

Project Red Card: An Analysis of Legal, Moral and Ethical uses of Personal Data Collected During Football Games

1. Introduction

Data collection and the subsequent legal and ethical frameworks associated with it are a topic of debate in modern society for many reasons. Referred to as “more valuable than oil” (The Economist, 2017), data is a crucial element of almost all everyday technology and systems that we use and rely on. It is used to improve predictive outcomes of AI based systems that inform sectors such as financial, medical and technology, to name a few.

As governments and the public are catching up with the practices being employed in data collection and processing, there are increasing concerns being raised and controls being placed on companies and individuals involved. The aims are to ensure that these institutions are developing systems that not only protect the interests of the individuals involved, from data subjects to the environment, as well as ensuring no unnecessary harm is brought upon them. This paper will introduce the concepts that should be applied when generating systems utilizing AI and when processing personal data, along with an investigation into some of the legal frameworks and principles that have been established, along with a look to what is on the horizon.

Often the applications of specific legislation can be difficult to interpret. This paper will examine specific use cases surrounding the processing of footballer's personal data in the English football leagues, for gambling and betting purposes, Project Red Card.

Due to the increase of data collection techniques in sports and novel usages of this data, a grey area is created with respect to what is legally, ethically, and morally acceptable with respect to the collection, distribution, and processing of this data. Project Red Card is a project led by former football manager Russel Slade and Jason Dunlop which consists of a lawsuit towards various companies that are involved in the collection and processing of football players, raising questions about consent and legal means to process data under UK legislation.

2. Key ethical issues and data governance practices that need to be addressed when building a data mining application, product, or service, with an artificial intelligence element

When designing a data mining application, product or service that utilizes Artificial Intelligence (AI), there are numerous ethical issues that must be considered concerning how data is collected, what data is collected and why data is being collected. Not only that, but there is a responsibility on those handling data to make sure they are abiding by the appropriate data governance rules, to ensure that data is being stored and processed correctly.

There is a real risk in the development and utilization of AI, that systems can exhibit behaviors that may put certain categories of people at a disadvantage, for example, consider a mortgage application system that has been trained with data that contains historical bias against certain ethnic groups, or against specific genders; these biases would be proliferated throughout the new system. Therefore, it is crucial in the development of new AI, that it does not result in instances such as manipulation, biases, social discrimination, violations of privacy or incorrect censorship, to name a few potential issues.

To achieve this, many factors must be considered, such as race, gender, and age, along with any other characteristics that could be seen to contribute to discrimination, such as disabilities. Development must include results for all cases and must be tested accordingly using people of every given category. Testing is crucial due to the nature of AI and its lack of guarantee that equal conditions will lead to equal results. Organizations and governments across the world have begun to define governance strategies to protect individuals and society, an example would be High Level Expert Group set up by the EU Commission and their recommendations for trustworthy AI (European Commission, 2022), as well as the UK's National AI Strategy (UK Parliament, 2021).

Despite this, there is still a lack of scholarly multidisciplinary research that defines an understanding and the impact of algorithms and the possibilities for regulation. Scholarly multidisciplinary research is essential in this area as it allows developers, researchers, organizations and governments to collectively discuss and define regulations and to be on the same page as one another.

A key step to moving towards this is transparency in the AI decision making processes, i.e., how has the AI reached this decision, and making sure that this is explainable to the people it affects. For example, if an AI system has rejected someone for a mortgage, is there the ability for the system, or the company, to fully communicate why that decision was reached in a way that can be understood and isn't overly technical?

These are all the challenges facing governments, industry and the individuals currently collecting and processing data. Below, we will look at some examples of how this is shaping out in various regions around the world.

3. An overview of current and emerging ethical guidelines, frameworks, principles, and legislation

When discussing anything to do with the collection and handling of data, it's important to understand that there are several legal requirements and industry standards in place that define how those that are collecting, and processing data should operate. As data is collected and processed, oftentimes by artificial intelligence, it's also important to include both AI and data protections in this conversation.

Firstly, it's important to differentiate between the legal requirements that are set by individual countries and/or regions – these are ones in which the requirements to follow are obligatory and to the word. The mechanism of which may change depending on where the data processing is taking place and/or the data subject is located, so it's important that anyone processing data is aware of the implications.

There are too many different regulations, with different aims and nuances, globally, to mention in any meaningful way within this essay, so instead, below, a select group of regulations will be introduced to paint a picture of the global regulatory horizon pertaining to data collection and handling, including the use of AI, diving into more detail on EU and UK GDPR as they will come into prominence more later in the paper.

It's also important to be aware that while regulations are legal requirements, a lot of the regulations surrounding data collection and processing are still very much in their infancy. The era of big data and AI is still relatively new, and regulations are often playing catch up with innovations in development. Depending on the region they are developed in, some regulations may err on the side of caution and more heavily regulate areas in which there are knowledge and experience gaps, instead, leading to large regulatory burdens for those operating under them. Such regulatory programs rely on the development of experience working with the frameworks they have created, along with public

consultations, to iterate on and improve the working for all involved. To that end, recently proposed changes to the UK GDPR will also be discussed to provide some context for the mechanisms to change.

3.1 Legislation and regulatory frameworks

United States of America

Within the USA there are no federal legislation that govern the specific requirements of AI or data protection; however, The Federal Trade Commission Act broadly empowers the Federal Trade Commission to act on both AI and data protection issues (Jillson, E., 2021) (Pittmann, P and Levenberg K., 2021). Namely, AI programs which are shown to use unfair or deceptive practices, and/or are biased or discriminatory, or if AI is used to deny people employment, housing, credit, insurance, or other benefits. For data protection, the FTC can also apply the grounds of unfair or deceptive practices to the handling of personal data.

Governance of AI and data often time falls into the remit of the legislation that pertains to the specific use case. For example, the Food and Drug Administration published the “Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan (Action Plan),” which is seeking to ensure that the safety of users of medical devices applying AI/ML is maintained through regulatory control.

Finally, laws at the state level can also impose their own individual requirements on the users of AI and those handling personal data, and vary widely from state to state, with “47 states having weak or non-existent consumer data privacy laws” (Security.org team, 2020).

European Union

In April 2021 the EU produced a 108-page proposal document for a new regulatory framework surrounding AI within the EU, with the aims of the regulation to create a “well-functioning internal market for artificial intelligence systems” that is based on “EU values and fundamental rights” (Human Rights Watch (HRW), 2021). This framework is still under review but will have a significant impact on companies who are producing and utilizing AI processes in the future.

In the EU, data protections are governed under Regulation (EU) No 2016/679 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, otherwise known as the General Data Protection Regulation, or GDPR (Council Regulation, 2016/679). This came into force in the EU in 2016, replacing and building directive 95/46/EC. More importantly, being a regulation and not a directive meant this was no longer translatable into individual Member State (MS) law in which each individual MS could cherry pick the sections they liked, or even ignore it entirely, but now required a common approach, EU wide. The basic aims of the GDPR are to protect people and their personal data and provide the rules in which people handling personal data must abide, to uphold this protection. Personal data is defined in the regulation as

“... any information relating to an identified or identifiable natural person (‘data subject’) ...”.

It then goes on to explain that an identifiable natural person is one in which any of the data can reference back to, such as

“...a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;”

The key takeaway here is that personal data identifies back to the individual it is related to.

Importantly - paragraph (26) of the regulation states

“Personal data which have undergone pseudonymization, which could be attributed to a natural person by the use of additional information should be considered information on an identifiable natural person”,

It goes on to explain that consideration of the things such as the time and costs required to identify the person should be considered when considering if the data is personal data and states that

“The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.”

