Computer Fraud and Security
ISSN (online): 1873-7056

Unified Consent in U.S. Sports and Media Analytics: Double Opt-In, Data Governance, and the Reconfiguration of Fan-Centric Marketing

Aditya Bhoga
EXL Service, USA

Abstract

Digital fan engagement has fundamentally reshaped how professional sports leagues and media organizations collect, process, and act on behavioral data. Where broadcasters once relied on ratings estimates and stadium attendance figures, they now operate layered digital ecosystems—mobile applications, streaming services, loyalty programs, and in-venue sensor networks—each generating continuous, individually attributable behavioral telemetry. This expansion has unfolded alongside increasing regulatory scrutiny. The California Consumer Privacy Act and the California Privacy Rights Act have formalized consumer rights over personal data at a scale that directly implicates sports and media enterprises managing millions of fan records. In parallel, third-party cookie deprecation and mobile platform transparency controls have eroded the cross-platform tracking infrastructures that historically underpinned audience targeting.

In response, unified consent frameworks—centralized, verifiable, and architecturally enforced—have emerged as a credible governance model for fan data activation. This article examines how unified consent, and particularly the double opt-in mechanism embedded within it, reconfigures fan data governance across sports and media operations. It analyzes implications for first party data monetization, consent-conditioned personalization in streaming environments, organizational governance, fan trust, sponsorship economics, and the evolution of privacy-enhancing analytic infrastructures.

Keywords: Unified Consent, Double Opt-In, First-Party Data, Fan Data Governance, Privacy-By-Design, Sports Media Analytics

1. Introduction: The Datafication of Sports and Media

Professional sports in the United States have quietly become one of the most data-intensive sectors in the consumer economy. A single league property, say, an NFL franchise, may simultaneously operate a ticketing platform, a branded mobile application, an OTT streaming channel, a fantasy sports integration, an in-stadium beacon network, and a multi-tier loyalty program. Each of these systems generates its stream of behavioral data [1]. Taken together, they produce fan profiles of remarkable granularity: content preferences, purchase sequences, physical attendance patterns, streaming habits, device fingerprints, and social engagement signals all flowing into centralized analytics environments.

For years, this data was collected under consent models that were generous in scope and vague in disclosure. Fans who clicked "agree" on a cookie banner or simply continued browsing a team website were often treated as having granted broad permissions for data collection and downstream commercial use. Few challenged this approach, and regulators were largely still catching up. That era is now closing [2].

The legislative landscape shifted meaningfully with the enactment of the California Consumer Privacy Act and the subsequent amendments introduced through the California Privacy Rights Act. These laws codify specific consumer rights: access to collected data, correction of inaccuracies, deletion upon request, and opt-out of data sales or sharing that apply directly to sports franchises and media platforms serving California-based fans. Beyond legislation, platform-level changes have added further pressure. Privacy changes like app tracking transparency frameworks and the removal of third-party cookies in major web browsers have broken the cross-platform identity infrastructure that programmatic advertising systems have historically relied on.

The industry response unfolding centers on a concept called "unified consent." Rather than patching together disconnected cookie banners and opt-out links across siloed platforms, unified consent builds a single governance layer that captures, stores, propagates, and enforces fan permissions across every channel where data is collected and used. This article traces that shift in depth: what unified consent means structurally, how the double opt-in model strengthens its integrity, and what the transition implies for sports marketing, broadcast analytics, organizational governance, fan loyalty, and the economics of sponsorship [2].

Methodological Approach. This article adopts a conceptual–analytic approach rather than an empirical one. It synthesizes insights from privacy, data governance, sports management, and media analytics literature with regulatory analysis and observed industry practices across U.S. sports leagues and media organizations. The objective is not to present original primary data or statistical estimation, but to develop an integrative framework that explains how unified consent architectures—particularly those incorporating double opt-in mechanisms—reshape fan data governance, analytics methodologies, and fan-centric marketing strategies under evolving privacy and platform constraints.

