ENTERTAINMENT AND SPORTS LAW JOURNAL

Hill, TR and Rhodes, J. 2023. Data Decision Making in Sport: Can Players Stop Clubs from Collecting Their Data? *Entertainment and Sports Law Journal*, 21(1): 3, pp. 1–5. DOI: https://doi.org/10.16997/eslj.1517

INTERVENTIONS

Data Decision Making in Sport: Can Players Stop Clubs from Collecting Their Data?

Toby R. Hill[1] and Jamie Rhodes[2]

[1] Independent Researcher, UK

[2] Charles Russell Speechlys, UK

Corresponding Author: Toby R. Hill (toby.r.hill@hotmail.co.uk)

Data analysis has become a fundamental aspect of the sports industry. It is used to improve performances and results, enhance experiences, and increase engagement. As technology has evolved, it has given rise to new means for data collection and analysis, and also new commercial applications for data. This article explores the interest shown by professional athletes in asserting their data rights and the data protection regulations of the United Kingdom as they relate to professional athletes. In particular, the article considers the extent to which the interests of sports clubs conflict with the rights of their players in respect of their special category data. This intervention piece argues that the current data regulations make it impracticable for sports clubs to carry out player special category data collection and analysis, to the extent required to be competitive in modern sport, without being exposed to potential claims from their players.

Keywords: data; regulation; sport; personal data; special category data; data protection; athlete data; analytics

Introduction

Data is both naturally and artificially intertwined with sport, to the extent that is impossible to imagine sport without it. Advances in the collection of data and its diverse applications continue to influence almost all aspects of sport, shaping the future of the sports industry. One such aspect is the use of data in informing decision making within team sports. While the collection of player data by clubs is established practice and, most would argue, a necessary element of modern-day competitive sport, this does not necessarily account for the position prescribed by data protection laws. This article will explore how data is being used to make decisions in sport, how players have demonstrated an interest in asserting their data rights, and how existing data protection laws could enable players to restrict the data that clubs collect from them.

Data decision making in sport

The use of data decision making in sport is nothing new. Two decades ago, Billy Beane of the Oakland A's revolutionised Major League Baseball (MLB) by identifying undervalued players through data mining and recognising which statistics were extrapolative of the runs they would score. Contemporaneously, Sir Dave Brailsford took charge of British Cycling and implemented his (now much heralded) strategy of the 'aggregation of marginal gains'–the hypothesis that hundreds of miniscule improvements will combine to achieve a significant improvement overall.

More recently, advancements in technology and financial pressures have meant sports are increasingly turning to data-led strategies for talent recruitment, pre-game preparation, in-game activity, and post-game activity. Take the Pittsburgh Steelers of the National Football League (NFL), who have partnered with data analysis tool Cognistx, which leverages AI and deep video analytics with multiple models to interpret individual player movements for performance optimization and play selection (Linder 2019). Or New Zealand Rugby's analytics platform dubbed 'Play in Grey', which provides their coaches near real-time analytics by collating one million data points every minute on player actions and match events through machine vision algorithms, which are then converted into usable information by statistical modelling tools (O'Neill 2019). Even the semi-professional football team Leatherhead F.C. has embraced data, entering a somewhat unlikely partnership with IBM Watson; this AI tool provides analysis of Leatherhead's opponents by collecting and analysing data from match reports and other sources, such as Twitter feeds (Pavitt 2019).

Beyond using data to enhance performance, data is also being leveraged within the sporting context to enhance fan experiences and drive engagement, develop automation in refereeing/umpiring, and improve the management of sports organisations. Such is the importance of data in modern sport, data scientists are becoming stars, with former Treasury advisor Laurie Shaw making a high profile 'transfer' to Manchester City in January 2021 (Austin 2021).

Whilst data is irrepressibly permeating every aspect of the sporting world, there remains an elephant in the room. Beyond the Daedalian descriptions peddled by their creators, any data analysis tool fundamentally relies on data subjects in order to operate. In the three examples above, these data subjects include Steelers players and draft prospects, All Blacks players and their opponents, and Leatherhead's rivals in the Isthmian League Premier Division. Do these data subjects know about the use of their personal data and, if so, have they consented to its use? Is consent required for data analytics tools to use publicly available footage and data? Those involved in Project Red Card certainly thought so.