To protect the rights of people regarding their personal data, the regulation lays out several principles, such as the following. Personal data shall be:

- Processed lawfully, fairly and in a transparent manner
- Collected for specific, explicit, and legitimate purposes
- Adequate, relevant, and limited to the purpose it is being collected
- Accurate and kept up to date
 - Any inaccurate data is to be erased or rectified without delay
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose in which it is processed
- Processed in a manner that ensures appropriate security of the data

The EU GDPR introduces several vital concepts such as (but not limited to) -

- A “controller” (sometimes referred to as a Data Controller) – this is defined under paragraph 7) Article 4 of the GDPR as “a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data...”. Anyone involved in the collection of data and the subsequent processing of said data must appoint a data controller.
- The right to be forgotten (Article 17) – where users can request their data be removed from the organization entirely, in which real world applications have already been seen, such as Facebook; previously users could only deactivate their accounts, but there is now also the option to delete an account entirely.
- The right to have a legal decision, or ones with similar impacts, not solely made by automated AI (Article 22) – i.e., a human should be involved in the decision-making process at some point or be able to explain the decision. The data subject should also be able to contest any decision with a human.
- Legitimate interests – these serve as a lawful basis in which data can be further processed beyond that in which it was initially collected for. The ICO guidance on legitimate interests contains several key points to be aware of (ICO, no date):
 - Most flexible means for data processing, but cannot assume the most appropriate
 - Reliance on legitimate interests includes extra responsibilities for data controllers, such as protecting people’s rights and interests
 - Three-part test to consider, one needs to:
 1. Identify a legitimate interest
 2. Show that processing is necessary to achieve it, and
 3. Balance it against the individual’s interests, rights, and freedoms
 - Legitimate interests can be that of the data controller or a third party, including commercial, individual, or societal interests.
 - Perform, record, and store a legitimate interest assessment (LIA) to demonstrate compliance
 - Details of legitimate interests must be recorded in privacy notices

United Kingdom:

When the United Kingdom began its process of leaving the European Union, EU GDPR was adopted into UK domestic law as UK GDPR under the Data Protection Act 2018 (UK Parliament, 2018), which acts to supplement certain sections and bring relevance to the GDPR under UK law. At the time of writing, there have been no significant changes to the operational aspects of UK GDPR, from that of EU GDPR, other than those of the governing bodies and relevant changes to the overall decision makers – for example, changing from the EU commission to UK parliament.

There have, however, been several proposed changes: on the 10th of September 2021 a consultation titled “Data: A new Direction” (UK Department for Digital, Culture, Media & Sport, 2021) was issued, requesting feedback by November 2021. Within it, the UK government detailed plans in which to reform UK GDPR – citing the UKs requirement to have “...agile and adaptable data protection laws that enhance its global reputation as a hub for responsible data-drive business that respects high standards of data protection” as the key driver.

The proposals aim to achieve the following:

- Support vibrant competition and innovation to drive economic growth
- Maintain high data protection standards without creating unnecessary barriers to responsible data use
- Keep pace with the rapid innovation of data-insensitive technologies
- Help innovate businesses of all sizes to use data responsibly without undue uncertainty or risk, both in the UK and internationally
- Ensure the Information Commissioner’s Office (ICO) is equipped to regulate effectively in an increasingly data-driven world

Which can be summarized into several key categories:

- Burden of compliance
- Reform of the ICO and review of its responsibilities
- Business innovation
- Personal protection

There are numerous key areas that are being addressed within the proposed changes, such as:

- Legitimate interests – the government is proposing to create a limited, exhaustive list of legitimate interests in which organizations can use personal data without having to apply for a balancing test (or LIA). Feedback from stakeholders found that 42% identified that the lawful grounds for data need to be clearer, often leading to an over reliance of consent and a general lowering of protections for individual, who are unknowingly suffering from “consent fatigue” – where they are so often asked for consent that they might accept, despite not having the time or resources to properly review what they are accepting – providing an exhaustive list for controllers to apply should, in theory, reduce this fatigue and increase protections.
- AI and Machine learning – The document acknowledges that there is a “legitimate need for certain ‘high risk’ AI-derived decisions to require a human review”, however, the taskforce on innovation, growth and regulatory reform has recommended that Article 22 be removed entirely. The reasoning given that in principle, Article 22 is not implemented very often as there is “generally always” a human somewhere in the system. Instead, the emphasis is being placed on generation of better (i.e., fairer, less biased) AI and development of unified standardized assessments for specific use cases.
 - A special note on the generation of fairer and less biased AI, is that the use of special case data – such as ethnicity – that is generally not required for the purpose that the

data is being collected, should be allowed to monitor, and measure bias, unintended or not.

- Data anonymization – suggested changes to the criteria for data to be anonymized are within the document, including that the test should be conducted from the point of view of someone holding the data and shouldn't consider whether there might be data elsewhere that could serve to identify a data subject, which would be implemented into a statutory test for data anonymization
- Removal of the requirement to appoint a data controller – the suggestion instead is that a responsible individual would be required to oversee and manage the privacy management process.
- Reform of the ICO – the document specifies that the ICO should change its focus to dealing with more “serious threats to public trust and responsible data use” commenting that it need to move away from dealing with all the many, smaller, individual complaints that have been raised. To achieve this, the government is suggesting that the issues should have at least been attempted to be resolved between the two individuals in question, before it is raised to the ICO to handle, requiring companies to have transparent complaint processes and publish relevant complaint statistics.

These changes are not exhaustive, but some of the examples of those that are being suggested and have been commented on late last year. It's not clear yet what the outcome of the consultation have been, but some general comments that can be made are that some of the changes are positive – providing exhaustive lists of legitimate interests can only be seen to be a good thing, provided that these lists aren't vague or open to interpretation. It is difficult to see how this could be the case, with data touching on so many industries, but clarification and guidance only serves to help all of those involved. Some of the other proposed changes, however, do appear to either be rebranding of specific requirements, or reduction in protections for the data subjects, such as the changes to anonymization and the removal of article 22. Time will tell whether these changes pass the consultation period and if the intended benefits outweigh the regulatory burden, they place on those processing data.

With respect to AI in the UK, the government is undergoing work to generate a national AI strategy (UK Parliament, 2021) which will include details on cross sector governance and should look past the general scope of AI in GDPR, which is only interested in personal data management.

3.2 Principles

The OECD is a collection of countries that looks to improve the global economy and promote world trade. As part of being an OECD country, there are certain requirements, such as the implementation of certain regulation programs. The OECD has several principles on data privacy and AI (OECD, 2019), which member countries must implement into their respective national/regional laws. These principles serve to provide inform the frameworks in each member country, to help ensure that the wider global regulatory landscape is closer to regulatory harmonization.

The United Nations Educational, Scientific and Cultural Organization (UNESCO) ratified, with its 193 member countries, recommendations in 2021 on data ethics (UNESCO, 2021), stating that governments should “.... conduct ethical impact assessments... and put in place “strong enforcement mechanisms and remedial actions” to protect human rights. dedicate public funds to promote diversity in tech, protect Indigenous communities and monitor the carbon footprint of AI technologies”. However, these recommendations are entirely voluntary up to this point.

