally known to, or readily ascertainable through proper means by, others who can obtain economic value from its disclosure or use. The simplified definition of trade secrets is knowledge or material that is (1) kept secret and (2) valuable because they are kept secret.

Other than being secret and having value, trade secrets do not have the same complex limitations on their protectable subject matter that patents, copyrights, and trademarks do. Trade secrets can take a variety of forms, covering information like customer lists, pricing information, manufacturing processes, encrypted code, internally developed game engines, or any other material that provides a company a competitive advantage.

By their nature, the existence of many trade secrets is secret. But some famous examples of trade secrets from other industries are the recipe for Coca-Cola, the formula for WD-40, the Google search algorithm, and the method by which the New York Times compiles its “Best Seller” list. Examples specific to video games might include source code for software, game engines, user profiles and identification, or, in some cases, agreements.

1. These materials have been prepared solely for educational and entertainment purposes to contribute to the understanding of intellectual property law. These materials reflect only the personal views of the authors and are not individualized legal advice.
2. Please note that this series of papers focuses on the intellectual property laws of United States. Other countries often have their own versions of these intellectual property rights, though the rules can be, and are usually, different. You should consider the laws of any country in which you plan to make, use, or sell your game when considering intellectual property protection. Further, for those located outside of the United States, if you plan on selling games within the United States, you should still become familiar with its intellectual property laws and seek out protection where appropriate. Foreign entities may obtain intellectual property protection in the United States.
Importantly, it is not enough that something is a secret. To obtain and maintain trade secret protection, you need to take affirmative steps to keep it a secret. The way you are required to keep information secret is case-specific, and some of these options are discussed below. But generally, having a plan or policy for protecting the information identified as a trade secret that includes a duty to maintain confidentiality, and more importantly, following it, is a best practice for all companies.

Information can be valuable ("demonstrate independent economic value") for many reasons. The information can take almost any form, such as scientific, technical, engineering, economic, business, or financial. One example of valuable information is whether that information makes a product easier or cheaper to manufacture or produce. Another example is if that information results in a better-quality product than without the knowledge.

Furthermore, just because you protect certain information does not mean it qualifies as a trade secret. If a third party obtains the information just by looking at a product or taking a product apart, then it is likely too readily ascertainable to qualify. Generally, if the information you want to protect can be worked out from just purchasing and playing a game, you likely cannot get trade secret protection for it. But if it would require breaking the encryption on a codebase, it may qualify.

Often, software is a gaming developer’s most valuable business asset. Software is easy enough to keep secret from the players, as they see the front-end product rather than the underlying code. Protecting software as a trade secret, however, can get complicated when collaborating with other design studios or when employees transition from company to company. As discussed in more detail below, entering into a nondisclosure Agreement is a good first step at protection.

Another thorny issue can be open-source software, because open-source software is publicly accessible, and thus not secret. You, however, may still be able to protect the way you combine publicly available software with proprietary software as a trade secret in some cases.³

Finally, trade secret laws protect against the unauthorized use of a trade secret. Unauthorized use may occur when the information is misappropriated or stolen. More commonly the trade secret is improperly disclosed by someone who initially acquired the information by proper means. The laws governing trade secrets do not protect against discovery of the information by fair and honest means such as independent discovery, negligent or accidental disclosure by the owner, or legitimate reverse engineering. The laws do protect trade secrets that are obtained by proper means, but are then utilized outside the scope of the trade secret protections in place.

How Can Trade Secrets Help My Company?

One of the largest advantages of trade secret protection over other forms of protection may seem obvious, but it is that you get to keep your information a secret. By protecting innovations as trade secrets, you are not required to disclose it to the public (versus, for example, a patent, which requires disclosure). This protection allows your company to continue to derive the value that comes from knowing the secrets, so long as it remains secret.

Typically, companies treat trade secrets as complementary, or as an alternative, to patent protection. (For a full discussion of patent protection, please refer to the utility and design patent white papers in our series). Companies will weigh many factors (such as how easy it is to reverse engineer the technology) to determine whether it is best to patent the innovation, treat the innovation as a trade secret, or, more likely, protect different aspects of the innovation using both methods.

One advantage that trade secrets have over patents is that they are faster to obtain. There is no examination process for trade secrets, whereas patents can take years to obtain. Thus, in situations where speed is necessary, trade secrets are advantageous because they are instantaneous.