Project Red Card

In a concerted effort to assert control over the use of their data, over four hundred footballers from across the Premier League, English Football League, National League, and Scottish Premiership, united to form Project Red Card. Coordinated by football manager Russell Slade, the 'project' has targeted third-party gaming, betting, and data-processing companies for using the footballers' personal performance and tracking data without their consent. The group is seeking damages for lost income spanning six years (LA 1980: 9). These amounts may of course vary from player to player, but the sum is cumulatively likely to amount to hundreds of millions of pounds (Ornstein 2020). The recoverability of these damages has become less certain following the Supreme Court's decision in *Lloyd v Google* to not award damages in respect of a representative action brought for breaches of the Data Protection Act 1998. That being said, there are key differences between these two actions. Most crucially, the representative action in *Lloyd v Google* encompassed in excess of four million generic iPhone Safari users, whereas Project Red Card involves a self-nominated group of commercially viable professional footballers. Consequently, Project Red Card could pursue an 'opt-in' group litigation order, rather than the 'opt-out' representative action model used in *Lloyd v Google*. With this, damages could be assessed on an individual basis by examining the exploited commercial value of each Project Red Card member's data–an approach that was not possible in *Lloyd v Google*.

Participating players' motivations may be more diverse than the obvious financial incentive. However, a desire to exercise a greater degree of control over their data will certainly be mutual. Football clubs were explicitly excluded from Project Red Card's claims, but, if the claims succeed, they could still be impacted by a court's judgment if it gives direction on the application of data laws to players. After all, clubs are significant data collectors (as set up by standard league contracts, i.e. clause 21 of the standard Premier League Contract), especially with regard to biometric data, and they are also commercial entities (PL 2020: 328). As such, clubs are not the only parties who could be indirectly impacted by a successful outcome for Project Red Card, or indeed any similarly motivated action; the impact could extend to any party in the sports industry that is in any way involved with the collection of player data.

While Project Red Card did not focus its claims on football clubs, it clearly demonstrates player dissatisfaction for missing out on income due to their lack of control over their data. This issue was acknowledged in the United States, by the National Basketball Players Association and National Basketball Association's updated 'Collective Bargaining Agreement', which sees the National Basketball Association gain ownership of players' biometric data on the basis that that data must not be used in contract or transfer negotiations (NFLPA 2020). These could well be the precursors of claims brought in the future against clubs, with a view to limiting the way in which personal data can be used to influence decisions over recruitment, employment, and management. The strength and basis of any such claim would naturally depend on the wording of data laws and their contextual application.

Legal analysis

Data laws in the UK are currently comprised of the Data Protection Act 2018 and the UK General Data Protection Regulation (GDPR).[1] However, it is important to note that where claims cover dates prior to the advent of newer legislation, it is the legislation in force at the time that will be applied to each relevant period covered by the claim, as data laws are unlikely to be applied ex post facto. The earlier window of Project Red Card's claim, for example, falls before the GDPR, when the Data Protection Act 1998 and the Data Protection Directive 1995 were in force.

To assess whether players have a legitimate claim over the data that is collected from them under the current laws, it is first important to set out the types of data that are being collected. This data can be categorised as:

- data recorded from public observation;
- data recorded from private observation; and
- monitoring data.

Data recorded from public observation covers data that anyone could endeavour to record while watching a game, such as the duration a player has been on the pitch for in a football match or the number of passes they made. Data recorded from private observation includes the data collected, generally by appointed individuals, in closed settings like training sessions. This data may include a player's fastest sprint speeds or their aptitude in a training drill. Lastly, monitoring data would be data that relates to the athlete's body. It could include heart rate and other physical quantifiers of exertion. Monitoring data may be collected in training sessions or matches using wearable technology or other equipment,

but, unlike the other categories, it is not visually observable, and requires slightly more involved or intrusive recording methods. Evidently, data from all of these categories can and does play a useful role in decision-making in clubs regarding the players with whom the data originated.

The DPA 2018 and the UK GDPR protect and regulate the processing of 'personal data'. The key elements of the almost identical definitions of this phrase are that:

- the data must relate to a living person; and
- that person must be identifiable from the data either directly or indirectly by information specific to the person (DPA 2018: 3; UK GDPR 2021: 4).

It is quite clear that the above categories of collected player data all constitute personal data, as players are alive, and the data being collected would be redundant if players were not identifiable by it, and therefore they always are. Article 9 of the UK GDPR contains additional and more stringent regulations that restrict the collection of 'special category' data.