3.3 Standards

Aside from current existing legislation, there are a lot of standards out there which look to guide specific sectors and industries into modes of best practice. The difference between standards and legislation is that they aren't legal requirements – often place standards arise where certain industries have gaps in their legal requirements, but there are ethical concerns that need to be addressed, so standards fill those gaps. Being voluntary does mean that not everyone is going to abide by them, but incentivization, such as certifications which may open doors to wider business deals, are often the driving force behind them. For example, in the food industry, there is BRC (British Retail Consortium) certification that is globally seen as a gold standard for food safe manufacturing. Where there isn't a legal requirement for food producers to have this, access for their ingredients to major food producers, or access for their goods into major supermarkets, may be restricted by not having it.

Such standards exist in the data sector already, with certifications such as International Standards Organizations ISO 27001 around information security management and ISO 27701 which relates to the way businesses collect personal data and prevent unauthorized use or disclosure. Such standards don't yet exist for the use of AI, however, there is ongoing work with the International Electrotechnical Commission to define these standards, with the key aim looking at trustworthiness of AI (Gasiorowski-Denis, E., 2020).

4. Project Red Card

Former football managers Russel Slade and Jason Dunlop of the Global Sports and Data Technology Group (GSDT) launched 'Project Red Card' in pursuit of compensation for football players who have had their personal performance data wrong used by the gaming and betting industry (De Freitas et al., 2021; Kowalski, 2021). The claims span over 850 football players, both active and retired, wherein the usage of this data is a breach of data protection laws, dating back six years. Project Red Card is significant as the GSDT are working to avoid a precedent being set within the gaming and betting industry where performance data for players of other sports may also be utilized, seemingly without the consent of the data subject involved.

The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act of 2018 (DPA 2018) define personal data as "Any information pertaining to a natural person who: can be identified, directly or indirectly, from that data." Additionally, some of the data gathered by the gaming and betting industry relates to heart rate, body composition and personal injury, this variety of data is known as personal health data and has further legal implications associated with it. Any organization processing this variety of data must have a lawful basis for the acquisition of player data under article 6 of the UK GDPR (Kowalski, 2021). The lawful acquisition of data requires the consent of the natural person the data is representing. The claim is that the betting and gaming industry processed the personal data of many hundreds of players without their express consent, therefore unlawful conduct has occurred and the GSDT are correct in their assertion that compensation is due to the affected players.

Mr. Slade of the GSDT asserts that football clubs are not the target of the legal claims of Project Red Card. The GSDT intend to educate football clubs with respect to the data their players generate and how this data should be managed. Importantly, the clubs and football governing bodies are not capable of being defendants in this case anyway, as the production and distribution of player data is conducted by third parties who have been licensed by the Football DataCo (De Freitas et al., 2021). These third parties then license the data further to the gaming and betting industry. In summary, the football clubs and governing bodies are not controllers of player data.

The scope within the claim for compensation owed to the players spans tens of thousands of pounds for an individual, and into the millions for a club. However, these estimates are backed by third party litigators who are interested in a significant return on their investment should the players they back receive sufficient compensation, as suggested by Mr. Slade (De Freitas et al., 2021). Thus, the defendants of the claim have a particular interest in persuading the third-party litigators to withdraw their support of the players and cause the case made against them to collapse. The GSDT claim to have identified approximately one hundred and fifty separate defendants. Of these one hundred and fifty defendants, some of them will be appropriately licensed by the FA premier league, Football league and Scottish Premier League, as such, it is feasible these defendants consolidate the grounds of their defense rather than act as individuals, reducing the likelihood of liability. However, the remainder of the defendants operate without any such license, and if caught under the provisions of the UK data protection laws, will be held liable for their usage of player data, and prosecuted for the compensation of the affected players.

5. An analysis of the social, moral, cultural, environmental, legal and ethical issues of Project Red Card

5.1 Assessing the legal veracity of Project Red Card claims

The main complaint from those involved in Project Red Card, is that their data is being processed by betting and gambling companies and gaming companies, and profiting from that personal data, without their knowledge. To assess the credibility of these claims, and discuss what this might mean, it is important to understand the processes involved in the collection, licensing, and use of the data.

Central to the collection of personal data in UK GDPR (hereby referred to as GDPR) is the tenant of consent. Consent under the GDPR needs to be freely given, with the Information Commissioners Office (hereby referred to as the ICO) (ICO, no date) defining freely given as “Consent means giving people genuine choice and control over how you use their data. If the individual has no real choice, consent is not freely given, and it will be invalid. This means people must be able to refuse consent without detriment and must be able to withdraw consent easily at any time. It also means consent should be unbundled from other terms and conditions (including giving separate granular consent options for different types of processing) wherever possible. The UK GDPR is clear that consent should not be bundled up as a condition of service unless it is necessary for that service.”

This is further re-iterated in section Article 7 paragraph 4 of the regulation which states: “When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.”

When analyzing the claims made in project red card – it is clear the defendants believe consent has not been given for that specific cause – i.e., the claimants defend the position that they never consented for their personal data to be used for betting and gambling purposes. Without knowing specific details of each players circumstances, the approach that must be taken here is to assume that players are operating under the general policies of their respective leagues, which will be discussed below. It is important to note that if no agreement to such policies was made, then the grounds for collection of their data and subsequent use, will be much harder to defend.

Where the use of player data for specific uses that weren’t expressly consented to is defensible by the premier league and EFL is in the use of legitimate interests, which have been defined earlier. Their data is being collected in line with data collection agreements in the respective leagues data

policies, and it is in the respective leagues organizations legitimate interests to license this data to commercial partners, including those using the data for betting and gambling purposes.

For the purposes of this discussion, the Premier League's "Players and Related Persons Privacy Policy" (hereby referred to as the PL data policy or PLDP) (Premier League, 2020) and the EFL's "Regulated Persons Privacy Policy" (hereby referred to as the EDL data policy or EFLDP) (English Football League, No Date) will be referenced. The former is dated August 2020 and the latter is dated November 2019, with neither having version numbers or previous versions that are available to the authors at the time of writing. To that end, any discussion points can only be made based upon the information available using the most recent policies and where assumptions are being made, they will be explicitly said to be that.

Both policies recognize that the collection of tracking data is considered personal data, so no argument can be made there to say it isn't. Moreover, for the use in betting and gambling purposes, it would be impractical, to the point of rendering the data useless, to anonymize it in any way, considering bets are placed often against specific players and specific events, e.g., Harry Kane to score a goal in the next 10 minutes, James Milner to get a yellow card, etc. Removing the ability to identify players from that personal data would serve no purpose for the betting companies – moreover, it is not reasonable to think that this data could ever be anonymized, as anyone with access to recordings of the game would easily be able to identify the data subjects out of the 22 players on the field.

According to the PLDP – under paragraph 2.7 it is explained that Football DataCo creates itself, or via their media licensee is Perform Content Limited, trading as Opta. live "tracking data" during football matches, which is then licensed out to various companies depending on their functions. For example, their betting and gaming license is Genius Sports Group Limited, trading as BetGenius. Under this structure, data related to the players performance on field, such as pass completion, on field location heat mapping, tackles made, shots made etc. can be collated by Football DataCo and passed to BetGenius, which in turn is licensed and/or access is further sold onto gambling companies, who can then process the data, and in turn, inform decisions on any odds being made, including in game betting. Later in paragraph 4.1 (m) it states:

"We procure the provision of Tracking Data and Match Data and video footage through our Data Licensees to Clubs, broadcast and sports data partners and other third-party licensees for commercial, statistical and analysis purposes including use in physical and online betting and gaming products and services".