Just as patents can be slow to obtain, they can also be slow to enforce. Patents cannot be enforced until issued, and generally, patent damages do not begin to accrue until issuance. To enforce a patent, a case must be brought in federal district court. The average time from filing a suit in district court until a court conducts a trial ranges from one and a half to three years, depending on the venue and the judge. Comparatively, trade secrets are immediately protected, and a misappropriation case timeline is only subject to the specific facts of the case and idiosyncrasies of the individual courts.

---

³. See e.g., Rivendell Forest Products, Ltd. v. Georgia-Pacific Corp., 28 F.3d 10422 (10th Cir. 1994).
Another limitation on patents is that they expire. A utility patent term is limited to 20 years from filing. Conversely, a trade secret’s term is indefinite, with no expiration, so long as the trade secret is maintained secret.

Trade secrets are also free from geographic restrictions or limitations. While patents are jurisdictional and require separate filings in individual countries, trade secrets have no such limits or requirements.

Trade secrets do have some limitations. The biggest is that trade secret protection ends when the information is no longer secret. Meaning, once a trade secret is “out of the bag,” the protection is lost. With so much information readily ascertainable by public means such as the internet, it can be difficult for information to qualify as or remain a trade secret. Reverse engineering is also prevalent and becoming less difficult, especially for electrical and computer products. Further, publicly released software can be easily decompiled to view the actual source code. These factors must be considered when determining whether to treat information as a trade secret or seek alternative protections.

Furthermore, unlike patents, trade secrets do not confer a right to exclude others from using or practicing a trade secret. Therefore, if a competitor obtains and uses the protected information by legal means identified above, there is no way to stop them from using that information.

Trade secrets can also require complex management scenarios. Maintaining trade secrets can involve detailed policies, employee training, and nondisclosure agreements which can be further complicated when working with third parties, or as a part of a joint venture.

Finally, patents are easier to estimate value than trade secrets. Patents are public, discrete documents, that lend to easier evaluation. If you are securing funding, a patent may be an easier way to demonstrate the value of your innovations, particularly if you can show the protected technology is the only way to address a problem in the industry.

What Is the Process for Obtaining a Trade Secret?

Unlike other forms of intellectual property, there is no official process or application for awarding information trade secret “status.” The information itself is the trade secret. Thus, if the information is kept secret and remains valuable from being secret, its status as a trade secret continues. This immediate protection is advantageous, as the trade secret status can be instant and endless without specific limitations on subject matter.

As highlighted below, however, you only have trade secret protection if you are actively protecting your trade secret. So, while there is no application process, you should still move early to set up your protections, or risk losing your trade secret to the public.

What Should I Do to Protect My Trade Secrets?

The simple answer is “keep it secret.” What that means in your individual situations and jurisdictions is more complex. Below is a nonexhaustive list of protections that may be used. But it is likely worth investing in advice to tailor the protection to your specific company and situation. Courts will analyze whether a company took reasonable steps to protect its trade secrets, and that “reasonableness” test will differ based on different factors such as the company’s size, resources, and experience.

The first category is physical protections. These protections can be as simple as locks on doors and other physical security measures. These not only physically prevent “thieves” from accessing trade secrets, but they also put those with access (such as employees) on notice that there is something valuable to be protected and that they should do their part in maintaining the secrets. Another example is to physically label the information as a trade secret so that it is obvious the information someone is looking at is treated and protected as such.

The second category is digital protections. These protections may be the most important tool for video game developers. Data should be stored in a secure database, behind firewalls and strong passwords. Additionally, not everyone should have access to all secret material. It is not uncommon to have different groups of coders working on discrete aspects of a game where there are a limited number of people who have access to the entire code set. Limiting the number of people with access to the trade secrets will go a long way in keeping it protected.
The third category is legal protections. Non-disclosure agreements may be required when sharing information with other companies or might be part of employee hiring procedures or your employment contract. Confidentiality agreements may also prevent employees from using secret information (that they cannot “delete” from inside their heads) if they move to a different company or start their own. Notice to employees with access to the trade secrets that what they see are trade secrets and must be protected can also be useful.

