Behind the Scenes of Sports, Data Never Takes a Break

March 18, 2026

Authors

Eric Lavallée

Partner, Lawyer Partner, and Trademark Agent

Ghiles Helli

Lawyer

The World Anti Doping Agency suffered a data breach in 2016—a vivid illustration that even the most prominent sporting institutions are not immune to cyber incidents. The authorities have now formalized what was previously just an observation: In a bulletin published in 2024, the Canadian Centre for Cyber Security warned that the entire sports ecosystem—spectators, athletes, organizations and government representatives—is the target of cyberattack campaigns.

Malicious actors will attempt extortion through business email compromise, ransomware attacks, phishing, malicious websites and search engine poisoning, among others. Take heed, as when an incident occurs that is serious enough to require a report to the authorities, it is often too late to establish sound governance and engage in due diligence.

The sporting competitions of today are producing massive amounts of data. The quantity is staggering, and the data itself almost Orwellian. Check the tables below to see for yourself.

Data collected on athletes

League	Information collected
NFL	Performance data (statistics, position and movement metrics, speed, and passing, rushing and receiving yards) Medical and/or health data (examinations, injuries, concussion protocols) Substance screening data Data on disciplinary actions and investigations Professional and contractual data Travel, logistics and security data

NHL	Performance data Medical and/or health data (examinations, injuries, concussion protocols) Substance screening data Data on disciplinary actions and investigations Professional and contractual data Travel, logistics and security data
MLB	Performance data Medical and/or health data (examinations, injuries, concussion protocols) Substance screening data Data on disciplinary actions and investigations Professional and contractual data Travel, logistics and security data

Collection of customer information online

League	Information collected
	Information provided by individuals
NFL	Identifiers: name, email, address, telephone number, date of birth; unique identifiers (username, password, SSN and other government identifiers if required, e.g. for awards) Demographic data and other protected categories: gender, race, ethnicity, sexual orientation Financial and commercial information: payment data, purchase history Real-time geolocation; precise geolocation Communication and marketing preferences Favorite team and inferences about preferences Audio, electronic and visual information (e.g., photos provided) Biometric data, if you opt for biometric authentication at the stadium; with consent and additional notice if required Information about your contacts (name, email) that you share; if authorized, access to your contacts, calendars and photos Search queries Content posted (comments, forums) Professional and employment information Education information Information that may be health-related (e.g., accessible seating) Correspondence, waivers, consents and other information sent
	Automatic collection
	Device and network identifiers and technical data: IP address, MAC address, advertising identifiers, device type, browser, OS Usage: page views, links clicked, browsing journeys, application usage data Tracking and emails: cookies, pixels, tags, interaction with emails (opened emails, clicks) Social media (if linked): data received according to your settings and

the platform's policy
Logs and traffic: server logs, stadium Wi-Fi traffic
Video and audio recordings: CCTV and pictures taken or video recorded during events

Information provided by individuals

Identifiers and contact information (name, email, telephone number, address, date of birth)
Commercial information (payments, purchases, services)
Demographic data (language, age, gender, race, ethnicity, household composition and income)
Preferences (favourite team, favourite players)
Photos and/or videos
Content, feedback (comments, surveys)
Contact information of friends
Application data (resume, references, checks permitted)

Automatic collection

Activity and interactions (content viewed, bids, purchases, time spent, cookies, tags), access methods (browser, OS, IP address, browsing history before and after)
Device information and identifiers (type, unique identifiers, local content if allowed)
Location (GPS, Bluetooth, Wi-Fi, cells)
Inferences about preferences
Commercial information about transactions (e.g., timestamps)

Collection from third parties

NHL

Member clubs (ticketing, login credential, usage logs)
Fanatics, NHL Shop, NHL Auctions (name, email, items purchased; marketing engagement statistics)
Other business partners, public sources, commercial sources (data brokers)
Connected social media (according to the platform's settings and policies)

NHL teams*

Contact information: name, email address, home address, gender, date of birth, telephone number (e.g., ticket purchase, ticket transfer, account creation, inquiries, contests, promotions)
Demographic data and preferences (age group, race, gender; preferred events, preferred products, e.g., surveys)
Health data related to accessibility needs
Video surveillance in venues (security; sharing limited by law)
Anonymous traffic analysis and device counting (cameras, technological devices; Wi-Fi); statistics that can be shared with partners

Depersonalized web analytics (Google Analytics); opt-out option
Online advertising and/or remarketing (Google, Facebook, LinkedIn, etc.) through cookies; opt-out mechanisms (platform settings; DAAC)
Geolocation through applications if enabled
Social media: profile data and authorized interactions
Technical data (IP, browser, OS, resolution, location, language, origin, keywords, pages viewed, data entered, ads viewed), identifiers (IDFA, AAID), connection information (operator, ISP, Wi-Fi); ability to recognize a device)