The EFLDP is less clear cut on this aspect – under "What do we do with your personal data?", section 1.1 explains that personal data may be collected and processed under legitimate interests, with the only indication that it could be passed onto gambling companies coming in paragraph 1.2 (n) where it states data can be used "to promote / commercialize EFL football including by publishing or sharing footage, photographs of and information on players and match officials and their performances and by sharing information such as Tracking Data with broadcast partners". Under "Who do we share your personal data with?" 1.1 (k) states "we provide Tracking Data and video footage to Clubs, broadcast partners and sports data partners for commercial, statistical and analysis purposes" and later it explicitly states in 1.1 (m) "we may share personal data concerning regulatory and sports integrity issues with the FA, the police, the Gambling Commission, betting partners (including any EFL official betting partner – currently Sky Bet) and (if required) FIFA/ UEFA" – which will be important later as this appears to be the only mention of an official bettering partner anywhere in the policy.

As the PLDP is clear in their policy on passing data to third parties, and specifically mentioning gaming and betting partners, it is hard to say that players are unaware of their data being used for such causes. The same cannot be said for the EFLDP – it is never explicitly mentioned that tracking data may be shared, with the only reference being in 1.1 (m) as mentioned above, around regulatory and

sports integrity data. The argument can be had that the EFL has an official betting partner in Sky Bet, so it would be implied that they fall under commercial interests of the EFL, but this requires the reader to have information that's not provided in the policy prior to specifying commercial interests and put two points together. It is true that there could also be an argument that common sense prevails – and in being a footballer one should expect bets to be placed against performances, but there is also a counter argument that players may not be aware to the extent of the data being collected on them during a game and the influence it has on profitability for gambling companies.

What can be assumed from the complaints, is that the data subjects were never made aware of the specific companies that have been holding and processing their data. In the PLDP it refers to the data being used for “betting and gaming” purposes but makes no explicit mention to the end companies involved, such as bookmakers. The EFL refers to Sky Bet as their official betting partner, but not in the relevant context of legitimate interests for commercial purposes. When approached for comments about the requirement for a data controller to inform a data subject of any third parties that are processing data under legitimate interests, the ICO commented (ICO, 2022) that this would fall under Article 5 a) of UK GDPR, which states: Personal data shall be: a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’), with the reference to transparency being the key point, however they didn't go on to explain any further how transparency should be applied in this context.

To interpret what this means, transparency isn't defined under GDPR, however, Article 12 has eight paragraphs of requirements for the handling and processing of data to be considered transparent. In the first of these paragraphs, it states:

“The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form”

and what is important here is references to article 14.

Article 14 pertains to

“Information to be provided where personal data have not been obtained from the data subject”

In the case of tracking data in football matches, this data cannot be said to be collected from the subject as it is gathered by the relevant data partners at the EFL and PL. When assessing if the EFL and the PL are fulfilling their requirements with respect to transparency, paragraph 1e) of Article 12 becomes important, stating:

“1. Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (e) the recipients or categories of recipients of the personal data, if any”.

What's interesting here is the reference to “categories” of recipients. There isn't any guidance on the ICO website which helps to understand how broad the application of category can be. The PLDP makes it clear that the recipients can include third parties which may include the use in “physical or online betting and gaming products and services”, but the EFLDP is much broader and only refers to commercial partners – but they have an official betting partner that isn't mentioned in their privacy policy.

The voracity of the legal claims of project red card should therefore come down to disputing the application of consent in legitimate interests, along with the application of the term “categories” in this context. There is a real argument to be had that the current EFL data policy is not transparent and without outside knowledge of their commercial partnerships, players shouldn't expect their personal

data to be shared with betting and gambling companies based purely on what is stated in the policy. On balance, however, it is hard to assume any footballer wouldn't know their data was being used for such purposes, which may turn the legal argument from one around whether it was the duty of the data controllers to explicitly inform the data subjects, or whether extraneous factors can be considered in the application of transparency.

There are also additional claims that have been made, such as the processing of health-related data and the collection and processing of data that is inaccurate. Data concerning health is defined as “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status” – which can be broad in its application. When it comes to footballers, this could be information in the form of injuries, but it's not totally unreasonable to say this could also be extended to say that any metrics measuring fatigue of player. If, for example, a player was playing in extra time and pulling up with cramp because no substitutions were left available, anyone collecting data specifically related to the fatigue and or/cramping could be collecting data concerning health. Moreover, a rapid decline in a player's statistics on movement and passing could indirectly identify a health issue. The problem with considering an angle like this, is that unless the data collected specifically identifies the injury in question, it is hard to argue that its health data specifically.

If data is being processed that identifies specific health conditions, this is considered special category data and processing of which falls under Article 9 on “Processing of special categories of personal data”. Paragraph 1 states “Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.” Paragraph 2 lays out several exemption criteria in which paragraph 1 should not apply, none of which seem applicable in this case. If that is the case, it would be hard to argue that if data being held by the controller falls under the definition of data concerning health, isn't breaching the data subjects' legal rights.

When it comes to incorrect data being held – this extends the original point of knowing where the data is being held, either with a controller or a third party, and whether the data subjects' rights to have that data rectified under Article 16 have been impeded by them not being aware of their data being used. If there is a situation where a data subject has requested that data be rectified and the controller hasn't provided them with confirmation within an appropriate timeframe, this can be a clear breach of their data subjects legal rights.

When looking at the above, it is very clear that there is a wide birth when considering what is legal versus what is ethical. Laws are generally created with a moral purpose, but the minutia involved may not always be ethical. Moreover, what is legal is not always what is ethical, and we have countless case studies available to show that; be it slavery which was still legal on British soil up until 1807, to more recent cases, such as the campaign to return The Parthenon Marbles, otherwise known as the Elgin Marbles, to Greece (BringThemBack.org, No Date). There is a large number of products that countless nations consider to have been stolen or plundered in the era of colonization and occupation, in which British Law protects from ever being returned (Fennell M., 2020-21). Legally, this is all above board, but ethically and morally, is it right?

5.2 Project Red Card: A moral and ethical perspective

As discussed above, legality doesn't always equate to what is ethically and morally right, and the question can be applied to the claims made by project red card.

On face value, it would be simple to say no, it's not right, simply because by virtue of the existence of the project; but it's important to remember that project red card isn't just about raising awareness and correcting perceived wrongs through making sure things are correct moving forward,

there is also a financial aspect in which players are seeking damages. Some could consider this to be people looking for loopholes to gain financial advantage, so it's important to look past this and look at the wider aspects.

The first and arguably most important part of this is consideration of Employer and Employee power dynamic. It can already be seen how there may be a huge disparity between the power of individual players and coaches and the leagues themselves. What's apparent is that playing in the EFL, and Premier League is conditional to agreements to their policies, including the PLDP and the EFLDP.

Within the PLDP, section 8 lays out the rights of the players with respect to their data, including the right to access, the right to correct, right to erasure, objection to use, withdrawal of consent and requests to restrict the use of data. Baked into all these rights, is the condition of legitimate interests – for example, under withdraw your consent, it states:

“Once we have received notification that you have withdrawn your consent, we will no longer process your personal data for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law”.

As discussed above, it's clear that consent was never given explicitly for the use in gambling and betting scenarios, instead there was a reliance on legitimate interests.