Special category data includes, amongst other types, both biometric and health data. The UK GDPR definition of biometric data covers data relating to a person's recorded physical, physiological, or behavioural characteristics that allow for their unique identification (UK GDPR 2021: 4(14)). Guidance from the Information Commissioner's Office (ICO) has set out examples of biometric data, which include, amongst many other types, gait analysis and digital imagery when used for automated identification analysis. Therefore, any video analysis data examining specific player movements, from which the player is identified or identifiable, would be biometric data. The definition of health data covers data relating to a person's physical or mental health (UK GDPR 2021: 4(15). The ICO guidance indicates that the definition is to be interpreted broadly, and one of the many examples given is data collected by fitness trackers/wearable technology. Player medical and injury records naturally fall under the remit of health data. However, given the ICO's broad guidance on the definition of health data, it is likely that any data from the tracking of player physical performance will also be considered health data (ICO 2019). From these definitions and the ICO guidance, it is clear that a very large proportion of the data that is collected from recording and monitoring players' bodies falls under the limitations applied to the collection of special category data.

Clubs have three available grounds for collecting players' personal data:

- consent from the player;
- for a legitimate interest; or
- for the performance of a contract that the player is a party to (UK GDPR 2021: 6(1)(a),(b) and (f)).

Clubs may only collect special category biometric and health data from players if either:

- they have received explicit consent from the player; or
- the data must be collected to fulfil the club's legal obligations as an employer (UK GDPR 2021: 9(2)(a) and (b); DPA 2018: 10(2)).

Therefore, while clubs are able to rely on the 'legitimate interest' and 'performance of a contract' bases for collecting players' personal data, these bases do not extend to the collection of special category data. As such, for clubs to be able to collect special category data, they are burdened with acquiring appropriate consents. Clubs are also permitted to collect and process special category data that has been made public by the data subject (UK GDPR 2021: 9(2)(e)). While this may be a useful ground in limited cases, the reality is that players do not routinely make their own biometric and health data public, and the extent to which they might do so would in any event be far more limited than the clubs' requirements. Consequentially, in most cases clubs must still acquire consent.

Many clubs attempt to obtain generalised data consents by way of player contracts. For example, clause 21 of the standard Premier League Contract requires players to acknowledge and sign in agreement to the collecting, sharing, and processing of both their personal and special category data (PL 2020: 328). However, to satisfy the UK GDPR definition of consent, a number of conditions must be met. Consent must be:

- clear;
- freely given;
- specific to the data being processed; and
- conveniently withdrawable (UK GDPR 2021: 4(11) and 7(3)).

Consent is not considered to be freely given if it is a necessary condition for the performance of a contract (UK GDPR 2021: 7(4)). The 'explicit' consent required for the collection of special category data is intended to be additionally onerous–and, as such, may require this consent to be given at the point of every separate instance of special category data collection.

A player faced with a request to consent to their data being collected and processed should be properly advised of the full implications of doing so. For example, if the purpose of the data collection being consented to includes making that data public, without either full transparency or advice, the data subject player may not be aware of the extent to which they would lose control of that data.

Evidently, the requirements for legitimate consent are problematic for clubs, as they in effect indicate that clubs cannot require players to consent to their data being collected (contractually or otherwise), nor can they prevent or obstruct players from withdrawing their consent. While this is not an issue for the collection of personal data, because of the viable 'legitimate interest' and 'performance of a contract' bases, questions are left concerning the legality of clubs' collection of player special category data, for which consent is usually required. This is because meeting the threshold for legitimate consent, let alone for the 'explicit' consent required for special category data collection, is likely impracticable in the professional team context. Even if a club were to introduce a closely compliant data consent procedure and environment, they would remain in a fragile position due to them having no guarantee over the permanence of consent from any player within the team. In confirmation that this was an intended impact of the GDPR, in the 2019 Guidelines the European Data Protection Board commented,

> "Where a sports club takes the initiative to monitor a whole team […] consent will often not be valid, as the individual athletes may feel pressured into giving consent so that their refusal of consent does not adversely affect teammates." (EDPB 2020).

This means that clubs could be exposed to Project Red Card type data claims brought by players who are disgruntled with the way their special category data has been collected or the purposes for which it has been used. If a player becomes disillusioned with the use of their special category data in the club's data decision making, even without bringing a legal claim, they have a right to withdraw their data consent without fear of it jeopardising their contract. Therefore, players do have the power to intervene, although they may not want to either for fear of negatively impacting teammates or their own career, over which the club has significant and immediate control.

The future of data protection issues for players

The current data protection regime has created an inherent tension between clubs' legitimate interests to assess the performance and condition of their players and the players' rights to restrict access to their special category data. Whilst a judgment from a Project Red Card type action may one day provide guidance on this issue, it is unlikely to provide a resolution to the specific question of special category data. Moreover, the usual arbitrators of the sporting world (national governing bodies, international federations and influential event organisations such as the Premier League) do not have the power to override national or international legislation.

