

Top U.S. Legal Issues for Companies Investing in Esports and Gaming Technology: A Primer

May 28, 2025

The esports and gaming technology industry is experiencing rapid growth, with global revenue expected to surpass \$3 billion by 2025. As companies rush to invest in this lucrative sector, they must navigate a complex legal landscape that includes intellectual property protection, contract law, regulatory compliance, and more. Below are the most critical legal issues facing businesses investing in esports and gaming technology in the U.S.

1. Intellectual Property (IP) Protection

Copyright and Trademarks

Video games and esports involve multiple layers of intellectual property, including game content, character designs, logos, and branding elements. Companies investing in the industry must ensure they own or properly license these assets.

- **Game developers and publishers:** Must protect their original game content through copyright laws.
- **Esports teams and organizations:** Need to secure trademarks for their team names, logos, and other branding elements.
- **Streaming platforms and content creators:** Must ensure that they have proper rights to broadcast gameplay and use in-game assets.

Licensing Agreements

Many companies invest in gaming technology through partnerships with developers or esports teams. Licensing agreements define how intellectual property can be used and prevent costly disputes. Companies should establish clear licensing arrangements to avoid infringement claims.

Case Example: Riot Games vs. Moonton

Riot Games, the developer of League of Legends, sued Moonton for copyright infringement over its mobile game Mobile Legends, claiming it copied substantial elements from League of Legends. The case highlights the importance of protecting game assets from unauthorized use and ensuring licensing agreements are properly structured. Both parties reached a global settlement in April 2024, with Riot Games formally withdrawing all lawsuits.

2. Contract and Employment Law

Player and Team Contracts

Esports teams sign players, coaches, and managers to contracts that outline salary, sponsorship obligations, and behavioral expectations. These agreements must comply with U.S. employment and labor laws to avoid disputes over unfair terms or unlawful termination.

- **Non-compete clauses:** Courts may scrutinize restrictions on where players can compete after leaving a team.
- **Sponsorship agreements:** Terms must be clear on exclusivity, duration, and compensation.
- **Player unionization:** Discussions around collective bargaining for esports players are growing, raising questions about employment classification.

Case Example: Tfue vs. FaZe Clan

Professional gamer Turner “Tfue” Tenney sued FaZe Clan, claiming his contract was “oppressive” and violated California labor laws by restricting his ability to earn sponsorship deals outside the organization. The lawsuit shed light on the importance of fair employment agreements in the esports industry. The case was settled in August 2020.

Endorsement and Sponsorship Deals

Esports athletes, streamers, and influencers frequently enter into sponsorship agreements with brands. These deals must comply with Federal Trade Commission (FTC) guidelines, including clear disclosures of sponsored content to avoid deceptive marketing practices.

Case Example: FTC vs. CSGOLotto

The FTC cracked down on CSGOLotto, an esports gambling website, for failing to disclose that influencers promoting the site were actually its owners. This case underscores the importance of proper sponsorship disclosures and compliance with advertising laws.

3. Regulatory Compliance and Gambling Laws

Gambling and Betting Regulations

Many esports tournaments involve prize pools, and some allow betting on matches. Companies investing in esports gambling platforms must comply with state and federal laws governing online betting.

- **Unlawful Internet Gambling Enforcement Act (UIGEA):** Restricts online gambling practices in the U.S.
- **Loot boxes:** Regulators are debating whether randomized in-game purchases constitute gambling, which could lead to future restrictions.
- **Fantasy esports leagues:** Must navigate legal challenges similar to those faced by traditional fantasy sports platforms.

Case Example: Electronic Arts (EA) and Loot Boxes

Electronic Arts has faced multiple lawsuits over loot boxes in FIFA Ultimate Team, with claims that these in-game purchases constitute illegal gambling. Some U.S. states are considering regulations that would restrict or ban loot boxes.

Consumer Protection and Data Privacy

Gaming companies collect vast amounts of player data, requiring strict adherence to privacy laws, including:

- **Children’s Online Privacy Protection Act (COPPA):** Protects data collected from users under 13.
- **California Consumer Privacy Act (CCPA):** Provides California residents with data access and deletion rights.
- **General Data Protection Regulation (GDPR) compliance:** While a European regulation, U.S. companies with international users must often comply.

Case Example: TikTok’s COPPA Violation

Although not specific to gaming, TikTok was fined by the FTC for violating COPPA by collecting data from children under 13 without parental consent. This serves as a warning to gaming companies that collect data from minors.

4. Antitrust and Competition Law

As the gaming industry consolidates, major acquisitions, such as Microsoft’s purchase of Activision Blizzard, have raised antitrust concerns. The Federal Trade Commission (FTC) and Department of Justice (DOJ) closely monitor large transactions that could stifle competition.

