Sports Litigation Alert

BakerHostetler's Anthony Bowen Talks About Turning Sports Data Into an Asset, Without Losing Control

By Holt Hackney

As professional sports organizations increasingly rely on data and artificial intelligence, questions surrounding privacy, ownership and governance are becoming more complex. Janine Anthony Bowen, a partner at BakerHostetler, advises organizations on technology, data and digital transformation matters, including the risks associated with emerging technologies. In this interview, Anthony examines how teams, leagues and technology providers should approach athlete and fan data, AI-enabled analytics, vendor agreements and evolving privacy regulations while building governance structures that allow organizations to pursue innovation without losing control of valuable data assets.

Janine Anthony Bowen

Hackney: Professional sports organizations are collecting more data than ever. Where do you see the biggest legal and governance risks emerging over the next five years?

Anthony Bowen: Continued broad sharing of personal information through third-party commercial arrangements, disputes regarding ownership of personal and business data shared online with third party vendors or tertiary service providers, and risk when organizations lose track of how or where data is being collected, shared, combined, and reused – those areas are where the risk sits. Athlete biometric information, fan data, betting-related data, AI-enabled analytics – they all create overlapping legal obligations. The challenge is controlling who can use it, for what purpose, and whether that use remains consistent with the original collection and disclosure framework.

Hackney: You have worked extensively in technology and data transactions. How should leagues, teams, and technology vendors structure agreements so that ownership, licensing, and future use of sports data are clearly defined?

Anthony Bowen: I encourage organizations to focus both on broad ownership concepts and specific rights and restrictions. Contracts should clearly define what constitutes and who owns customer data, derived data, and aggregated or de-identified data. They should also state whether data can be used for product improvement, benchmarking, AI training, model development, or other secondary uses. Many significant risks arise from vague provisions that were written before AI became part of the conversation, so concepts around data ownership, rights and obligations in legacy agreements may not provide the purported owners of sports data with the ownership rights they expect or assume.

Hackney: Artificial intelligence is rapidly becoming part of player evaluation, injury prevention, officiating, and fan engagement. What legal questions should sports executives be thinking about now before AI becomes more deeply embedded in the industry?

Anthony Bowen: The first question is what the athlete's expectation regarding the data is, and whether they have consented to its use for purposes potentially unrelated to its initial collection. The second question is where the data (whether or not it is personal information) ends up after collection. Executives should understand whether a vendor is using data for training, model improvement, evaluation, monitoring, or other value-generating purposes. They should also consider retention, security, and subcontractor access. The best time to address those issues is before deployment of the technology, not after.

I would also encourage organizations to focus on governance as much as technology. Even without a comprehensive federal AI law, documenting AI uses, understanding risk profiles, maintaining appropriate human oversight, and implementing governance processes today can help organizations adapt as legal requirements continue to evolve.

Hackney: Athlete data has become a valuable commercial asset. How should organizations balance innovation and monetization with privacy expectations and regulatory compliance?

Anthony Bowen: I do not view innovation and privacy as necessarily competing objectives. Organizations can monetize and innovate responsibly if they treat biometric and health-related data as sensitive, collect only what is needed for a defined purpose, and maintain strong controls around access, retention, disclosure, and secondary use. Trust and good governance are critical, particularly when without proper controls, athlete data may later be used in sponsorship, betting, marketing, or AI-related contexts.

Hackney: Sports organizations increasingly rely on outside technology providers. What are the most common mistakes you see in negotiating technology agreements, and how can organizations avoid them?

Anthony Bowen: The most common problem is assuming existing contract language adequately addresses modern AI-driven services. A clause that once covered basic software updates may now authorize AI functionality, new subprocessors, or new uses of organizational data. Additionally, I encourage clients to focus on data definitions, training rights, retention obligations, audit rights, vendor accountability, and clear restrictions on secondary uses because these are areas where unexpected vendor right can lie in wait. Organizations should also understand whether the vendor's commitments do, or should, flow through to underlying AI providers and other subcontractors. Finally, they should understand how the technology actually uses their data, including whether data may be used for model training, product improvement, benchmarking, or other downstream activities.

Hackney: The legal landscape surrounding data privacy continues to evolve. How difficult has it become for professional sports organizations with national or global operations to maintain a consistent compliance strategy?

Anthony Bowen: The challenge is that there is no single rulebook. Organizations may face different privacy, biometric, sports betting, and AI governance requirements depending on the jurisdictions involved. We are increasingly seeing a patchwork approach in which different states impose different obligations, standards, and expectations. For biometric technologies in particular, some jurisdictions emphasize consent, while others focus on notice, disclosure, or opt-out rights. That environment makes governance, transparency, documentation, and ongoing risk management essential parts of any compliance and growth strategy.

And that's just the United States…compounding the problem is the rest of the world. The EU AI Act and GDPR come from fundamentally different perspectives than US-based regimes when it comes to data protection and AI governance. A truly international organization has to synthesize a framework that complies with the most stringent requirements both internationally as well as in the US. It's clearly doable, but it's a heavy lift.

Hackney: Much of your career has involved helping organizations navigate digital transformation. Looking ahead, which emerging technologies do you believe will have the greatest legal impact on professional sports?

Anthony Bowen: AI is the driver and is sucking all the oxygen out of the room. Right now it is removing people interaction from the equation. Ultimately, technology that enhances athlete performance, enhances the sports viewing experience, and creates opportunity for connectivity between athletes and fan bases in new ways will be the most valuable.

It is fair to say that AI will continue to drive many of the most significant legal and governance discussions because it changes how organizations use and derive value from data. As adoption increases, sports organizations will need to carefully navigate issues like concerns about surveillance, tracking, privacy, and civil liberties, while balancing fan experience, security, and regulatory compliance.

Hackney: What distinguishes organizations that successfully treat technology and data as strategic assets from those that simply view them as compliance obligations?

Anthony Bowen: Organizations that understand and treat the protection and cultivation of data as a profit center-type activity as opposed to a cost center-type obligation will see the most value. The easy answer is for organizations to simply monetize data by selling it. The more nuanced and sophisticated answer is to extract value from data to enhance user and customer experiences. To do that organizations must understand where their data is and their data flows, classify data appropriately, and build governance into decisions from the outset. They involve legal, privacy, security, and business stakeholders early rather than treating data governance as a necessary compliance obligation. They understand the value their vendors and customers extract from data. In my experience, those organizations are better positioned to unlock business value while maintaining trust and managing risk.