Thus, absent a relevant case being heard, a change in the legislative regime initiated by lawmakers seems the only viable resolution. However, the specifics of such a change are equally challenging. The over-simplified resolution would be to create an exception to allow specified types of special category player data to be collected by clubs for the necessary performance of player contracts.[2] Doing this would in effect remove players' remaining scope to exercise control over almost all of their data rights within this context. Therefore, given the high threshold of justification that this would demand, the question remains as to what categories of special data could justifiably be carved-out for these purposes. Whilst often hackneyed, the 'slippery-slope' argument is clearly germane in this context.

Further issues are on the data-protection regime horizon. As demonstrated by Cognistx, it is now possible to collect biometric data–and possibly health data–through deep video analytics. Leveraging this on opposition players means special category data will be being collected without any sort of contractual relationship or consent. Whilst players may be reluctant to initiate proceedings against their own clubs, they may be more inclined to pursue third-party clubs who breach their personal data rights.

These issues are emblematic of a wider problem within the data protection world: technology and data usage are evolving so quickly, data protection regulation is rapidly becoming outdated. Axel Voss, one of the original authors of the GDPR, stated that it was already out-of-date just three years after is implementation, and would require significant revision to ensure it is fit for purpose (Sharma 2021).

Notes

[1] The UK GDPR is the EU GDPR as retained by the European Union (Withdrawal) Act 2018 section 3 and amended by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

[2] As provided for personal data generally by the UK GDPR article 6(1)(b).

Competing Interests

The authors have no competing interests to declare.

References

Articles and Reports

Austin, S 2021 Man City land big signing in quest to be the best in data science, 17 January 2021. Available at https://trainingground.guru/articles/man-city-land-big-signing-in-quest-to-be-the-best-in-data-science [Last accessed 2 October 2021].

European Data Protection Board 2020 Guidelines 3/2019 on processing of personal data through video devices, 29 January 2020. Available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices.pdf [Last accessed 2 October 2021].

Information Commissioner's Office 2019 What is special category data?, November 2019. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4 [Last accessed 13 March 2022].

Linder, C 2019 What can NFL teams gain from using AI? A play-calling edge and healthier players, some are finding., April 2019. Available at https://newsinteractive.post-gazette.com/field-study-podcast/artificial-intelligence-in-the-nfl/ [Last accessed 2 October 2021].

National Football League Players Association 2020 Collective Bargaining Agreement, 2020. Available at https://nflpaweb.blob.core.windows.net/media/Default/NFLPA/CBA2020/NFL-NFLPA_CBA_March_5_2020.pdf [Last accessed 2 October 2021].

O'Neill, R 2019 NZ Rugby looks to analytics and AWS for competitive advantage, 5 December 2019. Available at https://www.reseller.co.nz/article/669424/nz-rugby-look-analytics-aws-competitive-advantage/ [Last accessed 2 October 2021].

Ornstein, D 2020 Ornstein: Players to sue for hundreds of millions over use of their statistics, 27 July 2020. Available at https://theathletic.com/1949883/2020/07/27/ornstein-hundreds-players-lawsuit-southampton-leeds-wolves-premier-league/ [Last accessed 2 October 2021].

Pavitt, J 2019 How One English Football Club Scores Points with AI, 30 April 2019. Available at https://www.ibm.com/blogs/think/2019/04/how-one-english-football-club-scores-points-with-ai/ [Last accessed 2 October 2021].

Premier League 2020 Handbook Season 2020/21, 2020. Available at https://resources.premierleague.com/premierleague/document/2020/08/11/1256c4b9-23bb-4247-93c0-028f042b010d/2020-21-PL-Handbook-110820.pdf [Last accessed 10 March 2022].

Sharma, M 2021 GDPR is already out of date, founder warns, 3 March 2021. Available at https://www.techradar.com/news/gdpr-is-already-out-of-date-founder-warns [Last accessed 2 October 2021].

Legislation and Cases

Data Protection Act 2018.
Limitation Act 1980.
Lloyd v Google LLC [2021] UKSC 50.
UK General Data Protection Regulation 2021.

How to cite this article: Hill, TR and Rhodes, J. 2023. Data Decision Making in Sport: Can Players Stop Clubs from Collecting Their Data? *Entertainment and Sports Law Journal*, 21(1): 3, pp. 1–5. DOI: https://doi.org/10.16997/eslj.1517

Submitted: 11 September 2023 **Accepted:** 11 September 2023 **Published:** 19 October 2023

Entertainment and Sports Law Journal is a peer-reviewed open access journal published by University of Westminster Press.

OPEN ACCESS