Companies should evaluate:

- **Market dominance concerns:** Avoiding monopolistic behaviors that could trigger legal scrutiny.
- **Exclusive agreements:** Ensuring that partnerships and exclusivity deals comply with competition laws.
- **Mergers and acquisitions:** Obtaining regulatory approval for significant industry consolidations.

Case Example: FTC vs. Microsoft-Activision Merger

The FTC challenged Microsoft’s acquisition of Activision Blizzard over concerns that it would reduce competition in the gaming industry. The case exemplifies the legal complexities surrounding major gaming mergers and acquisitions. The merger was ultimately approved and completed in October 2023, with the FTC’s appeals being rejected as recently as May 2025.

5. Cybersecurity and Online Safety

Gaming platforms and esports organizations face increasingly sophisticated cyber threats, requiring robust security measures and compliance with evolving regulatory frameworks. The intersection of cybersecurity law, data protection, and gaming presents complex challenges that have intensified significantly in 2024-2025.

The gaming industry faced significant cybersecurity challenges in 2024, including major breaches at Ubisoft where cybercriminals accessed sensitive internal systems and leaked employee credentials and game files. Microsoft’s Xbox Live network experienced multiple DDoS attacks causing service outages for millions of users, highlighting vulnerabilities in online gaming infrastructure.

Cyberattacks cost gaming companies millions of dollars annually through immediate recovery costs, long-term financial consequences, lost revenue, legal fees, and significant reputation damage that leads to consumer trust erosion.

- **Federal and state data breach notification laws:** Companies must inform users of data breaches in a timely manner. All 50 U.S. states plus Washington D.C. and three federal territories have data breach notification laws, and the SEC requires public companies to report material cybersecurity incidents in Form 8-K within four business days. New SEC rules effective August 2024

require registered investment advisers, transfer agents, and broker-dealers to notify customers within 30 days if their information may have been stolen.

- **State-specific gaming cybersecurity laws:** Nevada and Massachusetts recently passed laws with specific data security requirements for gaming operators and licensees, reflecting targeted regulatory attention to the gaming sector's unique risks.
- **Online harassment and moderation policies:** The FTC's updated COPPA rule, finalized in January 2025, significantly strengthens cybersecurity requirements for platforms serving children, including mandatory opt-in consent for targeted advertising, strict data retention limits, and enhanced transparency requirements for Safe Harbor programs.
- **Consumer Financial Protection Bureau (CFPB):** The CFPB has issued guidance stating that insufficient data protection or information security violates the Consumer Financial Protection Act's prohibition on unfair acts or practices. Gaming companies must avoid practices like failing to patch known vulnerabilities or lacking procedures to prevent unauthorized account access.
- **Mandatory security measures:** Various federal and state cybersecurity laws require organizations to take specific security measures including implementation of reasonable security procedures, data encryption requirements, and written security program.
- **Critical infrastructure:** The federal government has issued sector-specific guidance for critical infrastructure operators, with detailed statutory and regulatory requirements for various sectors that may apply to large gaming platforms.

In terms of regulatory trends, state regulators in New York, Texas, and California are expected to intensify privacy and cybersecurity enforcement in 2025, leveraging newly enacted state laws and existing UDAP statutes with greater punitive focus than federal enforcement. Additionally, AI is increasingly being used in gaming for safer gambling through behavior tracking, enhanced security measures, and compliance monitoring, while also raising new regulatory considerations.

Case Example: Twitch Hate Raids

Twitch has faced lawsuits over inadequate moderation, as streamers have been targeted by "hate raids," where malicious actors flood their streams with hateful content. The case highlights the need for strong online safety policies in esports and gaming.

6. Other Recent Developments

The gaming and esports industry has experienced significant regulatory changes in 2024-2025, with increased government attention to consumer protection, children's safety, and fair business practices. These developments reflect the industry's growing mainstream recognition and corresponding regulatory scrutiny.

Major FTC Enforcement Actions

Genshin Impact Loot Box Settlement: In January 2025, the FTC secured a landmark \$20 million settlement with HoYoverse (Cognosphere) over Genshin Impact, marking a significant expansion of regulatory oversight into loot box mechanics. The settlement included several groundbreaking elements:

- **Novel Legal Theory:** The FTC argued that selling loot boxes to children and teenagers without verifiable parental consent constitutes an "unfair and deceptive trade practice" under Section 5 of the FTC Act.
- **Age Restrictions:** Companies must block children under 16 from making in-game purchases without parental consent.

- **COPPA Expansion:** The FTC broadly interpreted Genshin Impact as “child-directed” despite its “T for Teen” ESRB rating, based on content analysis and advertising practices targeting children.

Implications for Industry This settlement creates precedent for state attorneys general and private class action litigants to file lawsuits under state unfair business practices statutes, significantly increasing litigation risk for games with loot box mechanics appealing to minors.