Touchpoint Category	Primary Data Types Generated	Consent Classification Requirement
Mobile Applications and Team Websites	Content engagement, session duration, click-path telemetry	Marketing and analytics consent
OTT Streaming Platforms	Viewing history, content preferences, device identifiers	Functional, personalization, and ad-targeting consent
In-Stadium Wi-Fi and Beacon Networks	Geo-location, dwell time, proximity signals	Location and behavioral consent
Ticketing and Loyalty Systems	Purchase history, redemption events, identity attributes	Transaction and CRM consent
Fantasy Sports and Betting Integrations	Preference signals, gameplay behavior, financial transactions	Expanded purpose consent with data-sharing disclosures

Table 1: Digital Touchpoint Categories and Associated Data Types in Sports and Media Ecosystems [1], [2]

2. Defining Unified Consent in Sports and Media Contexts

A consent banner that appears on a team website, collects a user's preferences, and then disappears into a local database with no connection to the mobile app, the streaming platform, or the loyalty program constitutes fragmented consent. It is, at best, a fragmented compliance gesture. Unified consent means something structurally different: a centralized governance model that captures permissions wherever a fan interacts, stores those permissions as verifiable artifacts with timestamped provenance, and actively propagates consent signals to every downstream system that might want to activate that fan's data [3].

In practical terms, achieving this goal requires integrating several distinct technologies. Consent management platforms (CMPs) provide the consent capture and storage layer. Customer data platforms (CDPs) unify fan identity records across channels and associate them with permission profiles. Identity resolution systems stitch together cross-device and cross-platform records. Marketing automation and advertising technology systems then query the CMP before triggering any outbound communication or audience activation. The result is an architecture where no system can access a fan's data without first confirming that the fan has granted permission for that specific purpose [4].

What makes this approach genuinely different from legacy approaches is the concept of a single source of truth. Siloed fan identity records, one in the ticketing system, another in the CRM, a third in the OTT platform, carry inconsistent consent assumptions and create both regulatory exposure and analytical noise. Unified consent collapses these silos into a coherent permission profile that follows the fan across touchpoints rather than residing independently in each system [3].

Fig. 1 illustrates the high-level interaction between consent capture surfaces, the centralized CMP, identity resolution pipelines, and downstream activation systems in a representative deployment.