Data subjects have a right to object to legitimate interests, but that isn't an absolute right for the data subject. ICO guidance on the right to object (ICO, No Date) states the following “If you are deciding whether you have compelling legitimate grounds which override the interests of an individual, you should consider the reasons why they have objected to the processing of their data. If an individual objects on the grounds that the processing is causing them substantial damage or distress (e.g., the processing is causing them financial loss), the grounds for their objection will have more weight when balancing the individual's interests, rights, and freedoms with your own legitimate grounds. During this process you should remember that the responsibility is for you to be able to demonstrate that your legitimate grounds override those of the individual.” This means that players cannot object based on the grounds that they don't like gambling – there would have to be compelling case for harm, such as religious grounds (which will be discussed later) to provide context to the objection.

The only means in which the data subject could truly remove their data for processing with betting and gaming companies, would be to remove their consent for the respective leagues to process any personal data at all, meaning no legitimate interests could be applied. In section 8.3 of the PLDP, it states the following with respect to requests made by the data subject “8.3. Note: in responding to such requests, we will explain the impact of any objections, restrictions or deletions requested, which may be significant if our use of your personal data is necessary for you to fulfil your role or relationship with the Premier League.” Simply put – you may no longer be able to work within the structure of the premier league without consenting the personal data being collected. #

Coming back to the question of employee and employer power imbalance, this is extremely clear here that the premier league holds practically all the cards when it comes to players personal rights to their data. Legally, everything is done within the books, but it's an all or nothing situation for the players and coaches. Consent and you have a job, don't consent and you risk your career. It's safe to assume this situation is commonplace across all footballing leagues in the world, which further widens the gap between the employer and the employee if they have no real options.

As part of the consideration of the utilization of legitimate interests, companies are required to perform a balancing test on the rights of the data subject, vs the legitimate interest of the data controller.

5.3 Ethics - Harms Modelling

Harms modelling is a practice designed to help anticipate the potential for harm when using AI and collecting data, identify gaps in products that could put people at risk, and ultimately create approaches that proactively address harm (Microsoft, 2021). This practice is based around ethics and can bring comfort and assurance to the users/consumers as well as keeping the provider company in check with the law and regulations. When relating to Project Red Card this sort of model should have been applied by the BetGenius when considering collecting tracking data and licensing it to gaming, betting, and gambling companies.

CATEGORY	TYPE OF HARM	CONTRIBUTING FACTORS	Severity	Scale	Probability	Frequency	POTENTIAL
Risk of injury	Physical or infrastructure damage			▼	▼	▼	LOW
	Emotional or psychological distress		▲	■	▲	▲	HIGH
Denial of consequential services	Opportunity loss			▼	▼		LOW
	Economic loss			▼	▼	▼	LOW
Infringement on human rights	Dignity loss		■	▼	■	▼	MODERATE
	Liberty loss		■	▼	▼	▼	LOW
	Privacy loss		▲	■	▲	▲	HIGH
	Environmental impact			▼	▼		LOW
Erosion of social & democratic structures	Manipulation		▲	■	■	▲	HIGH
	Social detriment		■	▼	■	▼	MODERATE

NOTE: This summary represents the outcome of a qualitative assessment and is used to inform prioritization of responsible innovation mitigations.

Figure 1 - Harms modelling

It is important to consider that bias can play a part in determining the results of harms modelling – for example, when it comes to considering emotional or psychological distress, someone who works in the gambling and betting sector might view the impact as lower due to their opinions, whereas someone who has family members addicted to gambling, may slide completely the other way.

Regardless, these results show that there are some high-risk categories here that should have been due some consideration from the data controller and leaves some questions as to whether they were considered in the balancing test for legitimate interests.

5.4 Cultural considerations

When considering the ethical and moral side of betting we must consider if certain athletes will ever decide to oppose the idea of themselves being an individual betting option. This would cause an inconsistency or an empty space for betting companies and their player data becomes null. Betting in some religions is forbidden, such as Islam. Under Sharia law, there are several things that would be pertinent to understand:

- Money must be earned through hard work and knowledge – money must not be earned through chance
- Muslims must not benefit from lending money to individuals
- Islam strictly prohibits the drinking of alcohol

It's interesting when considering the cultural aspects and their crossover with ethics, morality, and legality. When considering an objection to personal data being processed for gambling purposes, on religious grounds, the argument could be made that the data subject themselves aren't partaking in gambling, so their religious rights aren't being impacted. But ethically and morally, is that right?

This goes wider than project red card and we can see case studies to show that religion is grounds for objection of forced participation in the sports industry. In 2013 (The Guardian, 2013), Papiss Cissé, a Muslim footballer playing for Newcastle United, objected to the new sponsorship deal with payday loan company, Wonga, on the grounds that it offended his religious belief. In 2017 (The Guardian, 2017), Sonny Bill Williams, a New Zealand All Black rugby player and Muslim, was allowed to cover up shirt sponsors for financial institutions on his playing shirt. Finally, in 2021 (The Islam Channel, 2021), UEFA agreed to stop placing alcoholic drinks from sponsors in front of Muslim players during interviews, after several complaints and players of high profile, such as Paul Pogba, who is an openly practicing Muslim, moved them away prior to interviews starting.

Interestingly, from the above examples, Papiss Cissé relented on his demands for removal of the sponsor from his shirt, which serves to further highlight employer and employee balance in the premier league. All of this goes to raise a very interesting ethical and moral question surrounding faith, the employer and forced participation in activities they wouldn't choose to do so otherwise.

5.5 Societal issues

The collection of footballers data for use in gambling and betting applications, at first glance, appears to have little societal concerns. However, when looking into what the data is being used for, it becomes evident how this does raise some issues. Gambling in general has existed for millennia now, with bookmakers deciding odds in their favor; that's the tried and tested business model. However, in the era of big data, bookmakers, through licensing agreements such as those with BenGenius, now have bigger pools of data to inform their odds further in their favor. The intention will always be to maximize profits, which only comes at the customer's expense

5.6 Environmental issues

The act of collecting players tracking data, the transport and storage of such data, and the processing of it all have environmental impacts that are impossible to quantify. Instead, a balanced approach can be applied when considering these issues – is the act of collecting this data, for use in gambling and better applications, necessary? One could argue the same could be applied to the likes of cinema, at home streaming services such as Netflix and other gaming application, but in the gambling industry, there are additional risks to vulnerable people, such as the loss of money, loss of jobs and addiction, that aren't prevalent elsewhere. Moreover, the collection of this data is only supportive to the gambling industry; without it, gambling would still occur, albeit with less oversight for the bookmakers. So, when asking the question again: is this necessary? It's hard to argue that it is, and as trends to move towards larger data sets and more information come to the forefront, it is only going to get worse.

6. Stakeholder impact: an analysis of the data collection and processing practices on (SELECT whatever stakeholders, business, society etc. you may want to talk about)

Data subjects:

The claims by PRC state that financial losses have been occurred by the data subjects in the region of tens of thousands of pounds each, but the question of how legitimate that figure is could be disputed, for example, would the player have got that amount negotiating their own data agreements with the individual companies? Would companies even be interested in singular player data without the bigger picture, should everyone be negotiating their own contracts and some players opting out? Was that data even financial valuable to the player themselves outside of the context of betting and gambling? There is even a counter argument that the commercial agreements in place bring revenue

into the premier league, which in turn is passed onto the clubs and contributes to paying their wages, so financial impact is a very difficult road to quantify.

Looking at PRC from a data rights perspective, the outcome of any claims, should they go to court and not be settled outside, may have further impacts in the footballing world. As discussed, the data policies are vague – this is understandable because companies would have to change them very often if they were too specific, but the level of vagueness compared with the transparency to the data subject should very much be in question:

- A win scenario for project red card should see policy improvements on the grounds of transparency in particular, with better efforts to communicate the use and location of the players data. Not only that, but it may serve to shine a light on what looks like questionable grounds for objection and application of data rights, based on employer and employee power imbalance
- A loss scenario should generally serve to keep things as they are, provided no concession have been made as part of that loss.