Updated COPPA Rule (2025)

The FTC finalized significant updates to the Children’s Online Privacy Protection Rule in January 2025, the first major revision since 2013. Key changes include:

Enhanced Consent Requirements

- Mandatory opt-in parental consent for targeted advertising and third-party data disclosures
- Separate consent requirements for different data uses beyond basic service provision

Data Minimization and Retention

- Companies can only retain children’s personal information as long as reasonably necessary for specific purposes
- Explicit prohibition on indefinite data retention

Increased Transparency

- COPPA Safe Harbor programs must publicly disclose membership lists
- Enhanced reporting requirements to the FTC for self-regulatory programs

FTC Workshop on Child Exploitation

The FTC has scheduled a major workshop for June 4, 2025, titled “The Attention Economy: How Big Tech Firms Exploit Children and Hurt Families,” indicating continued regulatory focus on gaming platforms’ impact on minors.

7. Immigration and Visa Issues

Esports relies heavily on international talent, and securing proper visas for players and staff remains a critical and evolving challenge. The U.S. offers several visa pathways for esports professionals, but navigating the immigration system requires careful planning and legal expertise.

- **P-1A visa classification:** Since 2013, when USCIS first recognized an esports player as an athlete and granted Danny “ShiphTUR” Le a P-1A visa for League of Legends competition, this classification has become the primary pathway for internationally recognized esports athletes. The P-1A visa requires evidence of international recognition at a high level of achievement; participation in competitions with distinguished reputations; and substantial skill recognition in more than one country. P-1A visas are valid for up to 5 years for individuals, with extensions possible up to a total of 10 years. Essential support personnel including coaches, trainers, team officials, and referees are also eligible for P-1 classification.

- **O-1 visa for extraordinary ability:** The O-1A visa serves as an alternative for esports professionals with significant achievements, valid for up to three years and extendable in one-year increments. This classification doesn't distinguish between individual and team events and may be more suitable for content creators and streamers with extraordinary abilities.
- **B-1/B-2 visitor visas:** Esports athletes training or competing without receiving payments may qualify for B-1/B-2 visitor visas, particularly those from visa waiver program countries. This option is suitable for short-term training, unpaid tournaments, and amateur competitions.
- **Challenges in visa processing:** The P-1 success rate varies significantly by game, with some esports athletes facing denials due to inconsistent interpretations of what constitutes a "legitimate sport." Recent cases, including Moist Esports' legal battle with U.S. immigration over B-1 visa denials, highlight ongoing procedural challenges and potential misinterpretation of eligibility criteria.
- **2025 Olympic Esports:** The introduction of Olympic Esports Games in 2025 is expected to create new opportunities for esports athletes, potentially strengthening their cases for P-1A and O-1A visas through increased international recognition and legitimacy.
- **Permanent Residency Options:** Qualified esports athletes may pursue EB-1A "green cards" for permanent residency if they can fulfill extraordinary ability requirements, providing long-term stability for top performers.
- **Best Practices for Companies:** Companies should begin visa applications 3-6 months before needed travel dates. They should also gather extensive evidence of international recognition, tournament results, and media coverage. Companies may consider developing backup plans using different visa classifications. Companies may also find it prudent to consider visa needs for coaches, analysts, and other essential personnel (e.g., P-1S classification). Finally, companies should monitor ongoing developments in esports recognition and potential legislative changes that could streamline the immigration process for gaming professionals.

Case Example: Visa Denials for The International

Several Dota 2 players were denied visas to compete in The International, a major esports tournament, due to confusion over esports classifications. This case demonstrates the ongoing challenges in securing visas for competitive gaming professionals.

8. Compliance Recommendations

Immediate Actions for Gaming Companies

- Review and update COPPA compliance programs in light of 2025 rule changes
- Assess loot box mechanics for potential unfair practice exposure
- Implement enhanced parental consent mechanisms for users under 16
- Develop transparent odds disclosure and pricing information
- Monitor state-specific gaming tax and regulatory changes

Strategic Considerations

- Consider federal lobbying efforts as sports betting regulation discussion continues

- Prepare for increased state-level enforcement activity
- Evaluate international expansion opportunities in evolving regulatory environments
- Invest in AI-powered compliance and monitoring systems
- Develop comprehensive children's safety programs beyond minimum legal requirements

These regulatory developments reflect the gaming industry's transition from niche entertainment to mainstream regulated sector, requiring companies to invest significantly in legal compliance and consumer protection measures.

Conclusion

Investing in esports and gaming technology offers tremendous opportunities, but companies must navigate a complex legal environment to mitigate risks. From intellectual property protection and player contracts to gambling regulations and cybersecurity concerns, staying compliant with U.S. laws is essential for success. As the industry evolves, investors and businesses must remain vigilant and proactive in addressing these legal challenges to sustain long-term growth.

related professionals

Jodutt Marwan Basrawi / Associate

D (212) 238-8767

basrawi@clm.com