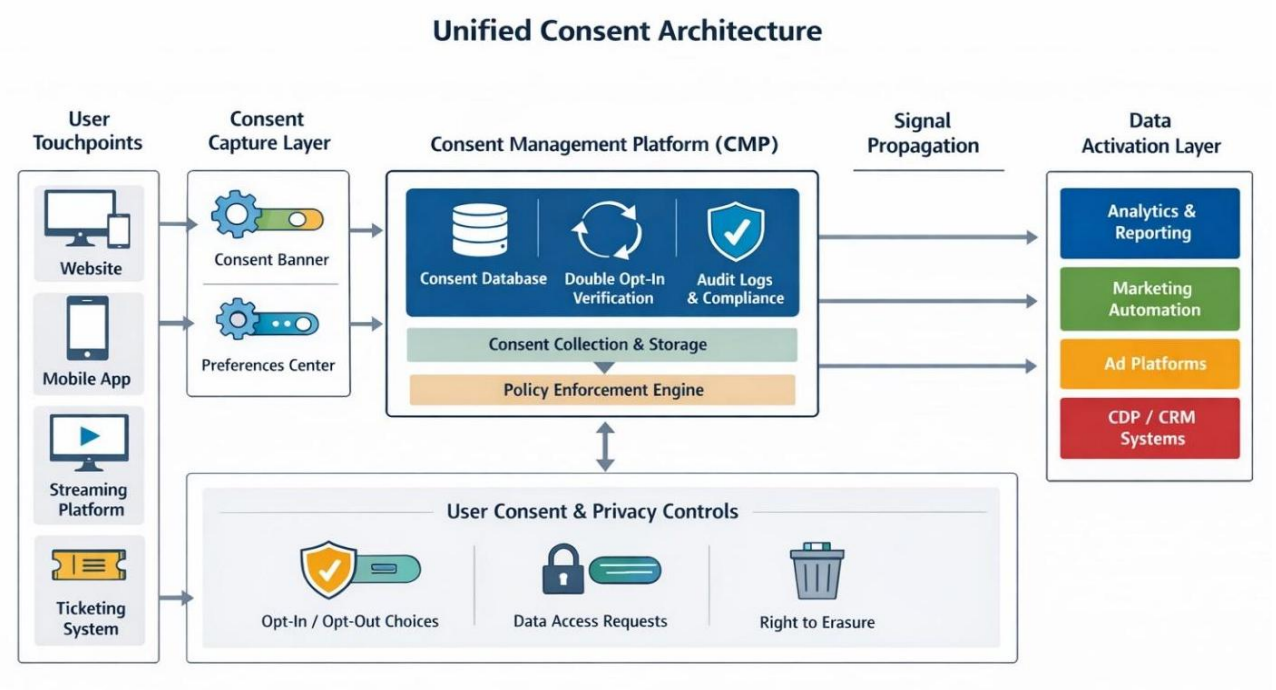

Fig. 1: High-level Unified Consent Architecture with Double opt-in verification

Treating consent as an architectural component rather than a compliance checkbox is a meaningful organizational posture shift, one that carries implications for system design, vendor selection, and product development that extend well beyond the legal team [4].

3. The Double Opt-In Model: Elevating Data Integrity

3.1 What Is Double Opt-In?

Most digital registration flows ask a user to provide contact information and, at the same moment, present them with consent options, checkboxes, toggle switches, or pre-selected defaults. Whatever the user submits in that single interaction is recorded as the consent artifact. That is single opt-in. Double opt-in adds a second step: after the initial submission, the system dispatches a verification message to the contact channel the user declared—an email or SMS—and waits for the user to confirm through a secondary action before the consent as valid [5].

The successful double opt-in creates a record that is meaningfully richer. It includes the channel through which the original consent was submitted, the device and IP address involved, the declared purpose scope, and a timestamp for both the initial submission and the confirmation event. That provenance depth is what makes the artifact useful not just as a permission record but as evidence in the event of an enforcement inquiry or litigation [6].

3.2 Strategic Value in Sports Marketing

Sports data environments create specific conditions that make double opt-in particularly valuable. Playoff seasons, draft events, and broadcast-linked promotions generate spikes in registration activity—and those spikes attract bot submissions, duplicate accounts, and entries tied to invalid contact information. Single opt-in captures all that noise without filtering it. Double opt-in requires an active response from a real inbox, which eliminates a substantial portion of the invalid records before they contaminate the database [5].

Sponsors care about this distinction more than most league marketing teams have historically acknowledged. An audience of verified, intentional opt-ins is a fundamentally different commercial product than a raw list of registrations. Sponsors buying audience activation packages or campaign reach guarantees are increasingly asking for documentation of consent quality—not just audience count. Double opt-in provides that documentation in a way that passive consent models simply cannot [6].

The regulatory protection dimension is also worth stating plainly. Under CCPA and CPRA, an organization that cannot produce a verifiable, time-stamped consent record tied to a specific fan identity is in a weak position when challenged by

a regulator or a class-action plaintiff. Double opt-in artifacts, by virtue of their bilateral provenance, meet evidentiary standards that implied or single-stage consent records fall short of [5].

3.3 Quantitative Implications

The most common objection to double-opt-in is the drop-off rate. Not every user who submits a registration form will complete the verification step; some miss the confirmation message, some abandon intentionally, and deliverability failures account for a portion of the gap. Raw list growth slows [6].