Information provided by individuals

Identifiers and contact information: full name, email address, home address, telephone numbers, date of birth
Security and authentication: password
Payments: payment details
Demographic data: demographic characteristics
Content and recordings: voice recordings, audiovisual recordings
Preferences and interests: information about your interests and preferences
Activity and event related data: information requested for an activity or event (e.g., emergency contact)
Sensitive personal information: as defined by applicable laws (e.g., racial or ethnic origin; health information such as disabilities or allergies)

MLB

Automatic collection

Technical and usage data: IP addresses, device data, usage data
Location and contacts: location data; contacts saved on your mobile device

Collection from third parties

Data from third parties and integrations: information provided by other companies if individuals connect their services

*** This data is collected about website users, people who visit venues, people who apply for jobs or participate in contests, people who submit drafts.**

How leagues are structured

Regarding privacy and personal information, we must look at how sports leagues are organized to understand who does what. In most cases, sports leagues are non-profit organizations or corporations. An entire framework of rules is built around these structures, defining both how governance is done and what business model is used.

First, there are the articles of association and by-laws, which dictate governance, team admissions, voting rights, and the powers of the commissioner or board of directors. There are also the sporting

and competition regulations regarding eligibility, game schedules, transfers, drafts, salary caps and cost control mechanisms. The leagues also adopt integrity and security policies against doping, betting and manipulation, harassment and abuse, as well as commercial agreements covering broadcasting, sponsorships, ticketing and data leveraging, among others. There can also be collective agreements with players' associations and formal dispute resolution mechanisms.

In this environment, the league plays a central role. It generally has the power to adopt, interpret and amend its rules; admit teams; manage expansion and relocation projects and changes of control; as well as the power to impose sanctions such as fines, point deductions, suspensions or exclusions. It also centralizes strategic commercial rights, media rights, trademarks and data, and it implements revenue-sharing policies designed to maintain a competitive balance between teams.

Personal information: the roles of each

Teams

In day-to-day relations with athletes and customers, teams are generally the main point of contact. They sign contracts with players, sell tickets, manage subscriptions and operate online stores and loyalty programs. In practice, teams are often the ones that collect personal information, that explain what the information is used for, that decide what information needs to be collected and that put in place security and incident management measures.

Teams must therefore be able to clearly inform athletes and customers about the purposes for which personal information is collected, the means by which it is collected, the categories of information collected, who receives the information, and the rights that athletes and customers have. Teams must limit collection to what is necessary. They must ensure that information is accurate; they must obtain valid, manifest, free, informed and explicit consent for sensitive information such as health or biometric data; they must implement security measures adapted to risks; they must manage and report confidentiality incidents likely to cause serious harm; they must respond to requests for access and rectification; and they must stringently govern the sharing of information with service providers and mandataries.

Athletes and customers often see the team as the true holder of their data.

Leagues

The role leagues play regarding personal information is more difficult to understand, as it varies depending on activities. When a league directly collects information from an individual, for example through an official application, a broadcasting platform or a transactional site for its own purposes, it must assume responsibilities comparable to those a team has. This is what MLB Advanced Media does, for example, defining itself as a "data controller" with respect to its customers' data.

But in many cases, the league acts behind the scenes. In some respects, it acts as a mandatary for the teams, negotiating and signing technology contracts, broadcasting agreements and other commercial agreements that will be used by the teams. In other respects, it acts as a service provider, offering centralized technology platforms, ticketing systems, data infrastructure and shared administrative services.

Under Quebec law, these two roles—mandatary and service provider—are treated the same: The team can transmit to the league the information it needs to perform the mandate or service contract without having to ask for the consent of each person again, provided that a written agreement imposes clear measures to protect privacy, limits the use of data to the sole purposes of the

mandate or service and governs data retention. The league must also promptly inform a team's privacy officer of any privacy breach or attempted privacy breach and allow the officer to conduct checks.

Also, teams and the league can always choose to base certain exchanges of information on the explicit consent of athletes or customers. However, such consent must be genuinely explicit, free, informed, given for specific purposes and presented separately when asked to be given in writing.

Conclusion

Although professional leagues are the ones in the spotlight, the same logic applies to amateur or non-professional sports organizations. In all cases, the relationship between the league, the team and the athlete or customer must be clearly governed from a privacy standpoint. Sports organizations should map the flow of personal information, harmonize the information messages they give to the those concerned, establish a standard agreement governing the sharing of information between teams and the league, provide simple mechanisms for access and rectification, and have key employees trained in privacy matters.

Incorporating these points into articles of association, by-laws and team and league agreements will reduce risks and strengthen the confidence of athletes, parents, fans and business partners. Yet, a fundamental question still remains: Given that by law, data can only be collected for serious and legitimate reasons (necessity criterion), is the mass of information currently collected in the sports ecosystem really warranted? Sports organizations will have no choice but to delve into this strategic issue.