Insights, News & Events

SURVEILLANCE, CORPORATE ESPIONAGE, AND DEVELOPER PUSHBACK: 4 LESSONS TECH EMPLOYERS SHOULD TAKE AWAY FROM BUILD A ROCKET BOY LITIGATION

Insights
May 26, 2026

Surveillance, Corporate Espionage, and Developer Pushback: 4 Lessons Tech Employers Should Take Away from Build A Rocket Boy Litigation

Recent litigation involving the video game studio Build A Rocket Boy highlights an increasingly common flashpoint for employers in the tech sector: the tension between protecting intellectual property and respecting employee privacy in a distributed workforce. Developers working on the studio's game *MindsEye* have now initiated legal proceedings against company leadership, alleging that internal surveillance measures crossed the line from legitimate monitoring into unlawful workplace spying.

For employers in the tech sector, as well as any employers managing remote development teams and/or sensitive intellectual property, the dispute underscores the legal and reputational risks that can arise when implementing monitoring tools without first establishing sufficient compliance guardrails.

What Happened?

According to recent reporting, a group of developers at Build A Rocket Boy initiated legal proceedings alleging the company installed surveillance software on their work devices without their knowledge.

Related People

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate

858.964.1582

Andreas Moghimi
Associate

The employees, represented by the Independent Workers Union of Great Britain (IWGB) Game Workers Union, contend the company could track keystrokes, record screen activity, and capture microphone audio while they were working on *MindsEye*. The software reportedly remained on employee devices until March 2026, but was removed after more than 40 employees filed a collective grievance with management. The workers claim the company declined to explain why the software was installed, what data was collected, or how the data was stored or used.

The union alleges that the surveillance exceeded the legitimate scope of productivity monitoring and potentially captured information from employees' homes because many developers were working remotely. As a result, workers argue the monitoring constituted an invasive violation of privacy and may run afoul of applicable data-protection laws.

The union's claims have reportedly been escalated through regulatory and dispute-resolution channels in the United Kingdom, including ACAS and the Information Commissioner's Office.

Key Takeaways for Tech Employers

Based on the locations of your consumers, employees, and even the data itself, you may be impacted by surveillance laws and regulations in numerous jurisdictions, overlapping privacy requirements, and even competing responsibilities. Here are four key takeaways you should keep in mind.

1. Monitoring Tools Can Trigger Data Protection Risk

Many technology companies rely on monitoring tools to protect trade secrets, detect insider threats, and maintain cybersecurity. However, monitoring tools may implicate privacy and data-protection laws, especially those that capture keystrokes, audio/video, or screen activity.

You must make employees aware that they have no expectation of privacy when using work devices or accessing company systems, but must also allow them to be free from monitoring in some personal accounts accessed via company systems, locker and restrooms, and in private areas. This balance can become difficult to manage, particularly when employees work from home and personal environments become intertwined with the workplace.

213.402.9586

Brett P. Owens

Partner

813.769.7512

Service Focus

Employee Defection and Trade Secrets

International

Labor Relations

Litigation and Trials

Industry Focus

Tech

2. Transparency and Notice Remain Critical

A recurring allegation in this dispute is that the monitoring software was installed without employee knowledge or consent. Even when monitoring tools are lawful, lack of disclosure can create legal exposure and undermine employee trust. This is particularly true when you utilize artificial intelligence (AI) tools or functionality. If you use AI monitoring, check with your counsel to see whether it triggers additional requirements, including pre-use notices, human review, and numerous other obligations.

3. Unionization and Collective Action Are Increasing in Tech

The involvement of the IWGB's game-worker branch is yet another signal employees in the technology and gaming sectors are increasingly turning to traditional labor relations tools to address workplace concerns. But even where no formal union is present, coordinated employee complaints about workplace policies may constitute protected collective activity under applicable labor laws.

You should ensure your managers and HR personnel respond carefully to group employee concerns and that they avoid communications or actions that could be interpreted as unlawfully discouraging protected activity.

4. Corporate Espionage Concerns Require a Carefully Structured Response

If you are concerned about insider threats or sabotage, you should ensure any investigative or monitoring measures are narrowly tailored, legally vetted, and documented. Overly broad monitoring may create the very litigation risk you are attempting to avoid.

Conclusion

If you have questions about corporate espionage claims, privacy or AI statutes or regulations, or the latest developments in tech, reach out to your Fisher Phillips attorney, the authors of this Insight, or any attorney in our Technology Industry Group. We will continue to monitor the status of this ongoing legal proceeding, so make sure you are subscribed to receive Technology Industry updates by signing up through the Fisher Phillips' Insight system to get the most up-to-date information directly to your inbox.