What changes in parallel is the quality distribution of the list that does grow. Subscribers who complete double opt-in demonstrate a baseline of intentionality; they sought out the verification message and acted on it, which single opt-in subscribers do not necessarily share. Over time, this quality differential compounds into measurable differences in open rates, click-through performance, purchase conversion rates, and subscription retention. For organizations managing premium fan communities or high-value loyalty tiers, the trade-off favors quality over volume in both commercial and regulatory terms [5].

Consent Artifact Provenance	Initial submission timestamp only	Bilateral confirmation with secondary channel verification
Data Quality Risk Profile	Elevated exposure to duplicates, bots, and invalid entries	Substantially reduced contamination through active confirmation
Regulatory Defensibility	Limited evidentiary strength under CCPA/CPRA scrutiny	High-confidence audit trail satisfying documentary standards
Initial List Growth Rate	Higher raw registration throughput	Reduced completion rate offset by elevated subscriber quality
Downstream Engagement Metrics	Lower average engagement due to unverified record inclusion	Higher open, click-through, and conversion rates across channels

Table 2: Comparative Characteristics of Single Opt-In and Double Opt-In Consent Models in Sports Marketing [5], [6]

4. Unified Consent and First-Party Data Monetization

The decline of third-party cookies has forced a reorientation that the sports industry was, in many respects, better positioned to navigate than most. Fans have identities. They buy tickets under their names. register for loyalty accounts, subscribe to streaming services, and participate in fantasy leagues, each interaction producing first-party data points tied to verified identities rather than probabilistic cross-device guesses. The infrastructure problem has been governance: how to assemble those data points across platforms while remaining within the bounds of what each fan has explicitly authorized [7].

Unified consent is the governance architecture that makes first-party monetization work at scale. When a fan's consent profile is centralized and propagated across a league's digital properties, the organization can lawfully integrate signals from ticket purchases, app engagement, streaming subscriptions, merchandise transactions, and loyalty participation into a unified fan identity, and then activate that identity for marketing and sponsorship purposes that the fan has specifically approved [8]. The result is a direct-to-consumer ecosystem grounded in permission rather than inference.

What this displaces, importantly, is the dependency on external data brokers. Third-party audience segments carry regulatory risk, there is rarely clear documentation of how underlying consent was obtained, and their targeting precision has declined as tracking infrastructure has fragmented. First-party fan data, governed through unified consent, is categorically superior on both dimensions: it is sourced directly, the consent basis is documented, and the behavioral signals reflect genuine fan relationships rather than probabilistic audience approximations [7].

Clean room environments add another layer of commercial utility. They allow a league to offer its first-party fan audience for sponsor attribution measurement without exposing raw identity records, satisfying both the organization's privacy obligations and the sponsor's performance verification needs within a single compliant architecture [8].

5. Implications for Media and Broadcast Analytics

5.1 Transition from Deterministic Tracking to Modeled Attribution

Attribution in sports media has traditionally relied on persistent identifiers, cookies, device IDs, and hashed email addresses to trace individual fan journeys from content exposure through to conversion. Unified consent changes the data availability picture: when fans have not granted full tracking permissions, those identity threads cannot be followed across surfaces, and deterministic attribution becomes incomplete by design [9].

The industry adaptation has been a shift toward modeling. Media mix modeling reconstructs channel contribution from aggregate outcome data rather than individual paths, making it consent-agnostic by construction. Aggregated event-level reporting measures audience cohorts rather than individuals, preserving performance insight while avoiding the individual-identity dependency that consent restrictions foreclose [9]. Clean room environments have emerged as the favored mechanism for sponsor measurement specifically, enabling two-party attribution computation across consented audience overlaps without raw data exchange, a structure that satisfies both publisher and advertiser obligations simultaneously [10].

The important point is that these methodological adaptations are not inferior substitutes for deterministic tracking. In many measurement contexts, modeled attribution is more statistically robust than deterministic methods that are subject to identity fragmentation and cross-device gaps. Privacy compliance and analytical sophistication are not in tension here; they are converging on the same set of tools.