What is clear in all of this, is that the impact of the data collection policies in the footballing leagues present the players with a loss of opportunity; in the past, image rights deals have been struck between certain players and clubs to protect their own personal branding and allow them to strike their own personal deals for marketing containing their image. There doesn't appear to be this opportunity afforded, yet, for personal tracking data, but it may be that a consequence of PRC, succeeding or not, is that players now recognise the value in their data and act accordingly. This definitely isn't in the best interest of the leagues, so may only be available to players of the highest caliber and celebrity, those which the pull of that player to the league outweighs specific losses. The idea that the data subject can take control of their own data is one that should be universal, outside of football.

Finally, the mere existence of PRC should serve to make other players aware of their data and their rights. There is always a question where regulations are concerned with respect to education; who is responsible? Sense says it should be the government, and to its credit, there were campaigns around the time of the inception of GDPR, however, most were targeting towards business attaining compliance and not to the individual surrounding their rights. Its not in the club or the leagues best interests to educate the players on their rights either, as they benefit from them maintaining the status quo. So, the responsibility falls on the players agents and legal team – if the player is a high earner, this may be possible, but many players in league 1 and league 2 aren't on huge salaries, so retaining legal counsel to fully review, educate the player, and/or object to certain clauses that may not seem important on face value, wouldn't be high priority. That leaves events and campaigns such as PRC to highlight where these gaps might be and serve as an educational tool.

Data Controllers:

If the data controllers are found to be in breach of UK GDPR, there may be a number of impacts, such as financial ones mentioned above with respect to players. There could also be criminal proceedings and improvement notices filed, with the subjects being placed under increased scrutiny. It's would also be easy to assume that if they had problems in this area, there may be extension to others, such as the use of inaccurate player data and its impact on recruitment and transfers, or the use of consumer data being processed by respective leagues and what that is being processed for under legitimate interests.

One of the key focus points for PRC should revolve around the legitimate interest assessment that has been performed and analysing if it is fair and unbiased; should it be proven to be so, it can serve as case study to wider industry on what not to do.

In most cases, one would also argue that there may be reputational loss – but within the English Football Leagues and the Premier League it's hard to say how much impact that would have. The premier league and the EFL itself aren't the data controllers, but their own policies are those that may be brought into question, and those policies dictate the hierarchy of the data collection and licensing structure, so reputational loss may fall on them. By and large, football is a massive part of the culture of the UK, and the leagues have no competition other than themselves, or foreign leagues and the general public may not have much sympathy towards players they often consider as high earners. What could be interesting is if other foreign leagues policies are structured more in favour of the player, leading to a situation where the reputation of the premier league is off-putting for a player, who may have similar financial incentives to play in another league. Although this doesn't directly impact the data controller themselves, any loss of reputation may be pushed directly downhill from the leagues, onto the data controllers, in the form of removal of contracts and licenses, which may further compound their ability to exist as a business in the future.

Data processors:

Data processors, in this case, will be referred to as the bookmakers.

Legally, there won't be any impact on bookmakers as they aren't the data controllers; there may, however, be financial impact. In all likelihood, if PRC succeeds in its claims through court, it will fall on the leagues to improve their policies and transparency, but in a more extreme scenario where players are now able to opt out of data processing by the league, it may mean that data is no longer available to the bookmakers. There has to be a financial incentive for the purchasing of this data in the first place, and it's been discussed before that it is fed directly into the odds generation process, generating more profits. Without access to this data, or with access to reduced data if players are given more control, are able to opt out, etc, it will mean a reduction in profit. The bookmakers may be able to strike deals with individual players, or groups of players directly, but unless there are other business processes supporting, such as aggressive marketing, deals, etc, there should be a measurable financial loss.

Society:

Society, in this context, will be considered two-fold:

1. The general public
2. Customers of the gambling establishments

In the case of the general public, as discussed above, football is so engrained in the culture of the UK country, it's hard to think that a story like this wouldn't reach mainstream news. As is the case with the data subjects and other players, this should serve as an educational tool on your data rights and could help provide people with an understanding on what they are consenting to and what that consent actually means.

In the case of the customers of the betting establishments, if there is a case to be had that the bookmakers would lose profit, then there is a case to be had that this would be the customers gain.

7. Conclusion

Under the conditions analyzed – with a specific mention back to the fact that previous versions of data policies for the EFL and the PL not being available to the authors at the time of writing for comparison – it is hard to say, legally, that players of the PL would have much merit to their claims on a legal basis. Players of the EFL, however, it becomes more difficult due to the vagueness of their policies.

One must question the aims of the GDPR with respect to transparency, and then inclusion of clauses such as Article 12. Para 1.e), including statement such as “categories of companies”. If the intention is to provide transparency, then real definition of categories should follow. It would be perfectly reasonable for controller to believe that “commercial partners” would be sufficient to cover that clause, but does that really afford for transparency in such a wide application? This could bring a legal fight down to semantics and interpretability of the regulations which, pragmatically, should favor the EFL as they applied the law as they viewed it and its difficult to say they haven’t.

Legality aside, there are some serious ethical issues raised by Project Red Card, that may never get addressed; cultural problems surrounding the use of player data for gambling and betting purposes, the power position of the footballing leagues to supersede players choices with respect to what happens their data and the precedents that have come before, where players have tried to exact control over aspects of their selves being used to promote services against their wishes, and have failed.

What cannot be underestimate, however, is the platform for awareness that something like Project Red Card can offer to the wider world, even outside of football. Being a sport so engrained in the culture of the UK, highlighting data rights alongside it can only be seen as a positive tool for the public, to start questioning how their data is being used elsewhere. The question around responsibility for educating data subjects on their rights will continue, and with very little educational tools on offer for those who don’t even know they have rights to start with, steppingstones, like the publicity Project Red Card should garner, can fill this void.

8. References

BringThemBack.org (No Date) *Campaign for the return of the Parthenon sculptures and the reunification of the monument*. [Online] [Accessed 10th March 2022] <https://www.bringthemback.org/>

De Freitas, I., Pike, J. and Rudkin, T. (2021) *Project Red Card*. 5th November. [Online] [Accessed March 2022]. <https://www.farrer.co.uk/news-and-insights/project-red-card/>

English Football League (EFL). (No Date) *Regulated Persons Privacy Policy* [Online] [Accessed 3rd March 2022] <https://www.efl.com/regulated-persons-privacy-policy/>

European Commission. (2022) *High-level expert group on artificial intelligence* [Online] [Accessed on 14th March 2022] <https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai>

Fennell, M. (2020-2021) *Stuff the British Stole*. ABC News Australia. [Podcast series] [Online] [Accessed 10th March 2022] <https://www.abc.net.au/radionational/programs/stuff-the-british-stole/>

Gasiorowski-Denis, E. (2020) *Towards A Trustworthy AI...* 7th July. International Organisation for Standardisation. [Online] [Accessed 24th Feb 2022] <https://www.iso.org/news/ref2530.html>

Human Rights Watch (HRW). (2021) *How the EU’s Flawed Artificial Intelligence Regulation Endangers the Social Safety Net: Questions and Answers...* 10th November. Human Rights Watch. [Online] [Accessed 24th Feb 2022]

Information Commissioners Office (ICO). (2022) Telephone conversation, Receiver: Daniel Smith, 10/03/2022