Most, if not all, of these protections are preventative in nature, underscoring the need to have effective protections in place early. Part of any trade secret case is analyzing the protection surrounding the trade secrets to ensure that you have taken reasonable measures to protect your information. This analysis looks for a minimum degree of protection based on the company’s situation, so putting in effective policies, procedures, and protections up front can streamline the analysis and move your case along.

**How Do I Protect Myself From Allegations of Trade Secret Theft?**

Other companies have trade secrets, too. Most commonly, accusations follow employees as they move between competitive companies. Thus, when an employee begins work for a new company, the new company should ensure that their new employee did not take, or will not use, trade secret information from their previous employer.

While not specific to gaming, a cautionary tale from the world of self-driving cars is a good example. Anthony Levandowski was one of the founding members of Google’s engineering team working on a self-driving car project until he resigned to form his own company in 2016. The new company existed for only six months before Uber purchased it. Google took Uber to court alleging that Levandowski took Google’s trade secrets when he left and eventually sold them to Uber. The parties settled, but Levandowski faced criminal charges and jail time.

**How Are Trade Secrets Enforced?**

Trade secrets are enforced in court. Cases can be filed in federal court or the International Trade Commission for trade secret misappropriation, like patent litigation. But, unlike patents, you can also file complaints in state courts.

The remedies available for trade secret misappropriation include monetary awards. Such awards can vary greatly, often resulting in large verdicts against defendants. The damages determinations can be based on a variety of theories that seek to allow a party to recover for past harm and/or try to compensate the trade secret holder for what is now publicly available. In extreme cases, damages may be doubled where the misappropriation was done willfully. Some states even allow those seeking to protect their trade secrets to recover money for attorneys’ fees. Additionally, injunctive relief may hinder additional harm by preventing future use or disclosure by those who unlawfully took and used the trade secret.


It is not difficult to see how a similar situation could play out between game developers.
Ideally, trade secrets are never enforced. Only in very limited circumstances can the courts effectively “put the genie back in the bottle.” The best way to protect trade secrets is by preventing them from disclosure or theft in the first place.

**How Can My Company Look for Trade Secret Opportunities?**

When evaluating whether information may qualify for trade secret protection, start by thinking of what information you have that you wouldn’t want your competitors learning. With that in mind, game developers should consider whether the information (1) has been the subject of reasonable measures to maintain its secrecy, and (2) derives independent economic value from not being generally known. They must also consider how many people have access to the information, how the information is included in a final product, the cost of putting the necessary tools in place to keep the information secret, the length of time they wish to protect their trade secrets, and alternative avenues available for protecting them.

Indeed, due to the list of issues to consider for maintaining trade secret protections, the best time to set up a trade secret policy is before you develop the information that you want to protect. The second-best time is yesterday.

Based on the swath of tools available and specificities of each company and potential trade secret, developers should consider consulting with an attorney who understands the legal requirements for protecting their most valuable assets as part of their first activities as a company. Besides clarifying if information may qualify for trade secret protection, a good attorney may also help suggest additional ideas and avenues for protecting the information as well as how best to maximize the profitability of a developer’s overall intellectual property portfolio.

---

**Related Professionals**

**Anthony Del Monaco**’s practice involves all facets of intellectual property law in a wide spectrum of technologies. He focuses on patent litigation, primarily before U.S. district courts and the U.S. International Trade Commission (ITC), and arbitrations. His practice also includes inter partes reviews (IPRs), opinions of counsel, patent and trademark portfolio development, and complex licensing issues.

Anthony D. Del Monaco, Partner  
Washington, DC  
+1 202 408 4023  
anthony.delmonaco@finnegan.com

**Forrest Jones** focuses on patent litigation, including at the ITC, as well as IPR proceedings before the Patent Trial and Appeal Board (PTAB) and appeals before the U.S. Court of Appeals for the Federal Circuit. He has technical and legal experience in various areas of electrical and computer engineering, including computer software, signal processing, wireless networking, power electronics, power generation, and consumer electronics such as televisions, laptop computers, smartphones, and gaming systems and technologies.

Forrest A. Jones, Associate  
Washington, DC  
+1 202 408 4019  
forrest.jones@finnegan.com

**Seth Bruneel** focuses on patent prosecution and patent litigation in a wide array of technologies in the electrical field, including financial transaction processing, electric vehicle batteries, and machine learning systems.

Seth W. Bruneel, Associate  
Washington, DC  
+1 202 408 4204  
seth.bruneel@finnegan.com