5.2 Consent-Aware Personalization in Streaming Platforms

Streaming platforms serving sports content must maintain operationally precise distinctions between at least three consent categories: functional processing necessary for platform operation, personalization processing that shapes what content fans see, and data-sharing processing that routes behavioral signals to advertising partners or sponsors [10]. These categories carry different legal bases and require different consent treatments. Unified consent provides the runtime enforcement layer that ensures the right check is run against the right permission record before any of these operations are executed.

The scenario that best illustrates the challenge is a fan who has opted out of targeted advertising but consented to content personalization. The recommendation engine should operate, but it must do so using only viewing history and preference signals, with ad-targeting logic and cross-platform identity sharing excluded from the processing chain [9]. That exclusion cannot be a manual workflow control in a platform serving millions of concurrent users. It must be enforced architecturally, at the point where the personalization system queries for permission before execution. Unified consent frameworks provide exactly that enforcement layer, doing so with the latency and consistency that high-volume streaming environments demand.

Consent Category	Permissible Activation Scope	Excluded Processing Operations
Functional Consent Only	Session continuity, authentication, core content delivery	Behavioral profiling, ad targeting, preference modeling
Content Personalization Consent	Viewing history-based recommendations, genre profiling	Third-party audience sharing, cross-platform identity linkage
Marketing Communication Consent	Email and push notification campaigns tied to viewing interests	External ad network delivery, data broker sharing
Full Advertising and Data-Sharing Consent	Integrated behavioral targeting across all channels and partners	None within declared purpose boundaries
Consent Withdrawal or Absence	Functional processing only, no data activation	All personalization, marketing, and advertising operations

Table 3: Consent Categories and Corresponding Personalization Activation Scopes in OTT Streaming Environments [9], [10]

6. Organizational and Governance Impacts

Unified consent does not slot neatly into any single organizational function. It involves law, technology, and marketing operations simultaneously, requiring genuine cross-functional coordination rather than hand-offs between departments [11].

Cross-Functional Governance: The practical implication is that organizations need standing governance structures, committees, councils, or clearly defined accountabilities—where marketing, legal, IT, and data engineering teams jointly own consent taxonomy decisions, purpose declaration language, and preference center design. Without that shared ownership, consent policy becomes designed by one team and implemented inconsistently by others, producing exactly the fragmentation that unified consent is meant to eliminate [12].

Privacy-by-Design Architecture: New product development represents another organizational fault line. Fantasy platform features, sports betting integrations, augmented reality in-stadium experiences—each carries data collection implications that, if addressed only after launch, require expensive remediation. Privacy-by-design principles require consent capture mechanisms, data minimization controls, and preference center touchpoints to be specified in product requirements from the outset [11]. Treating them as features rather than afterthoughts is not just a compliance posture; it is an engineering efficiency decision.

Consent as a Strategic KPI: Perhaps the most significant organizational shift is the elevation of consent metrics—opt-in rates by channel, preference modification frequencies, withdrawal trend rates, and preference center engagement—to the level of strategic performance indicators tracked alongside commercial KPIs. These signals tell an organization something important about fan sentiment and brand trust that engagement metrics alone do not capture [12].

7. Trust, Brand Equity, and Fan Loyalty

The relationship between a sports fan and their team is not a transactional one. It is identity-laden, emotionally durable, and—when mishandled—capable of generating a level of backlash that comparably scaled brands in other sectors rarely face. Data misuse in this context carries heightened reputational risk: a franchise that is perceived as surveilling its fans or selling their contact information without clear authorization damages a relationship that its competitors cannot easily exploit because the relationship itself is predicated on loyalty that transcends product selection [13].

Unified consent addresses this risk by making the value exchange explicit. When a fan is told clearly what data will be collected, for what purposes, and with which partners, and is given a genuine mechanism to adjust those choices, the dynamic shifts from extraction to participation [14]. That shift matters psychologically. Fans who perceive themselves as having made an informed choice about their data relationship with an organization demonstrate higher satisfaction scores, stronger brand identification, and greater willingness to engage with personalized offers, precisely because the engagement feels invited rather than imposed.