Information Commissioners Office (ICO). (No Date) *What is valid consent?* [Online] [Accessed 3rd March 2022] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/consent/what-is-valid->

[consent/#:~:text=Article%20\(4\)%20says%3A,the%20performance%20of%20that%20contract.%E2%80%9D](#)

Information Commissioners Office (ICO). (No Date) *Right to object* [Online] [Accessed 10th March 2022] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-object/>

Information Commissioners Office (ICO). (No Date) *Legitimate Interests* [Online] [Accessed 24th Feb 2022] <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/>

Jillson, E. (2021) *Aiming for truth, fairness, and equity in your company's use of AI...* 19th April. Federal Trade Commission. [Online] [Accessed 24th Feb 2022] <https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai>

Kowalski, J. (2021) *Sports data mining: Project Red Card*. 29th October [Online] [Accessed 1 March 2022]. <https://www.lexology.com/library/detail.aspx?g=ba215723-a21a-4e88-a1dd-981589cec08c>

Microsoft. (2021) *Foundations of assessing harm* [Online] [Accessed 9th March 2022] <https://docs.microsoft.com/en-us/azure/architecture/guide/responsible-innovation/harms-modeling/>

Organisation for Economic Co-operation and Development (OECD). (2019) *OECD AI Principles overview...* May. [Online] [Accessed 24th Feb 2022] <https://oecd.ai/en/ai-principles>

Premier League (PL). (2020) *Player and Related Persons Privacy Policy...* August [Online] [Accessed 3rd March 2022] <https://www.premierleague.com/player-privacy-policy#:~:text=Requests%20should%20be%20made%20in,show%20your%20name%2C%20date%20of>

Pittmann, P and Levenberg K. (2021) *Data Protection Laws and Regulations USA 2021-2022* [Online] [Accessed 24th Feb 2022] <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa#:~:text=There%20is%20no%20single%20principal,Code%20%C2%A7%2041%20et%20seq>

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal L 119*, 4.5.2016, p. 1–88.

Security.org team. (2020) *47 States Have Weak or Nonexistent Consumer Data Privacy Laws...* 14th April. Security.org. [Online] [Accessed 24th Feb 2022] <https://www.security.org/resources/digital-privacy-legislation-by-state/>

The Economist. (2017) 'The world's most valuable resource is no longer oil, but data' *The Economist*. [Online] 6th May [Accessed 17th March 2022] <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>

The Guardian. (2013) 'Papiss Cissé refuses to wear Newcastle's Wonga-branded shirt' *The Guardian*. [Online] 17th July. [Accessed 10th March 2022] <https://www.theguardian.com/football/2013/jul/17/papiss-cisse-newcastle-wonga-shirt>

The Guardian. (2017) 'Sonny Bill Williams permitted to cover up sponsors' logos on religious grounds' *The Guardian*. [Online] 12th April. [Accessed 10th March 2022] <https://www.theguardian.com/sport/2017/apr/12/sonny-bill-williams-kit-alcohol-gambling-logos>

The Islam Channel. (2021) 'UEFA to stop putting alcohol in front of Muslim players' *The Islam Channel*. [Online] [Accessed 10th March 2022] <https://www.islamchannel.tv/blog-posts/uefa-to-stop-putting-alcohol-in-front-of-muslim-players>

UK Parliament. (2018) *Data Protection Act 2018*. 2018 c.12. London: TSO. [Online] [Accessed 24th Feb 2022] https://www.legislation.gov.uk/ukpga/2018/12/pdfs/ukpga_20180012_en.pdf

UK Parliament. (2021) *National AI Strategy* [Online] [Accessed 14th March 2022] <https://www.gov.uk/government/publications/national-ai-strategy>

UK Department for Digital, Culture, Media & Sport. (2021) *Data: A New Direction...* 10th September. [Online] [Accessed 24th Feb 2022] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1022315/Data_Reform_Consultation_Document_Accessible_.pdf

United Nations Educational, Scientific and Cultural Organisation (UNESCO). (2021) *REPORT OF THE SOCIAL AND HUMAN SCIENCES COMMISSION (SHS)*. 22nd November. [Online] [Accessed 24th Feb 2022] <https://unesdoc.unesco.org/ark:/48223/pf0000379920.page=14>

Appendix 1: Peer review:

Peer Review Template

Peer Evaluation

Please use this form to evaluate the contributions of each team member to the group effort.

Consider attendance and participation in team meetings, individual contributions to idea generation and research, communication within the group, etc. These evaluations are completely confidential and will never be shown to your team members. Please respond as honestly as possible.

1. Please allocate a total of 100 percentage points among your team member, including yourself, with higher percentages going to those members who contributed most. In the case of equal contribution, points should be divided equally among team members.

Your name: Daniel Smith

Your student number: 21435099

	<u>Name</u>	<u>% Points</u>
Yourself:	Daniel Smith	60%
Member 1:	Ammar	25%
Member 2:	Shahab	15%
		Total 100 %

2. Explain any particularly high or low allocations, providing concrete examples to illustrate your reasoning.

To be very clear, the majority of the word done for sections 1, 3, 5, 7 and 8 was performed by myself, and when I say majority, I mean vast majority. I also reviewed everything for 2 and 4 and made appropriate changes, such as adding in something to mention transparency and explainability in section 2 as well as rewriting biased language in section 5. In section 5, Ammar performed the Harms modelling, which I included the analysis of.

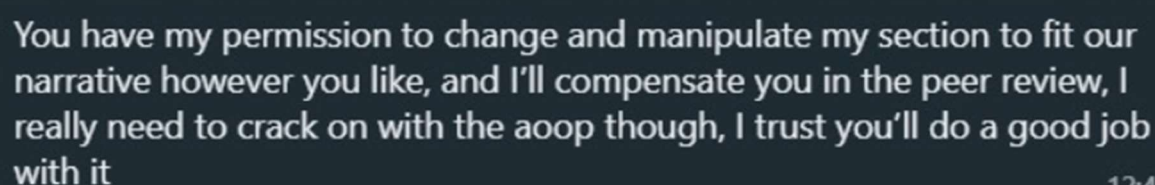
From beginning to end of the project I have felt like there has been very little participation from the group at all. Shahab, in particular, never attends university in person, only coming in on the weeks in which we had the quiz and the last week. He was also “sick” the first week in which the assessment came out after we had agreed on groups, and I don’t have concrete evidence of this, but he was playing a brand new game for hours called Lost Ark, with it constantly being on his discord profile. The week after that, Ammar took a week long holiday to turkey to get a hair transplant. In this two week period it was very very difficult to get any engagement on the project out of them at all.

Even simple requests for them to each come up with a topic they thought would be interesting to review were met with little contribution; Ammar provided something about facebook and facial recognition data in Texas and Shahab offered nothing at all. The group ended up settling on the topic I proposed with very little discussion on other topics we could have looked into.

Work was allocated and dished out in a way which felt like we were working on islands, with people being responsible for specific parts. I asked countless times for group meetings so we could have some form of discussion on the topic and what we were doing so we could make sure we were all working towards the same goals, but those meetings rarely happened, and when they did, they were not productive or involving discussion about what we had done, more direction towards how “easy” things were going to be to finish.