Double opt-in strengthens this dynamic right from the start. The act of confirming consent through a secondary channel is not just a data quality mechanism; it is a micro-interaction that signals intentionality. A fan who seeks out a verification email and clicks it is behaviorally expressing a level of interest that a fan who passively clicked through a registration form did not necessarily demonstrate [13]. Over time, databases built primarily from double opt-in confirmations embody a fundamentally different quality of fan relationship than those built from passive accumulation, one where trust is an asset that has been actively earned and documented rather than assumed [14].

Trust Dimension	Impact of Poorly Governed Consent	Impact of Unified Consent with Double Opt-In
Perceived Transparency	Reduced by opaque data practices and passive consent assumptions	Elevated through explicit purpose disclosures and bilateral confirmation
Data Control Perception	Undermined by inability to modify or withdraw permissions	Strengthened through accessible preference management dashboards

Brand Trust Trajectory	Degraded by incremental opacity disclosures and misuse events	Reinforced by consistent, auditable consent governance practices
Fan Lifetime Value	Suppressed by disengagement following trust erosion events	Enhanced through high-confidence, intentional fan relationship building
Sponsorship Brand Safety	Compromised by association with non-compliant data practices	Preserved through consent-governed, audit-trailed audience activation

Table 4: Trust and Brand Equity Dimensions Influenced by Unified Consent Framework Design [13], [14]

8. Economic Rebalancing: Sponsors and Advertisers

Sponsorship has always involved some degree of audience claim and some degree of trust that the claim is accurate. What has changed is the standard of proof that sophisticated sponsors now expect, as well as the infrastructure they are willing to invest in to verify it [15]. Major league sponsorship negotiations have shifted verified audience counts, documented consent provenance, privacy-compliant data access structures, and clean room-based attribution measurements from aspirational goals to contractual requirements.

Unified consent supports each of these requirements in complementary ways. Audience segments delivered for sponsorship activation carry consent documentation showing that each included fan has authorized the specific type of sharing involved. Audit trails provide chain-of-custody evidence for the consent basis underlying each data transfer. Clean room environments enable the attribution computation that sponsors require without exposing raw identity records to third-party systems, satisfying the league's privacy obligations and the sponsor's measurement need within the same technical framework [16].

What sponsors ultimately gain is not just compliance assurance; it is credibility. An audience of consented, verified fans is a more commercially defensible asset than an undifferentiated audience pool assembled through permissionless tracking [15]. The economic rebalancing that follows, smaller addressable audiences, higher per-fan value, and premium pricing for verified inventory mirror the transition that high-quality publishing environments underwent when programmatic advertising began differentiating by contextual and audience quality. Privacy-preserving attribution tools further strengthen this commercial architecture by making performance verification rigorous without requiring identity exposure [16].

9. Challenges and Constraints

Unified consent is strategically coherent and technically achievable. It is also organizationally difficult in ways that the governance literature tends to understate.

The integration challenge is the most acute. Major sports and media organizations have accumulated vendor stacks over years, sometimes decades in which ticketing platforms, CRM systems, OTT subscription databases, fantasy sports engines, and sponsorship reporting tools were each selected independently, often with no consideration of how consent data would flow between them [17]. These systems lack standardized consent schema, do not support real-time permission propagation natively, and frequently cannot produce the granular, purpose-specific consent records that modern privacy frameworks require. Retrofitting unified consent across this landscape means schema redesign, historical data reconciliation, identity stitching logic development, and middleware layer construction, none of which is trivial, and some of which requires platform replacement rather than modification. Third-party vendor contracts add further friction: real-time consent synchronization obligations must be negotiated rather than assumed, and that process takes time [17].

The user experience dimension is underappreciated. Consent flows that are poorly designed, repetitive prompts, confusing toggle arrangements, and intrusive re-solicitations during live game viewing do not just create frustration. Poorly designed consent flows not only create frustration but also measurably reduce session completion rates and content engagement, resulting in a significant commercial cost that sits uncomfortably alongside the compliance benefit being pursued [18]. The solution is not to simplify consent to the point of meaninglessness, but to invest in preference center design as a serious user experience discipline. Progressive disclosure, clear purpose language, and centralized dashboards that minimize repeated interruptions are engineering challenges as much as they are legal ones, and organizations that treat them accordingly tend to achieve better outcomes on both dimensions [18].

10. Future Outlook: Toward Privacy-Embedded Fan Ecosystems

The consent governance practices taking shape today are likely to look rudimentary within a decade. Several converging technical developments suggest that the next phase of privacy-embedded fan ecosystems will operate at a level of sophistication that current unified consent deployments cannot yet match [19].

Privacy-enhancing technologies represent one such development. Differential privacy mechanisms, secure multi-party computation, and synthetic data generation tools collectively offer pathways for extracting analytically meaningful insights from fan behavioral datasets without requiring those datasets to be assembled in a form where individual records are individually exposed. K-anonymity frameworks provide a structural approach to ensuring that individual fan identities cannot be inferred from query results, even in high-granularity analytical environments, a property that becomes increasingly important as consent coverage narrows and the remaining consented data must work harder analytically [19].

Federated learning offers a longer-term architectural direction of considerable relevance. Rather than centralizing fan data from multiple league or broadcaster properties into a single model training environment, federated approaches allow model updates to be computed locally, on a fan's device or within a platform's own data perimeter, without raw data ever leaving the source environment [20]. For sports media organizations with distributed data assets spanning multiple franchises, broadcast partners, and technology vendors, this architecture addresses both the privacy governance challenge and the practical difficulty of data consolidation across competitive organizational boundaries. AI-driven personalization constrained to federated or differentially private data inputs will require more sophisticated inference techniques, contextual modeling, behavioral cohort construction, and preference signal amplification, but those techniques are maturing rapidly [20].

Organizations that begin embedding privacy engineering competencies into their core product development and analytics functions now, rather than waiting for the next wave of regulatory pressure, are positioning themselves to absorb these technical transitions without the kind of reactive remediation that has characterized earlier compliance cycles.

Conclusion

Unified consent has moved from a peripheral compliance consideration to a foundational architectural requirement in U.S. sports and media organizations. The convergence of CCPA and CPRA obligations, third-party cookie deprecation, and platform-level tracking restrictions has made passive and implied consent frameworks structurally untenable, not merely legally risky but operationally inadequate for sustaining the first-party data ecosystems on which modern fan engagement and sponsorship monetization depend.

The double opt-in model stands out as the most consequential mechanism within this shift. By requiring bilateral channel confirmation before logging a consent artifact, it produces fan database records whose quality, provenance integrity, and regulatory defensibility cannot be replicated through single-stage alternatives. The short-term reduction in raw list growth is a manageable operational cost relative to the long-term gains in subscriber engagement quality, sponsorship credibility, and litigation resilience.

Beyond the mechanics of permission capture, unified consent carries organizational implications that reach into product development, cross-functional governance, and the metrics by which leadership assesses the health of fan relationships. Treating consent as a strategic performance indicator, alongside commercial and engagement KPIs, signals a maturity of data governance that increasingly distinguishes high-performing sports media enterprises from those still managing privacy as a legal afterthought.

Looking ahead, privacy-enhancing technologies, federated learning, and clean room measurement environments will extend the capabilities available to organizations that have already embedded consent governance into their core infrastructure. Those that have invested early are better placed to absorb these transitions without reactive remediation and to position verified, consented fan relationships as their most durable competitive asset.