Group sections were not finalised or reviewed or pulled together by the original deadline of the 10th of March which forced all of us into taking extensions. To compound that, neither of them had started any work on the other module we had running alongside it despite it being available for weeks, so further requests for help reviewing the document, questioning things, etc etc were all met with statements about how they were too busy or weren’t going to have time to review the document at all. What we had, up until this point, were a lot of individual pieces of work and nothing pulled together as a clear and coherent essay; lots of the work of the others conflicted things I had said because we had zero time for discussion and it felt like things I had said had been ignored or not understood and not questioned. This led to the responsibility for compiling the document to fall to me, with little recourse to ask them for their input or questions.

Not only that, but I truly feel like both of them missed the mark on the project entirely. Shahab charged himself with performing consequence scanning for our group analysis section, only he performed consequence scanning on the act of the legal complaint about the use of the data and not consequence scanning as if he was the data controller deciding collecting and process the data in the future. The outcome of which read very much like stakeholder impact assessment and didn’t provide any insight where we could look at the consequence scanning and discuss if the data controller should have considered certain things before going ahead with the use. He also made distinct comments about things such as consent being always required and wrote large amounts about the requirement for consent, even though I had mentioned a number of times that consent is only one legal basis for processing of data under UK GDPR and our focus was legitimate interests for this project, rendering a huge amount of what he wrote unusable. He also drew a line between project redcard, said it was directly responsible for a change in advertising trends in gambling to targeted advertising, which when I questioned him on where he got that from, he said it made sense, but I argued that it didn’t because this is a global marketing trend and not exclusive to gambling in England. Afterwhich he said to me:

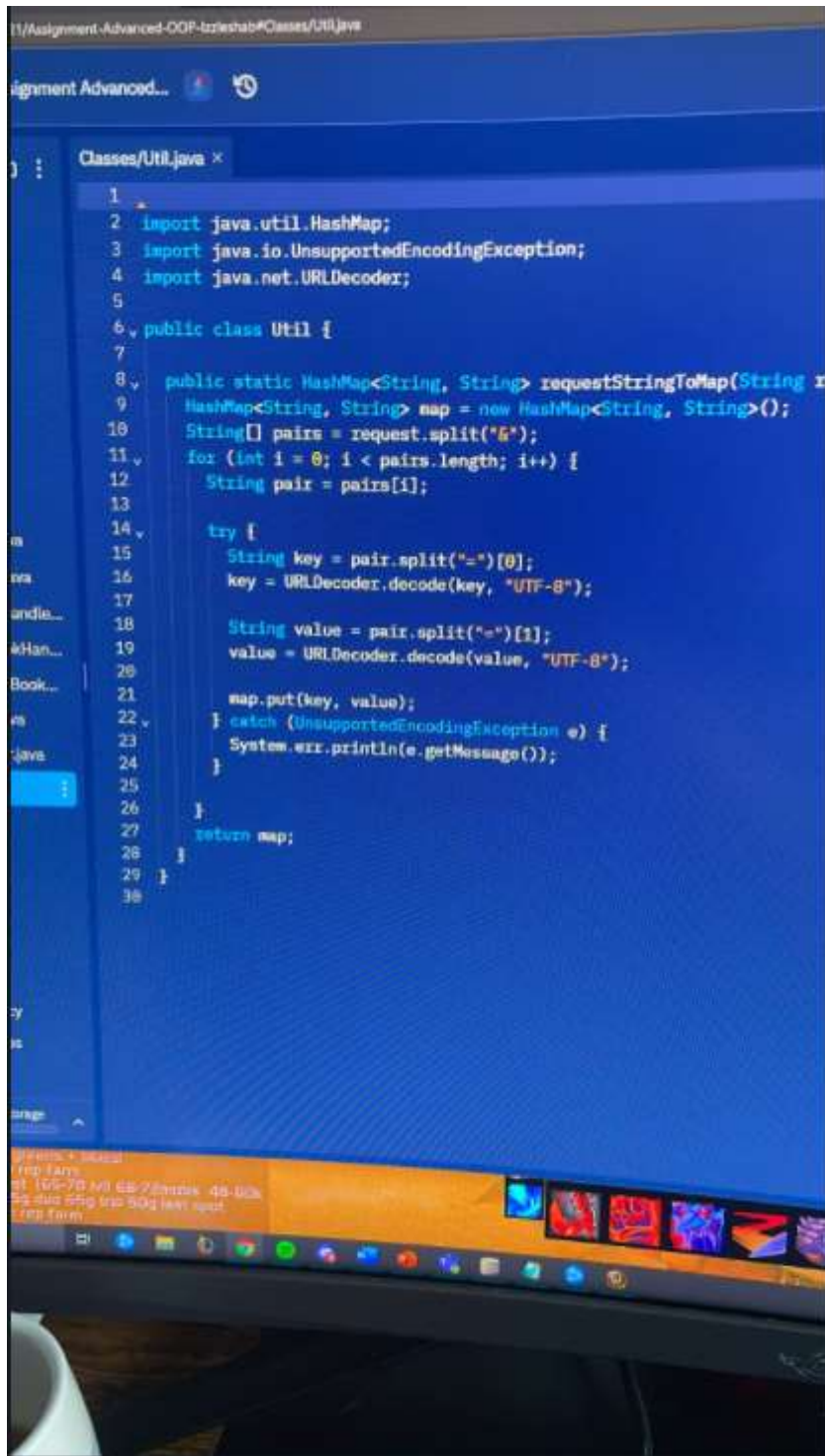


You have my permission to change and manipulate my section to fit our narrative however you like, and I'll compensate you in the peer review, I really need to crack on with the aoop though, I trust you'll do a good job with it

12:48

Which reads as though “you deal with it, I’ve planned my time badly and heres an incentive”.

He also shared screenshots of other things in group chats when he was saying he was too busy, such as the one below, where he is playing world of warcraft (below the IDE). I resent the idea that hes too busy to do a group project because of his own bad time management, so Im spending time picking up the pieces and pulling everything together, sorting references and citations, reading everything they have written, performing cricitcal analysis and trying to engage in real discussion for the betterment of the group and the project, without reciprocation. I have been working on this this morning till night, especially in the last week when it became clear no one else was going to step up and help bring everything together. However, he can find time for games:



Not only all of the above, but I had to change huge amounts of his intro section because he used incredibly biased terminology that, if he had attended lectures, he would understand.

I firmly believe that Shahab's lack of attendance in lectures and university at all contributed to him misunderstanding what the requirements were and instead of saying, he just went ahead with it anyway on his own. He didn't lack trying, but my complaint is that he felt it was appropriate to do a large section of group work, on his own, without engaging as a group for large sections of it and when it came back to be wildly different to what others were working on, his response was for me to tidy it up for him because he was too busy.

The work that Ammar did felt similarly confused and to his credit, he expressed that he hadn't understood a lot of what the project and the course was about. There was a lot missing regarding transparency and explainability in his section, which, when I spoke to him about he agreed should be included and we worked on it. A lot of the things he contributed to the group analysis section were largely either impact assessment for individual stakeholders and more appropriate to his individual section, or could have been things we discussed and talked about to see if they were relevant, which they weren't.

To Ammar's credit, he read everything and attempted to write a conclusion when I requested them to do it, because I had spent days collating the paper, where Shahab said he would and didn't, and only looked at everything once the paper was fully brought together. Ammar's conclusion, however, included nothing from the discussion points in the paper so it had to be rewritten.

I do not like to complain like this and in an ideal world, the paper would be high quality with equal input from all and good discussion, but it has not felt like this and it has not felt like an enjoyable journey at all. It's evident towards the end of the group analysis in social and environmental sections, and in my own individual impact analysis, that I had given up by that point and was just putting things in to cover points because of the fatigue I was feeling, getting this ready with minimal input from either.