References

[1] Brett Hutchins, "Tales of the digital sublime: Tracing the relationship between big data and professional sport," Convergence: The International Journal of Research into New Media Technologies, 2015. [Online]. Available: https://journals.sagepub.com/doi/10.1177/1354856515587163

[2] Alessandro Acquisti, et al., "Privacy and human behavior in the age of information," Science, 2015. [Online]. Available: https://pubmed.ncbi.nlm.nih.gov/25635091/
[3] Sarah Spiekermann, et al., "Engineering privacy," IEEE Transactions on Software Engineering, 2009. [Online]. Available: https://ieeexplore.ieee.org/document/4657365
[4] Tal Z. Zarsky, "Incompatible: The GDPR in the Age of Big Data," Seton Hall Law Review, 2017. [Online]. Available: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr
[5] Foster Provost and Tom Fawcett, "Data Science and Its Relationship to Big Data and Data-Driven Decision Making," ResearchGate, 2013. [Online]. Available: https://www.researchgate.net/publication/256439081
[6] PAUL M. SCHWARTZ and KARL-NIKOLAUS PEIFER, "Transatlantic data privacy law," Georgetown Law Journal, 2019. [Online]. Available: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf
[7] Amir Gandomi and Murtaza Haider, "Beyond the hype: Big data concepts, methods, and analytics," International Journal of Information Management, 2015. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0268401214001066
[8] Jaap Wieringa, et al., "Data analytics in a privacy-concerned world," Journal of Business Research, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0148296319303078
[9] Pavel Kireyev, et al., "Do display ads influence search? Attribution and dynamics in online advertising," International Journal of Research in Marketing, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0167811615001159
[10] Tuck Siong Chung, et al., "My Mobile Music: An Adaptive Personalization System for Digital Audio Players," ACM Digital Library, 2009. [Online]. Available: https://dl.acm.org/doi/abs/10.1287/mksc.1080.0371
[11] Peter Schaar, "Privacy by design," Identity in the Information Society, 2010. [Online]. Available: https://link.springer.com/article/10.1007/s12394-010-0055-x
[12] Alan F. Westin, "Social and Political Dimensions of Privacy," Journal of Social Issues, 2003. [Online]. Available: https://spssi.onlinelibrary.wiley.com/doi/abs/10.1111/1540-4560.00072
[13] Rui Biscaia, et al., "Sport Sponsorship: The Relationship Between Team Loyalty, Sponsorship Awareness, Attitude Toward the Sponsor, and Purchase Intentions," ResearchGate, 2013. [Online]. Available: https://www.researchgate.net/publication/258420806
[14] Nikolaos Tsigilis, et al., "Measuring Identification with a Sport Team: An Empirical Comparison of the Sport Team Identification Scale with the Sport Spectator Identification Scale," International Journal of Sport Management, 2023. Available: https://internationaljournalofsportmanagement.com/measuring-identification-with-a-sport-team-an-empirical-comparison-of-the-sport-team-identification-scale-with-the-sport-spectator-identification-scale/
[15] Daniel C. Funk, et al., "Sport consumer motivation: Autonomy and control orientations that regulate fan behaviours," Sport Management Review, 2012. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S1441352311000891
[16] Cynthia Dwork and Aaron Roth, "The Algorithmic Foundations of Differential Privacy," ACM Digital Library, 2014. [Online]. Available: https://dl.acm.org/doi/10.1561/0400000042
[17] William Roberds and Stacey L. Schreft, "Data breaches and identity theft," Journal of Monetary Economics, 2009. [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0304393209001214
[18] Laura Brandimarte, et al., "Misplaced Confidences: Privacy and the Control Paradox," Social Psychological and Personality Science, 2012. [Online]. Available: https://journals.sagepub.com/doi/abs/10.1177/1948550612455931
[19] Latanya Sweeney, "k-anonymity: a model for protecting privacy," ACM Digital Library, 2002. [Online]. Available: https://dl.acm.org/doi/10.1142/S0218488502001648
[20] Tian Li, et al., "Federated Learning: Challenges, Methods, and Future Directions," arXiv, 2019. [Online]. Available: https://arxiv.org/pdf/1908.07873